institute of development studies

Biometric Digital-ID in Africa: Progress and Challenges to Date – Ten Country Case Studies

December 2025

Edited by 'Gbenga Sesan and Tony Roberts

The Institute of Development Studies (IDS) delivers world-class research, learning, and teaching that transform the knowledge, action, and leadership needed for more equitable and sustainable development globally.
For more information visit: **www.ids.ac.uk**

This publication is part of an African Digital Rights Network (ADRN) project on digital authoritarianism. The African Digital Rights Network is a virtual association of more than 80 digital rights researchers from over 30 African countries, which is hosted by the Institute of Development Studies (IDS). Established in 2020, ADRN has conducted a series of unique studies including on digital citizenship, digital disinformation, and digital surveillance, which have been published as online reports and as part of a collected edition book series. All ADRN publications are open access and free to download from IDS Open Docs or our website **africandigitalrightsnetwork.org**.

Edited Collection

Editors: 'Gbenga Sesan and Tony Roberts

First published by the Institute of Development Studies in December 2025

Suggested citation:

Sesan, 'G. and Roberts, T. (eds) (2025) *Biometric Digital-ID in Africa: Progress and Challenges to Date – Ten Country Case Studies*, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2025.051**

ISBN: 978-1-80470-303-8

DOI: **10.19088/IDS.2025.051**

A catalogue record for this publication is available from the British Library.

Funding acknowledgements

This publication was made possible with funding from the Open Society Foundations.

Other acknowledgements

We wish to acknowledge the generous help and assistance of Shruti Trikanad from the Centre for Internet and Society (CIS) who helped our research team to understand the design of the CIS framework and the experience of using it in other contexts. We also want to respect and acknowledge the prior work of Research ICT Africa in this area, which we aim to complement (van der Spruy et al. 2020). Finally, we want to acknowledge the work of our team of country report authors, including Lesedi Bewlay (Botswana); Nashilongo Gervasius (Namibia); Jimmy Kainja (Malawi); Grace Mutung'u (Côte d'Ivoire); Mame-Penda Ba (Senegal); Arsène Tungali (DRC); Peterking Quaye (Liberia); Helen Beny (Ethiopia); Mohamed Farahat and Afef Abrougui (Egypt); and Yosr Jouini (Tunisia).

Copy editor: James Middleton
Designer: Blossom Carrasco
Proofreader: Catherine Brown

Institute of Development Studies, Library Road, Brighton, BN1 9RE, United Kingdom +44 (0)1273 606261
ids.ac.uk

IDS is a charitable company limited by guarantee and registered in England.
Charity Registration Number 306371
Charitable Company Number 877338

Biometric Digital-ID in Africa: Progress and Challenges to Date – Ten Country Case Studies

December 2025

Edited by 'Gbenga Sesan and Tony Roberts

 DOI: 10.19088/IDS.2025.051

Contents

List of tables

Notes on contributors

Afef Abrougui has more than ten years' experience researching and writing about technology and human rights. She is the owner of Fair Tech, a consultancy based in The Hague with a mission to protect human rights in the digital space. She holds a media studies MA (track: new media and digital culture) from the University of Amsterdam. Afef is an advisor, researcher, and community organiser at the intersection of technology and human rights, and has expertise in network shutdowns, content moderation, and online gender-based violence, working with communities from the global South.

Mame-Penda Ba is Deputy Dean of the Faculty of Law and Political Science and Professor of Political Science at Gaston Berger University of Saint-Louis–Senegal. She received her *agrégation*, which is the highest teaching diploma in the French system, in political science. Prof. Ba is currently Scientific Director of the PhD programme in Political Science. She also heads the Laboratoire d'analyse des sociétés et pouvoirs/Afrique-Diasporas (Research Laboratory on Societies and Powers Africa/Diaspora, LASPAD). Her research interests cover the political sociology of religion, analysis of public policy, gender studies, and the social genesis and dynamics of the state in Africa.

Helen Beny is a PhD candidate in comparative public policy in the Department of Political Science at McMaster University. Her research focuses on the intersection of technology and politics, specifically examining media policies, surveillance, and digital repression in both democracies and autocracies. More specifically, it analyses how regional internet shutdowns are increasingly used against ethno-religious communities in Ethiopia and India. Helen also works as Senior Research Analyst for the Tech Lobby Project, where she examines how tech companies may influence government policies through formal and informal lobbying in Canada. She has contributed to the publication of multiple reports, newsletters, and blog posts to share her findings. Outside of her research, Helen is a community organiser and advocate who supports youth through digital literacy sessions and post-secondary prep workshops.

Lesedi Bewlay is Deputy Director at The Engine Room, where he leads efforts to strengthen partnerships and advise project leads across sub-Saharan Africa. With a background in computer science, Lesedi is passionate about understanding and exploring the links between data, technology, and social change, in particular examining how these intersect across different sectors in civil society. Prior to his current role, he served as The Engine Room's Associate for Engagement and Support in the region, playing a key role in expanding the organisation's reach and deepening its impact. Lesedi co-founded Positive Innovations for the

DOI: 10.19088/IDS.2025.052

Next Generation, a non-profit focused on youth, health, and technology in Botswana, and later founded Tau Technology, which worked to create scalable and sustainable technology solutions across Africa.

Mohamed Farahat is an Egyptian lawyer, legal consultant, and researcher, and has worked as a consultant with various United Nations (UN) agencies such as the United Nations Educational, Scientific and Cultural Organization (UNESCO), United Nations Children's Fund, International Organization for Migration, and UN Women. Mohamed is an author and co-author with ADRN, the Collaboration on International information and Communication Technology Policy for East and Southern Africa (CIPESA), and pan-African social enterprise Paradigm Initiative. He is a member of the United Nations Commission on Science and Technology for Development Working Group on Data Governance; a member of the Multi-Advisory Group (MAG) of the Africa Internet Governance Forum (AFIGF); and a board member of ADRN. Furthermore, Mohamed is a member of UNESCO's Artificial Intelligence (AI) Ethics Experts Without Borders network, and the Global Network of Experts on AI and the Rule of Law. He was a member of the UN High-Level Advisory Body on AI, Vice Chair of the Multi-Advisory Group of the North Africa Internet Governance Forum, and a member of the steering committee of Internet Rights and Principles Coalition.

Nashilongo Gervasius is a technology researcher, and a communication and media lecturer at the Namibia University of Science and Technology where she is currently the Acting Director for Corporate Engagement and Internationalisation. She is the founding President and Board Member of the Internet Society Namibia Chapter and also serves as an advisor to the National Working Group of the Namibia Internet Governance Forum. Nashilongo previously served in the Namibian Presidential Taskforce for the Fourth Industrial Revolution where she chaired the Subcommittee on Infrastructure (Information Communication and Technology (ICT) and Energy) and National Data. She is a former Fellow of the Atlantic Council and GeoTech Center on Artificial Intelligence. Nashilongo is the Director of NamTshuwe Digital, a technology 'hive' at the intersection of tech policy and research, programme implementation, and design, as well as strategic communication.

Yosr Jouini is an interdisciplinary researcher studying emerging technologies and their social implications in the global South. She leads work at Technoloxia, a North Africa-based collective with a mission to provide community-centred perspectives on the region, from the region. Yosr is the founder of Accessibility ABCs, an initiative promoting accessibility across digital platforms. She also hosts the Digitally Yours Podcast, which specialises in digital rights. Previously, she served as an Article 19

Fellow in the algorithmic decision-making track, where she researched the ethical challenges of artificial intelligence and its development in the Middle East and Africa. Yosr was a laureate of the Lina Ben Mhenni Prize for Freedom of Expression for her writings on global voices.

Jimmy Kainja is a senior lecturer in the Media and Communications Department at the University of Malawi, and a PhD candidate in Journalism and Media Studies at the University of the Witwatersrand. He has over ten years' experience teaching Media, Communication, and Cultural Studies, and holds a BSc in media studies and an MRes in media and communication from London Metropolitan University. Jimmy's research focuses on media and telecommunications policy, journalism, digital rights, freedom of expression, access to information, and the intersection of media, democracy, and development. ORCID: **0000-0002-7036-3144.**

Grace Mutung'u is a digital policy researcher, and a research student at the University of Nairobi, working on digital identification (digital-ID) and social justice. She has been involved in ICT policy development and advocacy for over 15 years, contributing to regional and international debates on digital rights, internet governance, and data protection. Grace has held research fellowships at Strathmore University's Centre for Intellectual Property and Information Technology Law, and the Berkman Klein Center for Internet & Society at Harvard University. She co-authored the ADRN publication *Surveillance Law in Africa: A Review of Six Countries* and continues to contribute to multi-stakeholder processes around digital-ID, data governance, and the social dimensions of digital transformation.

Peterking Quaye is the Director of the West Africa ICT Action Network and Regional Coordinator for the Mano River Union Internet Governance Forum. He is a researcher and recent Science, Technology, and Innovation Fellow at Lund University, with over a decade of experience leading internet governance, cybersecurity, digital rights, and policy research across Africa. An Internet Corporation for Assigned Names and Numbers (ICANN) Fellow, and Summit Founder and Director for the Monrovia Technology Summit, Peter advocates for digital inclusion, digital rights, and equitable ICT policies. His work with organisations such as the African Union, World Bank, and Africa Cybersecurity Alliance focuses on bridging digital divides and fostering youth-centric internet regulation. A seasoned professional with degrees and certifications in business studies, and marketing, and an executive MBA in procurement and supply chain management, network, cybersecurity, AI policy, and internet governance, Peter drives strategic advocacy and capacity-building initiatives to promote a free, secure, and inclusive digital future for West Africa and globally.

Tony Roberts is a Research Fellow at the Institute for Development Studies (IDS). After a period as lecturer in Innovation Studies at the University of East London, Tony founded and led two international development agencies working in Central America and Southern Africa. When he stood down as CEO of Computer Aid International, he completed a PhD in the use of digital technologies in international development (Royal Holloway, University of London). After one year working as a Research Fellow at the United Nations University Institute in Macau, Tony joined IDS in 2016 where his research focuses on digital inequality and digital rights. He co-founded ADRN, for which he now edits online reports and is Series Editor of this Zed Books collected edition series Digital Africa for which he previously co-edited *Digital Citizenship in Africa*, *Digital Disinformation in Africa*, *and Digital Surveillance in Africa*. ORCID: **0000-0002-4228-246X**

'Gbenga Sesan is the Executive Director of Paradigm Initiative, a pan-African social enterprise working on digital inclusion and digital rights, with offices in Cameroon, Kenya, Nigeria, Senegal, Zambia, and Zimbabwe. A 2008 Ashoka Fellow, he served on Nigeria's Presidential Committees for Harmonization of the Information Technology, Telecommunications, and Broadcasting Sectors (2006) and the Roadmap for the Achievement of Accelerated Universal Broadband Infrastructure and Services Provision (2013). He served as Vice Chair of the African Technical Advisory Committee for the United Nations Economic Commission for Africa; was appointed to the inaugural High-Level Leadership Panel of the Internet Governance Forum by UN Secretary-General António Guterres in August 2022; is a member of the International Panel on the Information Environment's Scientific Panel on Global Standards for AI Auditing; and serves as Chair of the National Mirror of the Standards Organisation of Nigeria, and the National Technical Committee on Digitally Delivered Services and Trade.

Arsène Tungali is Executive Director of Rudi International, an organisation working at the intersection of technology and human rights based in the Democratic Republic of the Congo. He is a contributing writer with CIPESA, Paradigm Initiative, and ADRN, and has collaborated on ICT policy development processes, including within ICANN, the International Telecommunication Union, and the African Network Information Centre, and was appointed in 2018 to serve on the MAG of the UN's Internet Governance Forum. Arsène holds a master's degree in development studies, and has certificates from institutions including the Hoover Institution and the Global Digital Policy Incubator at Stanford University, and the University of Delaware. He is a Fellow of the United States State Department's Mandela Washington Fellowship for Young African Leaders.

Executive summary

This report provides the most comprehensive and up-to-date account of digital-ID across Africa. It addresses the critical governance challenges of digital identification (digital-ID) systems currently unfolding across the continent. The findings in this synthesis are drawn from ten country reports produced by African researchers from across the continent in a study coordinated by the African Digital Rights Network (ADRN) in collaboration with Paradigm Initiative. The ten country case studies form an integral part of this report and feature Botswana, Côte d'Ivoire, Democratic Republic of the Congo (DRC), Egypt, Ethiopia, Liberia, Malawi, Namibia, Senegal, and Tunisia.

Each country report provides the most detailed documentation to date of the evolving digital-ID system in that country. To provide historical and political context, each report is prefaced with a section detailing the development of paper-based ID systems in the country prior to the adoption of digital-ID and biometrics. The key milestones in the development of the country's digital-ID system is then outlined and its key characteristics documented in detail. At the heart of the report is a systematic assessment of each digital-ID system against 15 tests derived from the comprehensive *Framework for Evaluation of Digital Identity* designed by the Centre for Internet and Society (CIS) to assess digital-ID systems in India (Bhandari, Trikanad and Sinha 2020). Each country report concludes with actionable recommendations for policy, practice, and further research. The 15 tests are organised under three headings: rule of law tests, rights-based tests, and risk-based tests. Our main findings are shown in the table below.

DOI: 10.19088/IDS.2025.053

Table 1: Evaluation of digital-ID in selected African countries

Country	Botswana	Côte d'Ivoire	DRC	Egypt	Ethiopia	Liberia	Malawi	Namibia	Senegal	Tunisia
Rule of law tests										
Legislative mandate	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial
Legitimate aim	Yes	Partial	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial
Defined actors and purposes	Yes	Partial	Partial	Yes	Yes	Partial	No	No	Partial	No
Redress mechanism	Yes	Partial	Partial	Yes	Yes	No	No	No	No	Partial
Accountability	Yes	No	Partial	Yes	Partial	No	No	No	Yes	No
Mission creep	Yes	No	Yes	No	No	No	Partial	No	No	Partial
Rights-based tests										
Necessity and proportionality	Partial	Partial	Partial	No	Partial	No	No	No	Partial	No
Data minimisation	Yes	Yes	Yes	No	Partial	No	Yes	No	No	Partial
Access control	Partial	Yes	Yes	No	Yes	No	No	No	Partial	No
Exclusions	No	No	No	No	Partial	No	No	No	No	No
Mandatory use	Partial	No	Yes	No	No	No	No	No	Yes	No
Risk-based tests										
Risk assessment	Yes	No	No	Partial	Yes	No	No	No	Partial	No
Differentiated approach to risks	Yes	No	No	Partial	Partial	No	No	No	Yes	No
Proportionality	Partial	No	Partial	Partial	Partial	No	Not yet	Not yet	Yes	No
Response to risks	Yes	Partial	No	No	No	No	No	No	No	No

Source: Authors' own based on country reports.

Historical context

- In seven of the ten countries studied, ID systems were originally introduced by colonial powers to serve foreign interests.
- Pressure to adopt biometric digital-ID systems often comes from foreign funders and creates dependencies on foreign technology providers.

Rule of law tests

- The growing sophistication of digital-ID law in some African countries is evidenced by dedicated legislation defining and limiting 'legitimate aim' and 'designated actors'.
- In other African countries, there is a reliance on executive orders and outdated legislation that provide insufficient precision to effectively safeguard against rights violations.
- Countries with dedicated digital-ID and data protection laws often have more transparent and accountable digital-ID systems (e.g. Botswana, Malawi, Namibia).
- However, some countries where legislation is in place have weak enforcement (Côte d'Ivoire, Tunisia) or no independent oversight (Egypt, Malawi).
- As a result, some digital-ID projects risk entrenching inequality and mistrust rather than delivering inclusion or equitable development.

Rights-based tests

- Biometrics are being embedded in digital-ID systems across Africa without adequate justification of necessity or the utility of less intrusive alternatives.
- In some countries studied, digital-ID systems collect personal data such as religion, which is neither necessary nor proportionate to the legitimate aim of identification and creates new risks (Egypt).
- Most countries studied lacked data minimisation strategies, and vague 'public interest' exemptions are used to justify intrusive practices.
- This study highlights the danger of personal data being leaked, sold, or shared with private companies or international agencies (Côte d'Ivoire, Egypt, Senegal).
- Despite the rhetoric of inclusion used to sell the idea of biometric digital-ID, in practice it often results in exclusions – denial of services for marginalised communities.
- Exclusions without redress are resulting in a new class of digitally dispossessed people deprived of rights and entitlements, and without legal recourse.

Risk-based tests

- The lack of structured, legally mandated risk assessment prior to implementation of biometric digital-ID is a blind spot for most African governments.
- Only two out of ten countries in this study conducted risk assessments before implementing digital-ID systems, and none included all stakeholders in the process.
- No country studied used differentiated assessment for higher-risk uses such as biometric ID and other sensitive data use.

Recommendations

A number of recommendations arise from the assessment:

- **Dedicated biometric digital-ID and data protection laws are foundational** to protecting rights, building trust, and securing informed consent for digital-ID.
- **Legislation must clearly define legal aims, permitted actors, and precise exceptions**, and provide adequate resources for robust independent oversight and redress mechanisms.
- **Risk assessment should be carried out** prior to implementation of biometric digital-ID systems.
- **Public engagement and meaningful participation of stakeholders is essential** in the design, implementation, and evaluation of digital-ID systems.
- **Governments should move from the rhetoric of inclusion to concrete measures** targeted to prevent exclusion of people from rights, entitlements, and services.

Digital-ID in Africa: Assessing progress and challenges to date

'Gbenga Sesan and Tony Roberts

 DOI: 10.19088/IDS.2025.054

1. Introduction

This report synthesises evidence from new studies in ten African countries assessing the current state of digital identification (digital-ID) programmes across the continent. In doing so, it provides the most comprehensive and up-to-date picture of digital-ID in Africa. The report provides evidence that some African governments have put in place sophisticated legislative frameworks that provide protections for fundamental human rights that biometric digital-ID systems can put at risk. However, it also identifies gaps and failings that urgently need to be addressed. Fifteen diagnostic tests were applied to the evolving digital-ID systems in ten countries; the findings and recommendations are detailed below.

Governments and institutions across the world are increasingly adopting digital-ID systems to rationalise authentication, service delivery, and governance. A corresponding need has emerged for robust frameworks to evaluate the legitimacy, inclusiveness, and human rights compatibility of these systems. This report uses the *Framework for Evaluation of Digital Identity* developed by the Centre for Internet and Society (CIS) in India (Bhandari, Trikanad and Sinha 2020). This report applies the CIS framework as its primary analytical tool to assess the emerging digital-ID systems across the African continent.

Methodologically, the study also builds on the work of Research ICT Africa (RIA), which in 2020 used the CIS framework to produce ten country case studies from Africa (van der Spruy *et al*. 2020). Nine of their case study countries were from anglophone Africa, plus one lusophone country (Ghana, Kenya, Lesotho, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe, and Mozambique). We decided that rather than report on progress over the past five years in those same countries, we would provide ten additional case studies from regions in Africa that are under-represented in the existing literature. This led us to select countries from francophone West and Central Africa, and Arabic-speaking North Africa, as well as neglected cases from anglophone, East, and Southern Africa (Botswana, Côte d'Ivoire, Democratic Republic of the Congo, Egypt, Ethiopia, Liberia, Malawi, Namibia, Senegal, and Tunisia). Our aim in doing so was to provide knowledge about a wider and more representative range of case studies on which future research and analysis can be built.

Prompted by Breckenridge (2005) and Browne (2015) we aimed to trace the colonial roots of ID systems, but included Egypt, Ethiopia, and Liberia as counter-examples of countries that were never formally colonised. Our country selection was also influenced by the desire to

include countries of diverse size and political settlement, and the final choice was tempered by the availability of scholars with expertise who were able to join the research team. This report forms the first of two phases of our research, and we will now use this data to conduct more in-depth analysis of the drivers, dynamics, and direction of digital-ID in Africa, which will be shared in our forthcoming collected edition book.

This study contributes novel insights by confirming that while digital-ID systems are promoted for legitimate purposes such as fraud prevention and service delivery, their governance frequently falls short of necessity and proportionality principles that are foundational to human rights-based approaches. The term 'rights based', which is used extensively in this publication, refers to implementation or evaluation approaches that measure the extent to which a programme or policy positively or negatively affects people's ability to exercise the fundamental human rights agreed on in relevant conventions and legislation. The report reveals a widespread pattern where legal frameworks exist in theory but are weak or absent in enforcement, oversight, and transparency, leading to mission creep and expanded surveillance without adequate accountability. By integrating the CIS framework with detailed historical and contextual analysis, the report makes a unique contribution that moves beyond technical or policy narratives to critically interrogate the colonial, political, and neoliberal dimensions shaping digital-ID adoption in Africa. It underscores the urgent need for holistic, risk-aware, and rights-respecting governance frameworks that incorporate independent oversight, stakeholder engagement, and enforceable legal protections to safeguard citizens' rights and build trust in digital-ID systems across the continent.

The study has produced new evidence to highlight the growing sophistication of African legislative and implementation frameworks for digital-ID. It is clear from the country reports that dedicated digital-ID and data protection laws provide an essential foundation to ID systems that deliver benefits and avoid rights violations. It is also clear that such legislation is necessary but insufficient; translating legal provisions into tangible benefits also requires that adequate resources and expertise are dedicated to independent oversight and redress mechanisms to correct mistakes and errors that inevitably occur and demand prompt and adequate attention. The drivers of digital-ID have so far been driven top-down from government, and accelerated by the interests of external donors and technology vendors. To ensure that no one is left behind and that the benefits of digital-ID are shared equitably, it will be necessary to devise methods of consultation and participation that ensure that the drivers moving forwards are the interests, rights, and freedoms of all Africans, including those most directly at risk of

exclusion and disadvantage from biometric digital-ID systems. Only then can digital-ID systems evolve into tools of empowerment rather than control.

The remaining sections of this report are organised as follows: we begin with a review of the research on digital-ID in Africa that was conducted by CIS and RIA in 2020, which directly informs the country selection and assessment framework adopted in this research. The literature review will also address definitional issues such as those around 'identity' and 'identification'. This will be followed by our synthesis of the findings and recommendations contained in the ten country reports. Following our conclusions and short bibliography, the reader will then find all ten country reports included here in full. Each country case study begins by providing the reader with a historical account of ID systems in that country, plotting the key milestones in ID legislation, and the introduction of digital-ID and biometric ID. Fifteen tests are then applied to evaluate the current state of play and produce clear actionable recommendations. As editors, we note the need for researchers to balance critique with constructive policy guidance. Hence, this report adopts a critical and constructive approach, acknowledging that digital-ID may be beneficial when it respects rights and is inclusive, and can be problematic when policy or implementation gaps exist.

2. Background to the country reports

2.1 Research approach

This study uses the *Framework for Evaluation of Digital Identity* designed by the CIS to assess digital-ID systems in India (Bhandari *et al*. 2020). The CIS framework is built around three evaluative tests: rule of law tests, rights-based tests, and risk-based tests.

Rule of law tests evaluate whether a country's digital-ID system is grounded in a clear legislative framework that provides accountability. Questions in this group of tests include whether the rollout of the digital-ID system is backed by a validly enacted law that has a clearly defined purpose – to avoid mission creep – and whether the law clearly defines the rights and duties of key public and private actors. The rule of law tests also check whether the law provides sufficient accountability measures to regulate grievances and provide redress mechanisms.

Rights-based tests assess whether a digital-ID system impacts on fundamental human rights. Most African countries are signatories to the Universal Declaration of Human Rights and the African Charter on Human and Peoples' Rights. The tests assess whether a country's legislation includes data minimisation, access controls, and protections against exclusion from accessing basic entitlements that all people are entitled to in human rights law.

Risk-based tests evaluate whether adequate risk assessment is conducted as part of the design, policymaking, or ongoing assessment of digital-ID systems. The tests assess whether risk mitigation measures are put in place and adequately resourced. The tests also check that risk assessment and response are differentiated and proportionate, as stricter oversights and safeguards are necessary in the case of high-risk applications such as biometric ID.

The CIS framework also foregrounds the concept of mission creep – the expansion of ID systems beyond their original purpose without adequate legal or ethical checks. This is especially relevant in contexts where digital-ID systems, initially introduced for welfare delivery, have expanded to law enforcement or private sector uses (e.g. telecoms or banking), as seen in digital-ID systems in India and Nigeria. Despite its significant strengths, the CIS framework reflects some limitations in scope that affect its universal applicability, particularly in francophone, lusophone, and Arabic-speaking African countries. The framework does not fully address how

historical legacies have influenced current digital-ID policies. Countries such as Senegal inherited top-down, security-focused ID systems from French colonial rule, with minimal input from civil society. As highlighted by Masiero (2023), these systems often prioritise state surveillance and demographic control over citizen empowerment or inclusive development. By grounding the CIS framework in the specific historical context of each country in this phase of the research – and by using it alongside primary research in the second phase – we aim to extend its applicability and to show that an adapted CIS framework holds great promise as a foundation for inclusive, accountable digital-ID policy worldwide. Most published research on digital-ID has had a technical focus and has paid insufficient attention to the historical context of identification. In Africa, Donovan (2015) is a counter-example. Our study will contribute to addressing this gap in the existing research by prefacing each case study with a historical account of identification prior to the digital age.

2.2 Definitional issues in digital-ID

This section aims to clarify the use of some of the terminology used throughout this report.

Identity and identification

Identity includes the attributes, relationships, affiliations, and characteristics that define an individual, entity, or group. A person's 'identity' refers to their subjective sense of who they are, whereas 'identification' is an objective process used by institutions to verify that you are who you say you are (Harari 2018). This is traditionally accomplished through personal testimony or paper documentation such as a birth certificate (an ID document). Digital-ID replaces paper ID with machine-readable information in a barcode or microchip on a plastic or composite ID card. ID data held on a card can include biometric information such as electronic scans of a person's fingerprints, face, iris, etc. Different types of ID are explored below.

Foundational ID and functional ID

Foundational ID aims to provide a general legal ID, affording the opportunity to access multiple services or rights. It provides broad identity access; examples include birth certificates and national ID cards. Functional ID is designed with specificity in mind, serving a single pre-identified purpose such as accessing health care, using financial services, voting, etc. Examples of functional ID include voter cards, driver's licences, and international passports. Tensions arise when a functional ID becomes *de facto* a foundational ID, such as when mobile (cell) phone SIM-card

registration is used as proof of identity. Ideally, functional ID derives its legitimacy from the foundational ID that identifies the entity that holds it.

Analogue ID and digital-ID

Analogue ID includes traditional, paper-based systems – usually stored locally (e.g. paper birth records, paper-based school registration records). In contrast, digital-ID relies on electronically stored and managed identity data, which could be biometric. Analogue ID and digital-ID differ in terms of format, data, use, and risks. While analogue ID is physical or paper based, digital-ID is stored in electronic format; analogue ID uses minimal data printed on a document or card, but digital-ID can hold larger amounts of data, including biometric data that can verify each body; use of analogue ID is relatively limited in scope as each ID must be read manually, whereas digital-ID is machine readable and can potentially be integrated into any digital system for automated processing. While the main risk with an analogue ID is that it could be lost (or stolen) or copied, digital-ID exposes the bearer to new forms of risk as a central component of automated mass surveillance, profiling, targeting, discrimination, and exclusion.

Biometric authentication and verification

Biometrics include facial recognition, fingerprints, iris scans, and voice patterns, which are used to identify individuals uniquely. In a sense, they are biological signatures that distinguish between individuals based on their distinct nature, regardless of the relationship between those individuals. Authentication is the process of confirming that an individual is the person they claim to be. Increasingly, this is used to determine who should have access to services or entitlements. For example, fingerprint or iris scans are used during voting exercises to confirm that a registered voter is the person claiming to have access to that service in the particular polling area. The same system can be used to automatically determine who to send social protection payments to or who to employ.

2.3 Challenges introduced by digital-ID

The use of biometric digital-ID introduces new challenges and risks. These include risks to privacy caused by data leakage or sharing, and risks of exclusion due to poor data quality or mismatches, which could happen with manual labourers, children, older people, or pregnant women (Jain 2004). In many countries, minority ethnic groups are systematically denied registration into digital-ID systems (Mutung'u 2022; Masiero 2023). There are also privacy risks involved due to the permanent

nature of biometrics, hence the need to raise awareness and to ensure informed consent and implementation of data protection principles.

Digital-ID systems are not neutral because they are built by people who have (conscious or unconscious) biases and interests. As a result, the systems they build reflect, reproduce, and sometimes amplify existing power dynamics. This study uses a critical lens, influenced by technology and politics, that views ID systems as inevitably shaped by colonial legacies of control and exclusion, state-building and bureaucratic rationality, and contemporary neoliberal and donor-driven priorities of digital governance. The study explores identity as a site of power and resistance, and explores public–private partnerships and their governance implications, including the influence of multilateral institutions that play a role in the promotion of digital-ID systems.

3. Findings and analysis

Historical context of digital-ID

Our findings begin with what we learned from researchers as they documented the historical forms of paper-based ID that preceded digital-ID.

In seven of the ten countries studied, ID systems were first introduced by colonial powers. Of Africa's 55 nations, only Egypt, Ethiopia, and Liberia were never formally colonised. In the other cases studied, today's digital-ID systems evolved from systems imposed by colonial powers to legally codify the racial hierarchy that colonialism imposed, by distinguishing between citizens and subjects (Kwet 2023). When for example the protectorate administration in Botswana introduced travel and residence documentation for Europeans and British subjects, it implemented pass systems and required labour registration for indigenous *Batswana*. Similar to neighbouring South Africa, Nyasaland (now Malawi) had no official civil ID system but African workers were subject to 'pass laws' designed to control workers' mobility and enable tax collection. The fact that legal identification was introduced as a mechanism of colonial oppression and exploitation is often omitted from technical accounts of ID systems and resistance to their adoption.

The country report on Côte d'Ivoire in this publication shows that in 1904 the *indigénat* ID system was introduced across French West Africa. The system ranked people based on their race, creating a hierarchy of citizenship and rights. This was followed in 1908 by the *livret d'identité*, or passbook, a form of ID that was used to restrict the mobility of Africans. The Senegal country report in this publication documents that some urban Senegalese who lived in Saint-Louis, Gorée, Rufisque, and Dakar were granted French citizenship status in 1916 adding another division to the hierarchy of citizenship and rights.

Liberia, founded by freed African Americans, did not experience colonisation and this influenced the evolution of the country's ID systems. The earliest ID documents were land deeds and citizenship papers made available to repatriated freed slaves, serving as proof of settlement and land ownership. Ethiopia, a country that was not colonised but was briefly occupied by Italy for five years from 1936, had no colonial ID system but allowed local administration to provide foundational IDs and regional identity cards called *kebele* ID, named after the local description for the country's lowest administrative units.

It is clear from the ten country case studies that a country's political history has often been a key determinant of the forms of ID imposed

and the interests that they serve. As pressure mounts to adopt biometric digital-ID across Africa, it is important that a critical analysis is made of what interests are driving this change and who benefits.

4. Rule of law tests

This section presents findings from the first of the 15 tests from the CIS framework.

4.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

A foundational element of the rule of law is that state actions, especially those that impact fundamental rights, must be grounded in legislation enacted by a legitimate authority. In the context of digital-ID systems, this means that such initiatives must be supported by validly enacted laws that provide a clear legal basis and also avoid excessive delegation of power to the executive. Our researchers reviewed the legal mandates underpinning digital-ID projects to reveal varying degrees of legislative clarity, constitutional alignment, and procedural safeguards.

The country reports on Botswana, Malawi, and Namibia identified relatively strong statutory backing for their digital-ID systems. Botswana's framework is anchored in the National Registration Act of 1986, mandating ID registration from age 16. Namibia passed a comprehensive Civil Registration and Identification law in 2024, consolidating and modernising earlier laws. Malawi's system is grounded in the National Registration Act of 2010, which established a national infrastructure for digital-ID. Ethiopia's 2025 Digital Identification Proclamation and a 2024 personal data protection law position it among countries with more recent and comprehensive legal frameworks. In contrast, Côte d'Ivoire and DRC rely on decrees or older statutes, raising questions about legislative oversight and sustainability.

While most countries examined have introduced laws or decrees to support their digital-ID programmes, the quality and origin of these legal instruments vary significantly. One key finding is that a clear parliamentary mandate – such as those seen in Botswana, Ethiopia, Malawi, and Namibia – correlates with more transparent and structured ID systems. These countries tend to have specific legislation addressing digital-ID, often accompanied by data protection laws that define biometric data collection and use. This suggests a growing legislative recognition of privacy rights in digital governance. On the other hand, countries such as Côte d'Ivoire and DRC exemplify a trend where executive orders or outdated legislation are used to justify expansive ID programmes. This raises concerns about the democratic legitimacy and oversight of such systems. The study highlights how reliance on non-

parliamentary instruments could undermine accountability and weaken safeguards against abuse, especially where biometric data is involved.

In these findings, we see emerging divergence in how digital-ID systems are being legislated across Africa. While earlier literature has broadly categorised African digital-ID projects as under-regulated or driven by donors' agendas, this study reveals a more complex and dynamic legal landscape. However, this progress is uneven, and without region-wide standards or enforcement mechanisms, disparities may deepen digital inequality and erode trust in public institutions.

4.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Across the ten country reports, most digital-ID laws articulate legitimate aims aligned with governance, service delivery, and national security. However, the clarity and specificity of these aims vary, with some legal frameworks offering broad or implied justifications rather than clearly defined purposes. The Botswana country report shows that the Omang digital-ID system is anchored in public interest goals such as improved service delivery, national security, and administrative efficiency. The government provides a policy-based justification for digital-ID, with aims ranging from socioeconomic development to the digitisation of public services. These policy documents articulate a coherent link between digital-ID and development objectives.

The Namibia country report documents that the government has established a legal framework for digital-ID through the Civil Registration and Identification Act, 2024, but the law is vague about legitimate use beyond core ID functions and omits a public interest rationale. Côte d'Ivoire stands out for explicitly linking its digital-ID system to fraud prevention, service delivery, and efficiency – aligning with international norms – but risks legislative overreach due to excessive executive discretion. Ethiopia presents one of the clearest articulations of digital-ID objectives – legal identity, access to rights, and development – but still lacks clarity on the specific sectors or services.

This study reveals that while many African countries acknowledge legitimate aims in their digital-ID laws, there is significant variation in how clearly these aims are defined and safeguarded. The most compelling insight is the rarity of legally grounded, human-rights-aligned justifications for digital-ID deployment. Countries such as Botswana, Côte d'Ivoire, and Ethiopia demonstrate a more deliberate alignment with public interest goals, highlighting a promising but limited trend. In contrast, Egypt and Namibia

exemplify a pattern where legal frameworks either lack specificity or rely too heavily on executive orders, raising risks of 'function creep', misuse, or erosion of legal certainty. The term function creep refers to the gradual expansion of a system's application beyond its originally claimed purpose.

This confirms concerns in the existing literature about the fragility of legal safeguards in digital-ID ecosystems across the continent. However, it also contradicts assumptions that African states uniformly fail to articulate purpose: some do, and do so well. Moreover, the analysis adds nuance by showing that even where purpose is clearly stated, sectoral applicability is often undefined, potentially undermining both efficacy and accountability. The study contributes novel insights by emphasising that clarity in legitimate aims is not just a legal formality but a necessary foundation for trust, oversight, and protection against overreach – a gap that must be addressed to ensure that digital-ID systems in Africa support inclusion rather than entrench exclusion or abuse.

4.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

Clear definitions of who may access or use digital-ID data, what data can be collected, and the rights of individuals regarding their data are essential to protecting privacy and preventing misuse. Effective legal frameworks provide transparent rules about the permitted actors, including government agencies, private sector partners, or third parties, and specify the purposes for which digital-ID data may be accessed or shared. They also define the scope and type of data collected and, crucially, guarantee individuals' rights to access their data, correct inaccuracies, confirm data-processing activities, and opt out when appropriate.

As the country reports from Botswana, Malawi, and Namibia show, these countries share legal frameworks that authorise state use of digital-ID systems but offer limited citizen rights, and lack clear limitations on which actors may access sensitive personal and biometric data. In contrast, Côte d'Ivoire and Senegal provide stronger legal protections, explicitly defining authorised actors and granting individuals rights to access, correct, and control their data – though gaps remain in implementation. DRC and Liberia, however, illustrate weak regulatory clarity and minimal individual data rights, exposing citizens to significant risks of misuse and opacity.

This study reveals important divergences and emerging trends in Africa's digital-ID legal landscape. A key contribution has been made by the growth of legal sophistication in some countries – such as Ethiopia and Tunisia – that balance administrative efficiency with privacy, offering clearer protections and limiting data collection to necessary purposes. This challenges the prevailing literature that paints African digital-ID systems with a broad brush of weak regulation. At the same time, the persistence of vague legal mandates and minimal user rights in several countries confirms concerns about state overreach and the absence of data subject empowerment. Notably, our findings highlight that even where legal provisions exist, enforcement and practical implementation often lag behind, suggesting a gap between legislative intent and lived experience. This study underscores the need for harmonised regional standards and more nuanced assessments of digital-ID laws that go beyond legal texts to evaluate actual protections for individuals.

4.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

Effective redress mechanisms are critical to uphold individuals' rights in digital-ID systems, ensuring accountability for misuse or mishandling of personal data. This summary examines the legal frameworks across ten African countries, as described in each country report, and focuses on whether laws provide clear avenues for complaint, investigation, remedy, and sanctions related to digital-ID data use. While some countries demonstrate robust institutional structures and judicial remedies, others reveal significant gaps that expose users to risks without sufficient protection or recourse.

As detailed in the respective country reports, Botswana and Senegal stand out for providing relatively strong redress mechanisms for digital-ID systems. Botswana's legal framework includes timely notification of breaches of privacy, rights to correction and deletion, and multiple avenues for complaint resolution. Senegal's active data protection authority enforces compliance, and has a track record of processing complaints and issuing sanctions. In contrast, Malawi and Namibia exhibit significant shortcomings, including weak or unimplemented data protection laws and no clear redress processes. Côte d'Ivoire offers multiple legal channels but lacks user notification and struggles with enforcement capacity. Tunisia's framework includes rights to access and correction but lacks real-time data breach notifications and enforceable grievance procedures, limiting user accountability protections.

This study makes a significant contribution to the literature on digital-ID in Africa by moving beyond legal formality to assess the real-world implications of redress mechanisms. First, it challenges the assumption that African states uniformly lack redress provisions by highlighting functioning systems in the country reports on Botswana and Senegal, which combine administrative and judicial pathways. Second, it reveals how the mere existence of legal avenues – as in Côte d'Ivoire and Ethiopia – does not guarantee effective recourse when enforcement is weak or underfunded. Third, the analysis underscores that some countries, such as Egypt, lean heavily on criminal sanctions without offering accessible civil or administrative remedies, creating imbalanced systems of accountability. Finally, the findings illuminate a widespread issue: most legal frameworks do not adequately prioritise user notification or proactive transparency, essential elements for meaningful redress. By synthesising legal texts, institutional structures, and enforcement trends, this study provides a nuanced understanding of where gaps remain in redress mechanisms and what is needed to prioritise reform, particularly the need for harmonised standards, resource-backed independent oversight, and user-centred accountability to secure public trust in Africa's evolving digital-ID systems.

4.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

Accountability is a critical pillar for the legitimacy, trust, and proper functioning of digital-ID systems. It ensures that administrators of digital-ID systems are answerable to independent and effective regulatory mechanisms, which enforce compliance, protect data subjects, and address grievances. Across the country reports in this study, the level of regulatory independence, clarity of accountability frameworks, and enforcement mechanisms vary widely, affecting the extent to which digital-ID systems are transparent and inclusive, and respect rights.

Botswana offers one of the strongest accountability frameworks, combining its National Registration and Data Protection Acts with active judicial oversight and a designated regulatory body, though questions remain about the Data Protection Commission's independence and resourcing. By contrast, Namibia and Malawi lack fully operational accountability systems; Namibia's legislative delays and Malawi's absence of independent oversight leave digital-ID use largely unchecked. Côte d'Ivoire has strong legal provisions on paper – including criminal penalties and fines – but enforcement remains weak, and high ID access costs limit engagement with accountability processes. Senegal's digital-ID system is vulnerable to state surveillance

and political misuse due to weak parliamentary and administrative controls, while DRC and Liberia both lack independent regulators, resulting in minimal safeguards against misuse, and limited public trust.

This study offers new and compelling insights that both confirm and challenge prevailing assumptions in the literature on digital-ID governance in Africa. It confirms earlier concerns about the widespread lack of independent oversight and under-resourced regulators, which persist in countries such as Liberia, Malawi, and Namibia. However, the study challenges the notion of uniform regulatory weakness by showing that Botswana has developed a functional model of institutional accountability, combining legal provisions with judicial enforcement. It also reveals that even where legal penalties exist, as in Côte d'Ivoire and Ethiopia, enforcement is often symbolic due to operational or political constraints.

A novel contribution lies in highlighting how intra-country divergence – such as Tunisia's contrast between its underdeveloped biometric ID governance and its stronger Mobile ID governance – illustrates that accountability is not only a function of national legal frameworks but also of how oversight is distributed across systems and actors. Furthermore, this study underscores the overlooked impact of high entry barriers – such as ID acquisition costs – on the practical accessibility of accountability mechanisms. Ultimately, the analysis affirms that building trust in digital-ID systems in Africa requires more than legal texts: it demands independent regulators, enforceable oversight, user empowerment, and systemic transparency grounded in both law and practice.

4.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

Given the personal and sensitive nature of data collected in biometric digital-ID systems, it is important that the use of digital-ID is restricted to its legitimate aim to avoid it being used beyond its originally intended functions to serve other interests. The country reports reveal varying levels of clarity concerning limitations on the use of digital-ID, as well as the safeguards against mission creep. While some countries have clearly defined the scope of digital-ID use within their governing laws or data protection frameworks, most systems exhibit legal or practical gaps that make them vulnerable to function creep.

The Botswana country report clearly highlights the danger of mission creep. The Omang digital-ID system that was initially designed for citizen ID has subsequently become necessary for SIM-card registration and

voter verification, without adequate oversight or safeguards. Namibia's underdeveloped legislative framework and lack of a functional data protection regime leave it similarly exposed, with no clear restrictions on expanded ID uses. In Côte d'Ivoire, while the law articulates governance and service delivery as objectives, digital-ID is now used in migration control and visa processes, reflecting externally driven expansions unsupported by domestic legal or regulatory structures. Liberia's system has also expanded through executive orders beyond its initial legislative scope, highlighting a critical need for legal clarity and independent oversight to prevent unchecked extension of digital-ID functions.

This study reveals a troubling and largely under-addressed trend of mission creep across African digital-ID systems, confirming prior concerns in existing literature and offering novel insights into how this phenomenon is evolving on the ground. While previous research has acknowledged the dangers of function creep, our findings highlight that many governments lack even the most basic legal tools or institutional frameworks to identify, monitor, or counteract this expansion. More importantly, we observe that development partners' influence, and executive orders, play a significant yet poorly scrutinised role in expanding digital-ID functions. Tunisia's example underscores how transparency and public consultation remain elusive, even in states with relatively advanced legal ecosystems.

The Egypt and Ethiopia country reports provide examples of the shift from optional to functionally mandatory use of digital-ID across a range of essential public services, without clear legal mandates. This suggests that mission creep is not only a technical or administrative risk but also a structural and democratic one, undermining user consent and eroding civic agency. The lack of robust judicial or parliamentary oversight across the board reveals a gap between formal legal principles – such as purpose limitation – and their operational enforcement. Overall, this study contributes new empirical evidence to the literature by showing that unchecked expansion is a widespread and growing reality, calling for urgent reforms to safeguard rights and restore accountability in digital-ID ecosystems.

5. Rights-based tests

This section presents findings from the second five tests from the CIS framework.

5.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

A core principle in human rights-based approaches to digital-ID is the requirement that any privacy-infringing measure must be both necessary and proportionate to achieving a legitimate aim. In evaluating digital-ID systems, this principle helps determine whether the collection, use, and retention of personal data can be justified in democratic societies.

The country reports from Botswana, Malawi, and Namibia reveal key challenges in digital-ID systems. Botswana's heavy reliance on biometrics raises serious privacy concerns due to limited evidence that less intrusive alternatives were considered, despite constitutional protections. Malawi's extensive biometric data collection proceeds amid weak legal frameworks and political concerns, underscoring the absence of clear limits on data use and effective oversight. Namibia's lack of data protection laws creates a legal vacuum, increasing risks of unauthorised data use without safeguards. Elsewhere, Egypt's inclusion of sensitive attributes such as people's religion and profession in ID data violates proportionality standards, risking exclusion, and discrimination. Tunisia, while embedding principles of necessity and consent, suffers from excessive data collection and weak enforcement, raising doubts about actual privacy protections.

This study contributes new and compelling insights that both confirm and deepen existing critiques in the literature on digital-ID systems in Africa. While prior research has highlighted risks related to privacy and data protection, our findings demonstrate that many governments continue to implement biometric-heavy systems without adequately justifying their necessity or exploring less intrusive alternatives, revealing a systemic disconnect between legal principles and operational realities. The inclusion of sensitive personal attributes – such as religion in Egypt – exposes novel forms of exclusion and discrimination that have been underexplored in past analyses. Furthermore, the study uncovers a pervasive weakness in enforcement mechanisms and oversight authorities, which remain largely powerless or under-resourced to uphold proportionality standards. This gap points to a structural failure that perpetuates excessive data

collection and retention despite formal commitments to privacy, challenging assumptions that policy existence equates to effective protection. Notably, our findings reveal that even where consent is nominally required, practical enforcement is lacking, thus eroding genuine user agency. These insights underscore the urgent need for African states to adopt stricter legal safeguards, transparent data governance, and empowered independent oversight bodies to realign digital-ID implementation with human rights norms and rebuild public trust in these critical ID infrastructures.

5.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

Data minimisation is a fundamental principle in data protection, aiming to ensure that personal data collected, used, and retained is limited to what is strictly necessary for specific purposes. However, in practice, the application of this principle varies across countries, with many facing challenges in aligning their legal frameworks with data protection best practices. This summary examines the adherence to the principle of data minimisation in the collection, use, and retention of personal data across the ten countries, highlighting both the legal frameworks in place and the gaps or inconsistencies in their implementation.

Botswana, Malawi, and Namibia present distinct illustrations of how digital-ID systems challenge the principle of data minimisation. Botswana's legal framework incorporates minimisation and storage limitation, but the mandatory collection of biometric data – especially for SIM card registration – raises concerns about proportionality and necessity. Malawi's Data Protection Act is in place, but the enforcement is nascent, with concerns over the digital-ID system's use in politically sensitive areas and limited oversight, heightening the risk of data misuse. Namibia's new Civil Registration and Identification Act, 2024 introduces governance measures, yet the decade-long delay in passing the Data Protection Bill has left significant gaps, enabling the potential repurposing of digital-ID data – for activities such as voter and SIM card registration – without clear limits.

This study reveals a disconnect between formal recognition of data minimisation and actual practice across African digital-ID systems. It confirms some earlier critiques in the literature about weak implementation, but adds new depth by identifying the mechanisms through which data protection principles are undermined – particularly through legal exemptions for national security, ambiguous or absent data retention schedules, and political repurposing of ID systems. Contrary to policy rhetoric that

digital-IDs are tools for inclusion and service delivery, their design often enables surveillance, unchecked data expansion, and rights violations.

This synthesis highlights how vague legal language, insufficiently empowered regulators, and fragmented oversight structures not only erode public trust but also facilitate the normalisation of expansive, intrusive data practices. Addressing these issues requires more than just passing laws – it demands operational clarity, independent enforcement, and a fundamental rethinking of what data is genuinely necessary for identification.

5.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

Access control is a critical aspect of digital-ID systems, ensuring that only authorised entities can access or use personally identifiable information (PII). Effective access control measures protect individuals' privacy, prevent unauthorised data sharing, and safeguard sensitive information from misuse. This summary evaluates the protections in place to limit access to the digital trail of PII in Botswana, Côte d'Ivoire, DRC, Egypt, Ethiopia, Liberia, Malawi, Namibia, Senegal, and Tunisia.

The country reports from Côte d'Ivoire, Egypt, and Senegal illustrate particularly concerning trends in access controls for digital-ID systems. In Côte d'Ivoire, while access controls are legally mandated, vague exemptions for 'public interest' and weak enforcement – especially within government agencies – undermine these protections. In Egypt, broad, unchecked access is granted to various government entities under the Civil Status Law, with the Secured and Smart Documents Complex holding sensitive biometric data beyond the scope of national data protection laws – raising major concerns about transparency and accountability. Senegal permits extensive data sharing between public and private actors, including telecoms companies and banks, without adequate authorisation or oversight, and external actors such the European Union reportedly use biometric data for migration control.

While earlier research has acknowledged the lack of data protection laws, and the need for consent-based frameworks, our findings reveal a deeper, structural issue: even where laws exist, they often contain broad exemptions, lack clarity on implementation, or exclude critical institutions from their scope. The case of Egypt, where the primary ID-issuing bodies are not covered by data protection regulations, challenges the assumption that a single national data protection law ensures comprehensive safeguards. In countries such as Côte d'Ivoire and Senegal, we see that the justification

of 'public interest' is not only poorly defined but can be exploited to bypass essential oversight mechanisms. This cross-country analysis also draws attention to the underexplored issue of third-party and international access – in particular, how external actors can gain access to national biometric databases, often without public knowledge or consent. These findings not only confirm long-standing concerns about weak legal safeguards but also surface new dimensions – such as geopolitical and commercial data flows – that require urgent attention in discussions about digital-ID systems in Africa. Ultimately, the study highlights the urgent need for precise legal definitions, enforceable limitations, and independent oversight as foundational pillars for any rights-respecting digital-ID system.

5.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Across Africa, the shift towards digital-ID systems has raised concerns about inclusion, particularly for vulnerable populations. While digital-ID promises improved service delivery and efficiency, several countries face persistent challenges in ensuring equitable access and mitigating the risk of exclusion from essential services.

The Botswana, Egypt, and Malawi country reports illustrate distinct exclusion risks within digital-ID systems. In Botswana, reliance on the physical Omang card poses growing risks of exclusion in a digitalising environment, particularly for undocumented or marginalised populations. Egypt's national ID system severely disadvantages marginalised groups – including refugees, Bedouins, and gender-diverse individuals – through systemic barriers such as inaccessibility, religious and gender-based discrimination, and limited redress mechanisms. Malawi's mandatory ID system, combined with weak fallback provisions, has already resulted in exclusion from mobile services and public programmes, especially for those lacking documentation.

The synthesis of findings reveals a striking contradiction between the inclusive rhetoric of digital-ID systems and their exclusionary realities across Africa. While much of the existing literature focuses on the potential of digital-ID to expand access to services, this study highlights a widespread absence of safeguards for those most likely to be left behind. New and compelling evidence from countries such as Egypt and Malawi confirms that without robust legal protections, alternative access mechanisms, and inclusive design, digital-ID systems risk becoming tools of exclusion rather than empowerment. Furthermore, the lack of effective redress processes and accountability structures means that those excluded often have no recourse,

compounding existing inequalities. This research contributes a novel perspective by centring the lived realities of vulnerable populations and offering empirical evidence that challenges optimistic assumptions in current policy discourse. It underscores the urgent need for governments to rethink the design and implementation of digital-ID systems through a rights-based, inclusive lens – prioritising accessibility, flexibility, and legal redress.

5.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

Across the ten countries studied, legal frameworks have increasingly leaned towards mandating enrolment and use of digital-ID systems. This trend reflects governments' interest in establishing centralised, secure, and interoperable ID infrastructures to facilitate access to services, verify citizenship, and support national security and development agendas. However, while these justifications may be valid in principle, the implementation of mandatory digital-ID systems raises critical questions about inclusivity, legal proportionality, and the availability of alternative mechanisms for those who may be excluded.

Côte d'Ivoire, DRC, and Senegal illustrate how mandatory digital-ID enrolment is deeply embedded in law and practice. In Côte d'Ivoire, enrolment is compulsory from age 16, and the ID is linked to voting, health care, and even newborn registration, hence positioning digital-ID as central to civic and social life but raising concerns about fairness where infrastructure is lacking. In DRC, recent legal instruments make enrolment mandatory from age 18, framing the digital-ID system as definitive proof of citizenship, thereby creating a high-stakes environment where lack of ID may equate to lack of legal recognition. Senegal's biometric ID card is mandated from age 15, and its issuance from as early as age five suggests an early and far-reaching integration into the digital-ID ecosystem.

This study shows that while laws across several African countries provide a strong mandate for digital-ID enrolment, this legal certainty often overshadows more critical questions of equity, access, and rights protection. A compelling insight is the legal overreach of digital-ID mandates without corresponding safeguards – a gap that the existing literature acknowledges, but which this research illustrates through granular, country-level evidence. Contrary to the assumption that legal mandates inherently drive inclusion, findings suggest that mandatory systems, especially those linked to multiple essential services, can entrench exclusion where access pathways are limited or digital infrastructure is uneven. The study

contributes a nuanced understanding of how mandatory enrolment, when not counterbalanced by alternatives and oversight, can transform digital-ID systems into instruments of conditional citizenship, thereby challenging prevailing narratives that equate digitisation with automatic inclusion.

6. Risk-based tests

This section presents findings from the final four tests from the CIS framework.

6.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

Risk assessment is critical to ensuring that digital-ID systems do not infringe on individuals' rights and that their uses are legitimate, proportionate, and beneficial. While some African countries have taken initial steps towards integrating risk-based approaches, most systems still lack comprehensive, transparent, and participatory assessments that inform digital-ID design and deployment.

The country reports from Ethiopia, Liberia, and Senegal illustrate the fragmented approach to risk assessment in digital-ID implementation. Ethiopia has undertaken preliminary risk assessments through environmental and social screening guidelines, identifying threats such as privacy violations and social exclusion, yet inclusive consultation and actual implementation of safeguards are unclear. Liberia lacks any legal mandate for recurring risk assessments, leaving its population – especially in a fragile, low-literacy context – exposed to unmitigated harms such as surveillance and exclusion. Senegal's digital transformation strategy references feasibility and baseline studies, but no formal risk assessment process preceded the rollout of its digital-ID system, and a World Bank-commissioned report remains unpublished.

In this study, we found that the lack of structured, legally mandated risk assessments is a critical blind spot in most African digital-ID systems. Even where policy commitments exist, implementation is often inconsistent, non-transparent, or altogether absent, and accountability mechanisms are weak. The findings confirm the conclusions of existing literature on risks such as exclusion and surveillance, but go further by exposing how inaction or incomplete follow-through on risk assessments entrenches these dangers within digital governance frameworks. The study also highlights that international actors, such as donors, may initiate assessments that are neither public nor participatory, as seen in Senegal, thereby undermining their value. This underscores the urgent need to shift from fragmented and opaque practices to proactive, inclusive, and enforceable accountability mechanisms that can ensure digital-ID systems genuinely serve the public good without compromising rights.

6.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

As digital-ID systems expand across Africa, the question of whether laws and regulations adopt a differentiated, risk-based approach to governing their use has become critical. Such an approach ensures that higher-risk uses such as biometric ID or sensitive data processing are subject to stricter oversight and safeguards. This analysis reviews the legal frameworks of selected countries in the report in relation to their recognition and management of digital-ID-related risks.

DRC, Egypt, and Tunisia illustrate the varied and critical gaps in risk-based governance of digital-ID systems across Africa. In DRC, no specific information was reported, which itself points to a lack of transparency and regulatory clarity. Egypt stands out with a relatively strong data protection law that includes explicit consent, breach notification, and data minimisation, yet it does not tailor these protections to the distinct risks of digital-ID use, limiting its effectiveness in addressing exclusion and surveillance. Tunisia lacks a differentiated governance framework entirely; while there are grievance mechanisms and a focus on data integrity, there is no requirement for consent or alternative identity verification to prevent exclusion, and no tiered safeguards to mitigate risk across different use cases.

The report findings reveal that, while digital-ID systems are advancing rapidly in Africa, regulatory frameworks remain largely undifferentiated and unresponsive to the varying degrees of risk that different applications pose. This study surfaces three compelling insights. First, the presence of comprehensive data protection laws alone does not guarantee adequate safeguards – without specific application to digital-ID, even robust legislation such as Egypt's can fall short. Second, the complete absence of risk-tiered protections in countries such as Tunisia illustrates how exclusionary or coercive practices can take root even under formal legal regimes. Third, the lack of transparency or available information in jurisdictions such as DRC underscores a deeper accountability crisis, where both citizens and researchers face difficulty in assessing the risk environment. These findings challenge the assumption that the adoption of data protection laws automatically translates to effective digital-ID governance, revealing instead that targeted, contextual implementation and independent oversight are essential for protecting rights and fostering trust.

6.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

Proportionality is a key principle in human rights and digital rights governance, requiring that any measures infringing on individual rights be proportionate and the least intrusive means of achieving legitimate objectives. This principle demands a careful balancing act between the benefits of digital-ID systems and the potential risks they pose to privacy, security, inclusion, and more. Across the countries featured in the reports, the degree to which digital-ID laws and frameworks embed proportional governance varies widely, reflecting differing legal, institutional, and technical approaches to risk management.

The Botswana, Côte d'Ivoire, and Tunisia country reports illustrate important variations in how proportionality principles are applied in digital-ID governance across Africa. Botswana's 2024 Data Protection Act incorporates proportionality elements such as data minimisation and mandatory impact assessments, yet concerns about the necessity of population-wide biometric collection and limited public transparency remain. Côte d'Ivoire relies heavily on centralised biometric ID systems, justified by broad goals such as fraud reduction and economic growth, but lacks any legal consideration of proportionality or risk calibration, exposing users to potential privacy risks. Tunisia's biometric ID law exemplifies disproportionate government interference with centralised biometric data storage vulnerable to identity theft, inadequate breach notification, and no independent oversight, underscoring significant security and privacy gaps.

The synthesis of findings from this study reveals a nuanced and critical insight into digital-ID governance in Africa that advances the existing literature. While prior research has noted the general lack of robust legal safeguards and oversight, this study highlights the persistent inconsistency in and underdevelopment of proportionality as a core governance principle – an essential element to balance state security objectives with individual rights. Botswana and Egypt stand out for embedding proportionality in law, yet both demonstrate ongoing challenges in transparency and operationalisation, signaling that strong legal frameworks are necessary but insufficient to guarantee effective protections. Meanwhile, countries such as Côte d'Ivoire and Tunisia illustrate how the absence of risk-based approaches leads to potentially disproportionate and unjustified data collection practices, increasing vulnerability to misuse and rights violations. Notably, this study emphasises that proportionality must be operationalised

through enforceable mechanisms such as differentiated oversight, impact assessments, and public engagement, rather than merely stated in law. The findings call for a shift from uniform, one-size-fits-all governance towards risk-sensitive, accountable, and transparent digital-ID systems to safeguard fundamental rights and foster public trust, offering a vital framework for future legal reforms and policy development in African digital-ID ecosystems.

6.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

Digital-ID systems introduce significant risks to individuals' privacy, security, and rights, especially when biometric data and sensitive personal information are involved. A crucial question is whether national legal frameworks have established mechanisms to prohibit or restrict digital-ID uses when demonstrably high risks emerge. This synthesis reviews the responses in ten countries, evaluating the presence and effectiveness of legal tools aimed at mitigating or halting risky applications of digital-ID.

As the country reports from DRC, Egypt, and Namibia illustrate, there are significant gaps in digital-ID governance across Africa. In DRC, governance mechanisms are notably absent or underdeveloped, with limited information on risk mitigation and no targeted legal measures to address high-risk ID management practices. Egypt operates without a dedicated digital-ID law; while its general Data Protection Law promotes proportional data handling, it lacks specific provisions to categorise or restrict high-risk digital-ID applications, creating a critical legal gap. Namibia's legal framework focuses mainly on registration and lacks clear provisions to restrict or prohibit high-risk uses of digital-ID, leaving potential misuse unchecked.

The synthesis of these findings reveals that despite some progress in adopting data protection principles, most African countries' digital-ID systems fall short of effectively managing risks associated with high-impact uses. Unlike well-established global frameworks such as the European Union's General Data Protection Regulation, these countries lack adaptive governance structures, explicit legal restrictions on high-risk applications, and enforcement mechanisms to prevent their misuse. This study contributes novel insights by highlighting that risk-based regulatory approaches remain largely theoretical rather than operational, with many countries unable to translate laws into practical safeguards. The research also confirms a recurring pattern: digital-ID expansion into politically sensitive

or surveillance domains often outpaces legal protections, increasing vulnerability to rights violations. Importantly, it underscores the urgent need for holistic frameworks that combine robust risk assessment, inclusive stakeholder engagement, and enforceable restrictions to safeguard citizens' rights and build trust in digital-ID infrastructures across Africa.

7. Conclusion

Digital-ID systems in Africa emerged from colonial tools of control and post-independence mechanisms of power consolidation, and are now digitised infrastructures that increasingly serve government and corporate interests, often at the expense of rights, equity, and genuine inclusion. To understand digital-ID, we explore the definitions of identity, identification, foundational ID, functional ID, analogue ID, digital-ID, and biometric digital-ID authentication and verification. As described in the study, the location of country reports in the historical context of colonial identification makes possible an analysis of how ID systems make citizens visible and serve the interests of powerholders over workers and racialised groups. This highlights risks that repressive governments could use digital-ID to profile, discriminate against, target, and control citizens, which is why we argue that marginalised groups and human rights experts should be involved in the design, implementation, and evaluation of digital-ID systems.

Each country report in this study offers the most comprehensive and up-to-date analysis of digital-ID systems currently available. Grounding each case study in the historical evolution of identification practices helped us to move beyond narrow, technical narratives of politically 'neutral' technologies. By incorporating countries from North, East, Central, and West Africa – including francophone and Arabic-speaking contexts – this report represents the broadest geographic assessment of digital-ID on the continent to date. Building on the CIS framework first applied in the 2020 RIA study, this work expands the number of comparable country case studies from ten to 20, significantly deepening the regional evidence base and enabling a more nuanced, rights-based understanding of digital-ID in Africa.

Across the rule of law tests, the study finds that while some African countries are beginning to legislate digital-ID systems with increasing sophistication, particularly Botswana, Ethiopia, and Tunisia, the overall legal landscape remains patchy, imprecise, and inconsistent. Eight out of ten countries surveyed have no law specifically governing digital-ID, and none include differentiated protections for biometric data. Legal mandates often fail to clearly define actors, purposes, or user rights, and even where legal provisions exist, enforcement is weak or symbolic. Independent oversight bodies are rare, and judicial mechanisms to contain mission creep – where ID systems expand beyond their original scope – are mostly absent. Without stronger legislation, clearer accountability, and harmonised regional standards, digital-ID projects risk entrenching inequality and mistrust rather than delivering inclusion or security.

In response to the rights-based tests, we find that digital-ID systems often operate in ways that exceed the bounds of necessity and proportionality, with broad data collection mandates, weak consent regimes, and poor access controls. Most countries lack operational data minimisation strategies, and vague 'public interest' exemptions are routinely used to justify intrusive practices. Exclusions are a serious concern: without meaningful opt-out mechanisms or alternative access paths, mandatory enrolment often translates into denial of services for marginalised communities. Despite policy rhetoric around inclusion, the practical experience of digital-ID reveals a different story – one where many are rendered invisible or unentitled due to systemic design flaws and lack of legal recourse.

Analysis of the risk-based tests further reinforces these concerns, showing that risk assessments are rarely mandatory, public, or participatory. Legal systems generally do not differentiate governance based on the varying risks posed by digital-ID usage, and high-risk applications – such as surveillance or political profiling – are advancing without adequate safeguards. Even countries with strong data protection laws often fail to apply these frameworks specifically to digital-ID. The absence of proportionality in both law and practice enables unchecked expansion into sensitive domains, further exposing individuals to rights violations. To address these gaps, African countries must shift from rhetorical commitment to practical governance: adopting clear, enforceable protections; empowering independent regulators; and ensuring inclusive participation by those most affected. Only then can digital-ID systems evolve into tools of empowerment rather than control.

8. Bibliography

Bhandari, V.; Trikanad, S. and Sinha, A. (2020) ***Governing ID: Principles of Evaluation***, Centre for Internet and Society, Digital Identities Project (accessed 12 October 2025)

Breckenridge, K. (2005) '**The Biometric State: The Promise and Peril of Digital Government in the New South Africa**', *Journal of Southern African Studies* 31.2: 267–82 (accessed 10 November 2025)

Browne, S. (2015) *Dark Matters: On the Surveillance of Blackness*, Duke University Press

David, A. (2014) '**Identification in Ancient Egypt from the Old Kingdom to the end of the New Kingdom (2650-1100 BCE)**', in M. Depauw and S. Coussement (eds), I*dentifiers and Identification Methods in the Ancient World*, Legal Documents in Ancient Societies III, OLA 229, 57–74, Leuven: Peeters (accessed 12 October 2025)

Donovan, K.P. (2015) '**The Biometric Imaginary: Bureaucratic Technopolitics in Post-Apartheid Welfare**', *Journal of Southern African Studies* 41.4: 815–33, DOI: 10.1080/03057070.2015.1049485 (accessed 10 November 2025)

Harari, Y. (2018) *21 Lessons for the 21st Century*, New York: Spiegel & Grau

Jain, A, (2004) '**An Introduction to Biometric Recognition**', *IEEE Transactions on Circuits and Systems for Video Technology* 14.1: 4-20 (accessed 10 November 2025)

Kwet, M. (ed.) (2023) *The Cambridge Handbook of Race and Surveillance*, Cambridge: Cambridge University Press

Masiero, S. (2023) '**Digital Identity as Platform-mediated Surveillance**', *Big Data & Society* 10.1, DOI: 10.1177/20539517221135176 (accessed 12 October 2025)

Mutung'u, G. (2022) '**The United Nations Guiding Principles on Business and Human Rights, Women and Digital ID in Kenya: A Decolonial Perspective**', *Business and Human Rights Journal* 7.1: 117-133 (accessed 12 October 2025)

Van der Spruy, A.; Bhandari, V.; Trikanad, S. and Paul, Y. (2020) ***Towards the Evaluation of Socio-Digital ID Ecosystems in Africa***, Cape Town: Research ICT Africa (accessed 12 October 2025)

Digital-ID in Senegal: Country report

Mame-Penda Ba

 DOI: 10.19088/IDS.2025.055

1. Introduction

This report examines Senegal's digital identification (digital-ID) landscape, evaluating its legal framework through rule of law, rights-based, and risk-based tests. Digital-ID is increasingly critical for public administration and service delivery in Senegal, where the biometric Economic Community of West African States (ECOWAS) Biometric Identity Card (ENBIC) is mandatory for citizens aged 15 and above. Despite digitalisation ambitions and increasing digital access, the system faces significant legal, ethical, and inclusion-related challenges.

Senegal's digital-ID ecosystem is characterised by rapid biometric ID adoption and integration across sectors, including SIM card registration and banking. Key strengths include high biometric coverage, political support for digital transformation, and a formal data protection framework. However, weaknesses include outdated laws, weak oversight, and exclusion risks. Persistent legal gaps, particularly concerning facial recognition and data protection, raise serious concerns about surveillance, privacy, and exclusion, especially for vulnerable populations. The risk of data predation by external actors such as the European Union (EU) funding biometric programmes for migration control also raises sovereignty and data exploitation issues.

This report addresses the question: what is the current state of Senegal's digital-ID landscape, including its legal framework, assessed using rule of law, rights-based, and risk-based tests?

The sections that follow provide a historical overview of ID systems in Senegal, analyse the legal and institutional framework, evaluate compliance with Centre for Internet and Society (CIS) principles, and conclude with key risks, findings, and policy recommendations to support a more inclusive and rights-respecting digital-ID system.

2. History of ID in Senegal

2.1 Colonial ID systems

The French colonial administration introduced Senegal's civil registration system in the eighteenth century. Initially, civil status was reserved for French nationals but was later extended to native populations in four communes (Saint-Louis, Gorée, Rufisque, and Dakar), granting them 'French citizen' status in 1916 (Légier 2014). The majority of colonised inhabitants were excluded from legal identity. Fiscal, electoral, and military considerations drove colonial civil registration, creating inequalities between urban and rural areas. Colonial authorities prioritised civil registry offices in economically and strategically valuable territories, structurally excluding rural populations from legal identity.

The end of the *indigénat*[1] regime through the 1946 Lamine-Guèye law granted French citizenship to all in the French colonial empire, enabling registration and the issuance of the French West Africa (AOF) identity card in 1949 (Awenengo Dalberto 2020). From 1950, civil registration accompanied the exercise of new rights, such as voting, and access to pensions and family allowances (Cooper 2014). However, the vast majority of the population remained unregistered, as the generalisation of civil registration encountered technical, bureaucratic, and political difficulties in its implementation (Fouquet 2020; Cooper 2014). However, despite the shortcomings of the civil status system, it remained possible to obtain the AOF identity card, the establishment of which relied largely on testimonial evidence and not a civil status document many did not have (Awenengo Dalberto 2020).[2] The card typically included a photograph, handwritten or typed information, and official stamps or signatures.

2.2 Post-independence ID systems

Following Senegal's independence in 1960, significant reforms reshaped the identity landscape. While colonial-era systems maintained segregation, Law 61-55 of 15 June 1961 unified civil registration records. A postcolonial national ID system, marked by Law 1962-14 of 20 February 1962 then

1 The *indigénat* regime was the legal framework for colonial France's indigenous policy. It was a regime that legalised the use of oppression, repression, and violence by the colonial state against the indigenous peoples; for more details, see, for example, Merle (2004).

2 It was not possible through archival research to determine the number of cards issued in Senegal between 1949 and 1960.

instituted a national identity card, replacing the colonial-era AOF identity card. Mandatory for citizens aged 15 years and over, this card, valid for ten years, closely resembled its predecessor, with the key distinction of denoting Senegalese nationality. Family Code Law No. 72-61 (1972) further clarified the administration of the civil registration system.

In the early 1980s, the File Automation Directorate (DAF) within the Ministry of the Interior computerised this national card. A laminated document was introduced, featuring an 11-digit national ID number (Decree No. 85-1139 of 5 November 1985, establishing the National Register of Natural Persons (RNPP)). This initiative aimed to create a unique and compulsory national ID system for all citizens. The card included civil status, a photograph, physical characteristics, address, and profession.

Since 1962, the governance of foundational ID in Senegal has maintained relative stability, with key institutional actors largely unchanged. The Ministry of Territorial Collectivities oversees national civil registration policy, while the Ministry of the Interior manages the RNPP, issuing national identity cards and passports, and maintaining electoral lists. The Ministry of Justice is responsible for verifying civil status records. The Ministry of Foreign Affairs administers the civil status of Senegalese citizens living abroad through its network of diplomatic and consular posts.

2.3 Digital penetration in Senegal

Senegal has been a leader in digitalisation within West Africa. Digital technologies have penetrated daily life, particularly among its youth. As of January 2025, mobile telephony boasted a penetration rate of 121 per cent – attributed to SIM card registration and ownership of multiple SIM cards for access to diverse networks – while internet access has reached 60.6 per cent. The country counts 12 million internet users (out of a total population of 19 million) and 5 million active social media user identities (DataReportal 2025). Since 2004, e-administration initiatives have been pursued, though strategies have evolved (MCEN 2016; PAENS 2023), with mixed outcomes and only a limited number of administrative procedures currently digitised.

In February 2025, Senegal launched its digital strategy for the next decade, the 'New Deal Technologique'. This strategy 'aims to make Senegal a country of high value-added services, based on universal network coverage, the digital-ID of individuals, and the digital transformation of the administration and economic sectors' (MCTN 2025). The goals by 2034 include 90 per cent paperless administrative procedures, 90 per cent of Senegalese with a digital-ID, and 80 per cent utilisation of digital services. Additionally, 100 per cent of critical

data must be hosted within Senegal. This strategy has received strong support from the president and the prime minister, recognising digital technology as a crucial instrument for achieving development and social transformation objectives under the new government.

2.4 Digital-ID in Senegal

In 2005, Senegal adopted Law No. 2005-28 (6 September 2005), establishing a digitised national identity card. This law repealed the 1962 law and introduced a new digitised card based on biometric data, transitioning Senegal directly from computerised identity card to biometric digital-ID. Fingerprint biometrics were chosen to modernise personal identity and enhance reliability, with the law stating biometric data 'certifies and secures the identity of its holder.' The new digital national identity card featured a photo, ten fingerprints, and electronic signature as part of the government's efforts to modernise administrative identification. IRIS Corporation (Malaysia) was contracted to produce 10 million cards.

A decade later, these cards were replaced by a new biometric digital-ID card with regional scope, adhering to the Economic Community of West African ECOWAS's commitments. During the 46th Ordinary Session of ECOWAS Heads of State in December 2014, a decision was made to implement a common biometric smart identity card across all 15 member countries (ECOWAS Commission 2018), for reasons such as subregional economic integration, counterterrorism, and border management. In 2016, Senegal became the first country to adopt the ENBIC through Law No. 2016-09 (14 March 2016). This law repealed Law No. 2005-28. The new ENBIC included an electronic chip, facilitating interoperability within the subregion.

The 2016 law specifies the new ENBIC as a multi-application card, serving as a national ID, voter's card, and ECOWAS passport. The card integrates national ID information on the front and voter's ID details on the back; it functions as a travel document within the ECOWAS area. The ENBIC is Senegal's official digital-ID and has been mandatory since 2016 for citizens aged 15 or older, though it can be issued to citizens as young as five.

Table 2: Comparison of 2005 digitised national identity card vs 2016 ENBIC

Criteria	Senegal	ECOWAS
Identity card	Digitised national identity card	ENBIC
Legal basis	Law No. 2005-28 of 6 September 2005	Law No. 2016-09 of 14 March 2016 and Decree No. 2016-1536 of 29 September 2016
Nature of the document	Digitised card with photo, 10 fingerprints, and signature	Biometric card with electronic chip
Data contained	Photo, 10 fingerprints, signature, ID number	Photo, 10 fingerprints, signature, national ID number, possible electoral data
Use	Administrative identification (electoral use possible)	Identification, voter card, ECOWAS travel document
Electoral function	Possible if authorised by decree	Automatically included (electoral information on reverse)
Validity period	10 years	10 years
Minimum age required	15 years	5 years (mandatory from age 15)
Security technologies	Digitisation, electronic signature	Biometrics, encryption, laser engraving, secure electronic chip
Geographic coverage	National	Interoperable across the 15 ECOWAS countries
Main objectives	Modernisation and security of national identity	Regional harmonisation, anti-fraud measures, access to services
Responsible authority	Ministry of the Interior/DAF	Ministry of the Interior/DAF

Source: Author's own.

The card is issued by the DAF on presentation of an old identity card or passport, or a birth certificate less than one year old, or any document in lieu thereof, and a certificate of residence. It is free. This new digital-ID is required to obtain a telephone number or bank account; to access public services (electricity and water); and for all administrative procedures requiring reliable ID. Each card is valid for a period of ten years.

Senegal's population stood at 19 million in 2025 (ANSD 2023), with 39.1 per cent aged under 15, 57.1 per cent between 15 and 64, and 3.8 per cent 65 and over. Individuals aged 15 and over constitute 60.9 per cent of the

population, approximately 12 million people, who are required to hold an ENBIC. For the 17 November 2024 legislative elections, the biometric voter register listed 7 million registered voters. The Director General of Elections has reported that 2.9 million Senegalese possess an ENBIC without electoral data (APS 2025). Based on this, it is estimated that around 10 million citizens held a biometric national ID card in 2025, representing a coverage rate of 90.63 per cent for the population aged 15 and over. This suggests that around 10 per cent of that population – over 1 million people – lack ID and access to associated services and entitlements.

Recent data from the National Agency for Statistics and Demography (ANSD) (ANSD 2023) indicates that only 81 per cent of the population holds a birth certificate (88 per cent urban vs 73 per cent rural), a prerequisite for obtaining a national/digital-ID. Approximately 20 per cent of Senegalese (over 3.5 million) are unregistered at birth and death, thus evading identification. The birth registration rate in 2023 are 76.4 per cent, with significant regional disparities (85.7 per cent urban vs 67.9 per cent rural). Children (0–14), women, elderly people (70 and over), and rural residents are disproportionately represented among those lacking birth certificates or supplementary judgments.

Digital-ID is a foundational gateway to numerous fundamental rights and public entitlements. As highlighted by Fouquet (2020), the absence of civil status documentation continues to limit access to education, employment, health care, voting rights, and legal protection. Individuals born in areas underserved by the registration system are rendered invisible to the state and excluded from full citizenship. These dynamics, rooted in colonial governance, perpetuate structural marginalisation, affecting elderly people, children, and women, who are least likely to possess birth certificates (ANSD 2023).

The EU is currently funding the creation of a national biometric civil registry, the National Registration File (RNEC), through a partnership between Senegal's National Civic Registration Agency (ANEC), French company CIVIPOL, and the Belgian Agency for International Cooperation, Enabel.

Aligned with commitments made in the 2012 Durban (South Africa) and 2015 Yamoussoukro (Côte d'Ivoire) Declarations on civil status, the Government of Senegal has undertaken a significant programme to enhance the reliability and security of its civil registration system through computerisation and digitalisation. In addition to substantial public funding, ANEC was established in May 2023 (Fouquet 2020). ANEC's mission is to digitalise, centralise, and interconnect 689 civil registration centres through the centralised RNEC. As of 2024, 20 million civil status records had been

digitised and indexed,[3] and the civil status management application, *Nekkal*,[4] is being deployed in 400 civil status centres (ANEC 2025).

Regarding functional ID (single-purpose ID), Senegal currently maintains a dozen databases across various public and private organisations, each building its own ID system with multiple forms of disparate and varied ID data. A key challenge is the lack of interoperability between existing foundational and functional ID systems implemented by the public administration.

3 Interview with ANEC expert, 2025.
4 A Wolof word meaning 'existing'.

Table 3: Functional IDs

Type	ID	Issuer
Foundational ID	Civil registration (birth certificates)	ANEC
	National ID cards, passports, voting cards	DAF
Functional ID	Telecoms ID	Telecoms operators Orange, Free, Expresso
	Universal Banking Identifier	Central Bank of West African States (BCEAO)
	Capp Karangé for driver's licences and traffic fines	Ministry of the Interior
	CAMPUSEN digital identifier for students, which tracks their academic journey and associated social services (scholarships, health, housing); more than 400,000 students are registered with CAMPUSEN	Ministry of Higher Education and Research
	SIMEN (Ministry of National Education Information System), the largest information system in the administration, and an online portal that aggregates various services; as of 2020, more than 3 million students were registered in SIMEN	Ministry of National Education
	The Universal Health Coverage Agency (Agence CMU) produces the National Insurance Identifier (INA), which is linked to the universal health coverage system	Ministry of Health
	The Pension Fund (IPRES)–Social Security Fund (CSS) manages social welfare services with a unique identifier for family services, retirement, and workplace accidents	Department of Labour and the Civil Service
	E-Solde is a platform that allows civil servants to receive their payslips online	Payroll Directorate (Department of Finance)
	Unique National Register (RNU) for health, financial, and educational services for members of poor and vulnerable households; launched in 2013, the RNU contains data from 30% of the poorest households in Senegal	General Delegation for Social Protection and National Solidarity (DGPSN)

Source: Author's own.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Digital-ID lacks dedicated, comprehensive legislation in Senegal, which requires updates given the country's ambitions to establish a unique digital-ID for every citizen (Government of Senegal 2025; MCTN 2025). To address this gap, three bills concerning the computerisation of civil status, digital-ID, and digital health are being finalised. Currently, four main laws govern the regulation and protection of digital-ID:

1. Law No. 2016-09 (14 March 2016) and Decree No. 2016-1536 (29 September 2016) address the ENBIC, adding a secure electronic chip and enhancing interoperability within the subregion.
2. The Information Society Orientation Act (LOSI), Law 2008-10 (25 January 2008), serves as the foundation for Senegal's digital public administration and digitalisation of private enterprise activities, fostering citizen confidence in the information society.
3. Complemented by the law on electronic transactions, which recognises electronic signatures, electronic evidence reinforces the security of electronic exchanges, and equates electronic documents with paper documents.
4. Senegal's legal framework for digital identity protection is primarily governed by Data Protection Law No. 2008-12 (25 January 2008), concerning personal data protection and the establishment of the Personal Data Protection Commission (CDP). Defining personal data broadly, including any information relating to an identifiable natural person (Article 4.6), the law governs and protects digital identity, as foundational ID underlies digital-ID, and a person's identity constitutes personal data insofar as it enables identification or recognition. The computerisation of civil status files, the national biometric ID file managed by the DAF, and various sector-specific ID systems all constitute processing of personal data, falling under the purview of the Personal Data Act. The same 2008 law established the CDP, an independent administrative authority responsible for investigating personal data processing by the state, local authorities, and public or private legal entities operating in Senegal (LASPAD 2023).

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

The 2016 digital-ID law pursues legitimate aims by establishing a secure and modern ID system for Senegalese citizens, in accordance with regional ECOWAS commitments. Its objectives include:

- Strengthening the security and authenticity of ID documents.
- Facilitating access to public services.
- Enabling electoral participation through voter registry integration.
- Promoting free movement within ECOWAS by serving as a valid regional travel document.

These aims align with standards for public interest, including state security, efficient governance, and protection of citizens' rights.

Does the law clearly define the purposes for which the ID can be used?

Partially. Article 2 outlines key functions, including:

- National ID
- Electoral ID (voter card)
- Regional mobility within ECOWAS (travel document).

However, the law lacks an exhaustive list of potential future uses (e.g. banking, social protection, digital services), specific provisions regarding data sharing, surveillance risks, or limits to scope creep. The Data Protection Law 2008.12 addresses these concerns. The law sets strict conditions for data sharing, requiring explicit consent or legal justification (Articles 50–51). It mandates specific, legitimate purposes for data collection, forbidding incompatible processing (Article 35). To prevent surveillance, it regulates public data system interconnections, requiring prior authorisation from the CDP for certain categories (Article 53). The CDP authorises, monitors, and sanctions personal data processing (Articles 7, 9, 17). Despite its role, though, the law is now outdated and lacks modern safeguards such as mandatory breach notification, cookie consent management, and international data transfer frameworks.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

Based on a review of Senegal's Law No. 2016-09 (14 March 2016) and implementing Decree No. 2016-1536 (29 September 2016), the legislation does not explicitly define the actors permitted to access or use the ID data. While establishing the ENBIC and its functions (identification, voter registration, travel within ECOWAS), the law lacks detailed provisions specifying:

- Which public or private entities may access the card's stored data.
- Under what conditions this access is allowed.
- Mechanisms for oversight and accountability regarding data access and use.

Article 3 mentions the card's technical characteristics and biometric data storage, but it does not list authorised agencies or third parties. Although the law introduces a multi-application electronic chip card and mentions further modalities to be determined by decree, Decree No. 2016-1536 primarily details the card's physical characteristics and issuance procedures, without comprehensively regulating data access.

A comprehensive understanding of data access permissions requires referring to the 2008 data protection legislation. Senegal's Data Protection Law No. 2008-12 provides a broader personal data handling framework. The law defines 'data processors' as entities deciding to collect and process personal data, and mandates processing for specific, explicit, and legitimate purposes, prohibiting incompatible further processing. Prior authorisation from the CDP is required for certain activities, including database interconnections.

Does the law clearly define the nature of data that can be collected?

While Law No. 2016-09 and Decree No. 2016-1536 specify biometric identifiers such as fingerprints and facial images, they do not detail every data type, instead defining the scope of biometric data necessary for identification and verification.

For precise details on the scope of data, one must return to Article 20 of Data Protection Law 2008-12, which specifies that prior authorisation must be obtained from the CDP before processing any of the following data: genetic and health research data; data relating to offences, convictions, or security measures; a national ID number

or general identifier; processing biometric data; or data for public interest, including historical, statistical, or scientific purposes.

Data processors not subject to authorisation or notification must make a processing declaration. The CDP issued 2,165 authorisations and declaration receipts between 2014 and 2022 (LASPAD 2023).

Do individuals have rights to access, confirmation, correction, and opt-out?

Based solely on the law instituting the ENBIC and its related decree, there is no explicit mention of individuals having rights to access, confirmation, correction, or opt-out. These documents primarily focus on the establishment, implementation, and security aspects of the biometric ID card system. However, those rights are covered by Data Protection Law 2008-12.

The 2008 law recognises four rights: the right to information (Articles 58–61); the right of access (Articles 62–67), allowing individuals to request information from data processors regarding their collected/stored data, its nature, source, and any international data transfers; the right to object (Article 68), except where processing meets a legal obligation, which allows individuals to refuse data processing, and to be informed before data communication to third parties, with the right to object free of charge; and the right of rectification and deletion (Article 69), which allows individuals to require controllers to rectify, complete, update, block, or delete inaccurate, incomplete, equivocal, outdated, or unlawfully collected data. The law also consecrates data security and accuracy principles (Articles 36, 38).

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

The law establishing the ENBIC focuses on the card's creation, issuance, and validity. It does not include any provisions for redress mechanisms against misuse or governance of the system. However, the 2008 data protection law does provide for redress mechanisms that would be applicable to misuse of ENBIC data. The CDP is empowered to oversee data processing, investigate complaints, issue sanctions, and provide avenues for individuals to exercise their rights to access, correction, and objection. For example: in the event of an emergency, the CDP may decide to suspend processing for a maximum of three months, lock certain data, or temporarily or permanently prohibit processing that contravenes the law (Article 31). If the CDP observes a violation of the law on the protection of personal data, it can initiate proceedings and demand sanctions against the parties concerned. Senegalese courts have jurisdiction over disputes

relating to the protection of personal data. Senegalese citizens can lodge complaints with the courts for any violation of their personal data protection rights. The courts can order the immediate cessation of illegal practices, as well as compensation for damages suffered. Between 2014 and 2022, the CDP received 352 complaints and reports. It served 13 warnings and formal notices and carried out 32 on-site inspections (LASPAD 2023).

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

Senegal has an independent regulatory mechanism (the CDP) that should provide a degree of accountability for the administration of the digital-ID. The CDP is independent and has the powers to conduct inspections and investigations into the processing of personal data by Senegalese or foreign companies operating in Senegal. However, in practice the effectiveness of the CDP is questionable, given the limited human and financial resources, the type of leadership (the CDP is composed of 11 members appointed by decree; the chair is appointed by the president, instead of by a call for candidates) and strong resistance from powerful bureaucracies such as within the Ministry of the Interior.

Both foundational and functional ID systems are subject to serious flaws in the collection, storage, dissemination, and processing of data. It is possible for the state to cross-reference data and monitor individuals without any judicial oversight. Data collected for one legal purpose can be and is routinely and regularly used for other purposes with impunity due to an absence of documentation, control, and sanctions. Parliamentary, administrative, and citizen control mechanisms are not implemented and are sometimes not even known of by those responsible for this control. For example, Law No. 2016-33 of 14 December 2016 on intelligence services can serve as an illegal basis for surveillance, localisation, and political and administrative eavesdropping, including on social networks.[5]

5 Article 10: 'Special intelligence services intelligence services may, when they have evidence of one of the threats referred to in Article 2 and in the absence of any other means, resort to technical procedures, surveillance or location procedures to gather information useful in neutralizing neutralize the threat.'

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

No. The 2016 law's primary purpose is to establish a biometric ID card for ECOWAS citizens to facilitate movement within the region. The digital-ID card is a multi-application electronic card. The law does not include provisions that specifically limit the purposes for which the digital-ID can be used. Article 4 indicates that additional uses could be defined by decree in the future, expanding the scope beyond its initial purpose. This article leaves the door open.

Because the law does not explicitly limit the purposes for which it can be used, it is possible that over time the digital-ID could become a requirement to access more government services and entitlements.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

Without the ECOWAS biometric ID law and its related decree providing specific details, it is difficult to definitively determine whether privacy implications are necessary and proportionate. This depends on details such as the specific biometric data collected and its storage, the extent of system use beyond identity verification, and implemented data security measures. Nevertheless, the 2008 data protection law guarantees a number of principles that are applicable to digital identity. The principles of legitimacy, purpose, and proportionality: these principles require the consent of the person whose data is collected, except where collection is required by law, justified by the need to safeguard the fundamental rights and freedoms of the person concerned. The explicitly stated purpose of the collection must be respected (Article 35, para. 1), and the collection must be minimised or proportionate to this purpose (Article 35, para. 2). In terms of proportionality, for example, the information stored on the ECOWAS microchip seems a priori proportionate to needs. These are: forenames; surname; date of birth; place of birth; sex; home address; height (in cm); father's forename, and mother's forename and surname. In addition, ten fingerprints, a digital photograph, and an electronic signature are taken. For the electoral card, region, department, district, commune, voting place, and polling station are added.

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

No. From the 2016 ECOWAS biometric ID law and its related documents, it is *not* possible to determine whether the principles of data minimisation are adequately followed. The multi-application electronic chip card nature of the ID raises concerns about data minimisation. If the card can be used for various purposes beyond identity verification, there is a risk of collecting and using more data than necessary for each specific purpose. Indeed, a lot of data is collected without citizens being informed. For example, there is a total lack of information in the legislation on facial recognition, on-board technologies in vehicles and their uses, the data collected and where it is stored, and whether or not the data collected and/or processed

is regulated. Decree No. 2016-1536 of 29 September 2016 implementing Law No. 2016-09 of 14 March 2016 instituting the ENBIC is silent on facial recognition and its uses. In addition to the national biometric card and passport, the private companies responsible for toll freeway security and urban transport – respectively, Société Eiffage de la Concession de l'Autoroute de l'Avenir (SECAA SA), and Dakar Regional Express Train (TER) and Bus Rapid Transit (BRT) – illegally capture licence plate images and photos of public transport users on behalf of the state.[6] Surveillance cameras are installed on all the main arteries of the capital and major cities. The misuse of biometric data by the government is well known by the people. During the political turmoil of 2021–23, demonstrators were arrested through using facial recognition devices, probably collected and trained on biometric card data, subsequently forcing protesters to wear balaclavas. While it is obvious that the police use facial recognition, there is still a legal vacuum, and prior declaratory formalities to CDP have not been carried out.[7]

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

Data exchanges between government departments (ANEC and the DAF) and with private actors (telecoms and banks) are carried out without necessarily obtaining the authorisation or approval of the CDP. Technically, civil registration files, and those of the DAF, and telecoms operators (and banks) are siloed, but one-way interoperability channels do exist, enabling checks to be carried out. For example, operators[8] are required, to identify buyers and users of SIM cards when they subscribe to mobile phone services, in accordance with Decree No. 2007-937 of 7 August 2007. The Regulatory Authority for Telecommunications and Postal Services (ARTP) strictly monitors the ID of mobile (cell) phone subscribers in Senegal: the main aim is to ensure that each telephone number has a reliable identity (surname, first name, and national identity card number). On ARTP's orders, the database of biometric ID is made available in consultation with telecoms operators to verify individuals' identities (ARTP 2013). The link can then easily be made between the biometric ID card and SIM card number. During Covid-19, under the guise of epidemiological surveillance, this is how contact cases were located and monitored.[9]

6 CDP interview, 2025.
7 Interview with former CDP expert, 2025.
8 Senegal has currently three main telecoms operators: Orange, Free, Expresso.
9 Interview with former CDP expert, 2025.

Similarly, the fight against money laundering and terrorism (Law 2018-03) justifies the collection of economic and financial information from any person through the National Financial Information Processing Unit (CENTIF). In 2023, the proportion of households with access to banking services stood at 22 per cent (nearly 4 million people), but the thanks to microfinance and e-money services that increased to 60 per cent (11 million) (DER/FJ 2024). In theory, no structure – be that ANEC, the DAF, telecoms companies, banks, or microfinance institutions – can copy the files of another actor, and verifications never concern the whole population, but rather individuals or groups of individuals. But when it comes to implementation, the government has access to all data under the umbrella of public security, and the fight against terrorism, organised crime, and international trafficking: civil status, biometrics, data from telecoms operators, banks, and microfinance institutions. It therefore has discretionary powers to interconnect data for specific purposes. The linking of biometric digital-ID to a person's bank account and mobile phone provides the Senegalese state with a potentially powerful real-time panoptic surveillance capability that can track any citizen's GPS position, transactions, calls, network of associations, and messages.

Even more worrying is the predation of biometric data by third parties (notably the EU) for the purposes of controlling and repatriating undocumented migrants. The 'Support Programme to Strengthen the Civil Registration Information System and Consolidation of a National Biometric Identification Database', financed by the EU Emergency Trust Fund for Africa, has been formulated and implemented with a specific focus on identification issues related to the management of the return of irregular migrants (Commission européenne 2017). The operational framework for this EU programme is very clear: 'to prevent irregular migration and forced displacement and facilitate migration management and return; Strengthen cooperation to facilitate the return and reintegration of irregular migrants' (*ibid.*). The overall objective of the programme, which cost €28 million, is to ensure that the identification of individuals registered is secured by their biometrics and to establish a database that is 'exploitable by other user administrations, including its use to identify illegal Senegalese nationals' (*ibid.*). The programme is being implemented by CIVIPOL, the private international technical operator of the French Ministry of the Interior, and Enabel, the Belgian agency for international cooperation. Officially, the government assures that the data collected is housed locally, and there is no agreement with the EU to share civil status data. Technically, however, it is quite possible that, thanks to a backdoor system, the hosting system, and the software settings, European counterparts may also hold this data. Privacy International (2020) has

issued a report showing that the system presents considerable risks for the protection of Senegalese personal data, and demonstrates that this programme is actually designed to facilitate expulsions from the EU.

Article 49 of the 2008 data protection law prohibits the transfer of personal data of Senegalese nationals to a third country, except when: the guarantee of legal protection is at least equal to that prescribed by Senegalese law in the third country, or there is sufficient technical protection on the part of the data controller in this third country; and on the condition of informing the CDP in advance and obtaining authorisation. The CDP has never received such a request.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Current studies highlight the challenges of accessibility and inclusion. As we move towards digital identities, the right to a safe and secure digital-ID is certainly not guaranteed for everyone. The risk of exclusion for certain groups is very high, notably those without access to the internet, digital devices, or electricity – mainly rural populations, people with disabilities, elderly people, and other vulnerable groups. The population of Senegal is still largely rural (46 per cent according to ANDS 2023) and vulnerable (37.5 per cent). Without such ID, the people concerned will *de facto* be excluded from access to public, financial, and telecoms services, and will be in a situation of pure and simple digital statelessness. The risk of exclusion is linked to a failure to register births, particularly in rural areas, and the significance of documentary fraud (Fouquet 2020: 73). That is why the implementation of a universal-ID presupposes that these two problems have been properly resolved upstream. So far, the quite inefficient mitigation mechanism used consists of 'open hearings', with questionable results. Open hearings are public sessions during which the judicial authorities regularise the situation of all those present who can prove their identity, usually with the help of two witnesses (*ibid.*: 84). Another mechanism for inclusion on the electoral registers is the electoral census organised before an election is held, in order to update the electoral lists and enable all citizens to exercise their right to vote.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

Yes, for the ENBIC. Article 2 of Law No. 2016-09 of 14 March 2016 on the ENBIC states: 'This identity card is issued to Senegalese citizens. It is compulsory for all citizens aged at least fifteen (15) years and may be issued to any citizen aged at least five (5) years.' The legal grounds for making biometric ID mandatory are based on a mix of internal and external reasons.

The explanatory memorandum of the law emphasises that the card is intended for citizen identification, to facilitate mobility and deepen economic integration, and is in compliance with ECOWAS obligations. The other legal basis is related to improving security within the ECOWAS region and fighting terrorism.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

Regarding the 2016 law and decree, there is no explicit mention of a formal risk assessment having been conducted prior to the implementation of the 2016 law. However, a parliamentary report issued prior to the law's adoption does refer to a few risk factors, such as the legislature being aware of human trafficking; the government also guarantees it will do its best to avoid individuals in ECOWAS having multiple IDs.

The current phase in Senegal's new digital strategy (by 2034, 90 per cent of administrative procedures should be paperless, 90 per cent of Senegalese should have a digital-ID, and 80 per cent should be using digital services) is that of solutions production, under the technical leadership of the Ministry of Digital Affairs and its technical arm Senegal Numérique (SENUM). This phase involves discussion of the digital public infrastructure models to be implemented (e.g. centralised like Adhaar, a biometric ID system for the population of India, or decentralised like X-Road, Estonia's interoperable digital platform), and which digital public goods (e.g. Mosip, modular and open-source technology for countries to build and own their national ID systems) are best suited to achieving the aforementioned objectives and ensuring the country's digital sovereignty.

The New Deal Technologique, with its ambition to move towards an 'e-administration' and a single digital-ID, has not been the object of an impact study to identify potential risks, dependencies, and challenges, and to suggest practical and effective mitigation measures. However, a previous feasibility study of the national digital-ID project, conducted by Gaindé 2000 (2022), does exist. That study established a solid baseline. An assessment report has also been commissioned by the Project for the Acceleration of the Digital Economy in Senegal (PAENS), a project run by the Ministry of Digital Affairs with a loan from the World Bank, whose terms of reference for the implementation of a government enterprise architecture include a risk assessment (PAENS 2023). However, this report has not yet been made public.

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

Yes. The 2008 data protection law provides a framework that allows and requires a differentiated approach based on risk, even if the term 'digital-ID' is not mentioned. Its general principles and specific provisions would apply to the processing of personal data through the ECOWAS biometric ID system. The 2008 law follows a risk-based approach, even though it does not explicitly use that term. The obligations imposed on data controllers, the level of scrutiny applied by the CDP, and the conditions for processing depend on the sensitivity of the data and the potential impact on individuals' rights and freedoms. The law differentiates between data processing that requires prior authorisation from the CDP (Article 20) and processing that only requires a simple declaration (Article 18). Processing that entails a higher risk to privacy (e.g. genetic data, data relating to criminal convictions, interconnection of files) requires authorisation. Processing that entails a lower risk requires only a declaration.

Article 40 places restrictions on processing sensitive data (racial origin, political opinions, religious beliefs, health, etc.), recognising the higher risks associated with this type of data. The law requires data controllers to implement security measures appropriate to the risks (Article 71). The specific measures required would depend on the nature of the data and the potential harm that could result from a data breach. The public sector has derogations in specific cases for reasons of national security.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

Senegal's 2008 data protection law establishes a foundation for governing digital-ID systems in a manner that aims to be proportional to the potential risks involved. The law adopts a risk-based approach, where stricter regulations and oversight are applied to data-processing activities deemed to pose a higher threat to individual privacy. This includes heightened scrutiny for sensitive data categories, such as health or political affiliation, and a requirement for prior authorisation from the CDP for processing activities considered particularly risky. Proportionality is further embedded in the law through principles that limit data collection to what is adequate, relevant, and not excessive; restrict its use to specified and legitimate purposes; and mandate retention periods that are only as long as necessary. However, the effectiveness of this framework in

ensuring proportional governance hinges on several factors, including the CDP's capacity to thoroughly assess the specific risks associated with digital-ID systems, the implementation of targeted regulations that address challenges posed by these systems, and a demonstrated commitment to actively enforce the law and penalise violations.

6. Recommendations

Recommendation on inclusion

Iterative, creative and effective mechanisms can ensure that digital-ID does not lead to exclusion from services or rights. Designing for inclusion could involve varied or differentiated approaches for different target populations, providing multiple means of accessing and using digital identities; for example, through mobile devices or support services at local community centres. This inclusion must also be linguistic and technological.

Recommendation on governance

It is important to strengthen the role of civil society, particularly the National Human Rights Committee, in developing solutions, and implementing, monitoring, and evaluating digital-ID rights. Furthermore, researchers should be given a central role in documenting the process of digitalisation and addressing specific issues. In the absence of effective oversight and accountability, specialised journalists should also have a role in the governance system.

Recommendation on effective implementation of control

The Constitution gives the National Assembly a mission to evaluate public policies. Digital-ID, intelligence activities, and the use of sensitive data by the administration, the executive, and political leaders should be subject to strict oversight. The National Assembly, representing the people, has several instruments to carry out this work (committees of inquiry, special committees, fact-finding or study missions, written questions and oral questions with or without debate). Article 15 of the Intelligence Act gives the National Assembly the prerogative to hear the prime minister or ministers responsible for intelligence services before the Defence and Security Committee. And Article 12 authorises the total or partial declassification of a document by decree if it does not constitute a threat to national security or to intelligence personnel and sources. However, to date, none of these levers have been mobilised. The result is a situation of collective ignorance and general impunity, even though abuses have occurred and could occur, and the bodies responsible for digital-ID must be held accountable for their actions.

7. Bibliography

Amnesty International (2023) ***Sénégal: des manifestations sous haute tension*** (accessed 12 October 2025)

ANSD (2023) *5e Recensement général de la population et de l'habitat (RGPH-5, 2023)*

APS (2025) '**Près de 3 millions de Sénégalais détiennent une carte biométrique sans données électorales (DGE)**', *AllAfrica*, 14 February (accessed 10 November 2025)

ARTP (2013) ***Note explicative sur le projet d'identification des abonnés***, Autorité de Régulation des Télécommunications et des Postes (accessed 12 October 2025)

Awenengo Dalberto, S. (2020) '**La première carte d'identité d'Afrique occidentale française (1946–1960): Identifier et s'identifier au Sénégal au temps de la citoyenneté impériale**', *Annales. Histoire, Sciences Sociales* 75 année.1: 113–51, DOI: 10.1017/ahss.2020.114 (accessed 12 October 2025)

Awenengo Dalberto, S.; Banégas, R. and Cutolo, A. (2018) 'Biomaîtriser les identités ? État documentaire et citoyenneté au tournant biométrique', *Politique Africaine* 152: 5–29

BECEAO (2023) ***Rapport sur la situation de l'inclusion financière dans l'UEMOA au cours de l'année 2022***, Banque Centrale des Etats de l'Afrique de l'Ouest (accessed 12 October 2025)

Commission européenne (2018) *Évaluation ex post du projet d'appui à la modernisation de l'état civil au Sénégal (PAMEC)*

Commission européenne (2017) ***Document d'action du Fonds fiduciaire de l'UE: T05-EUTF-SAH-SN-07*** (accessed 12 October 2025)

Cooper, F. (2014) *Citizenship Between Empire and Nation: Remaking France and French Africa, 1945–1960*, Princeton University Press

DataReportal (2025) ***Digital 2025: Senegal*** (accessed 12 October 2025)

DER/FJ (2024) *Évaluations d'impact des dispositifs de financement inclusifs. Publications internes, 2020–2024*, Délégation générale à l'Entrepreneuriat Rapide des Femmes et des Jeunes (DER/FJ)

Dikhaté, J. and Dièye, M (2019) 'La conservation numérique de l'état civil sénégalais, un moyen d'une démocratisation de l'accès à l'information dans une ville intelligente', *Revue maghrébine de documentation and d'information* 28: 1–22

ECOWAS Commission (2018) ***Free Movement Protocol: The Context of ECOWAS Biometric Identity Card in the Community***, Abuja: ECOWAS Commission (accessed 12 October 2025)

Fouquet, K (2020) ***L'état civil sénégalais aujourd'hui, de l'enregistrement à l'archivage : Les difficultés d'un outil de bonne gouvernance et de respect des droits humains***, Angers: Université d'Angers (accessed 12 October 2025)

Gaindé 2000 (2022) ***Étude de faisabilité du projet identité numérique nationale*** (accessed 12 October 2025)

Gaindé 2000 (2021) ***Revue du cadre juridique pour l'identité numérique nationale*** (accessed 12 October 2025)

Government of Senegal (2025) **Conseil des ministres du 26 février 2025**, 26 February (accessed 12 October 2025)

LASPAD (2023) *Renforcer la protection des données personnelles en Afrique: vers un système harmonisé et efficient*, Rapport Sénégal, UGB LASPAD, Saint-Louis

Légier, G (2014) '**La législation relative à la nationalité française durant la Première Guerre mondiale**', *Revue critique de droit international privé* 4.4: 751–95 (accessed 12 October 2025)

Le Monde (2023) '**Sénégal: une « Mysterious Team » derrière les cyberattaques contre l'État ?**' , 29 May (accessed 12 October 2025)

MCEN (2016) ***Stratégie Sénégal Numérique 2016–2025***, Ministère de la communication et de l'économie numérique (accessed 12 October 2025)

MCTN (2025) ***New Deal Technologique***, Ministère de la communication des télécommunications et du numérique (accessed 12 October 2025)

Merle, I. (2004) 'On the "legalization" of violence in a colonial context. The indigenous regime in question', *Politix. Revue des sciences sociales du politique* 66: 137–62

Organisation internationale de la Francophonie (2020) ***Guide pratique pour la consolidation de l'état civil, des listes électorales et la protection des données personnelles: enjeux et principes fondamentaux***, Paris: Organisation internationale de la Francophonie (accessed 12 October 2025)

Ouestaf.com (2024) *Sénégal: la société civile dénonce les coupures d'Internet*, 14 December

PAENS (2023) *Termes de références pour la mise en place d'une architecture d'entreprise gouvernementale et d'une étude de faisabilité sur la mise en place de l'identification numérique et de l'interopérabilité des plateformes, pour l'État du Sénégal*

Privacy International (2020) *Comment une société de sécurité bien connectée crée-elle en catimini des bases de données biométriques à grande échelle en Afrique de l'Ouest avec les fonds d'aide de l'Union européenne*

TV5 Monde (2023) ***Sénégal: les coupures d'Internet à répétition, une mesure illégale?*** , 29 May (accessed 12 October 2025)

Digital-ID in the Democratic Republic of the Congo: Country report

Arsène Tungali

 DOI: 10.19088/IDS.2025.056

1. Introduction

The Democratic Republic of the Congo (DRC) does not yet have a functioning digital identification (digital-ID) system, despite repeated announcements and facilitating legislation. This study assesses the current situation of preparedness for the implementation of the digital-ID project using the Centre for Internet and Society (CIS) framework of tests. The report starts with an overview of the historical evolution of identification of citizens, beginning with the paper-based colonial systems. After independence, a new system of ID was introduced, as the country went through a political crisis and was divided, with each region having its own ID system. Later, political reunification paved the way for various forms of foundational and functional national IDs.

This report highlights the most widely used and known form of functional ID in DRC, the *Carte d'électeur* (Voter Card), which was designed to serve for electoral purposes and as a provisional national ID but ended up being used (and is still used) as the *de facto* national ID. The Voter Card is set to be replaced soon by a national digital-ID that has been in development for several years. This report employs the CIS framework to structure its analysis. This involves subjecting the digital-ID project to three sets of tests: a rule of law test, a rights-based test, and a risk-based test. Each involves responding to a series of questions that assesses, among other things, the ID's legality (looking at the legislative mandate that backs this project), and the principle of data minimisation (and whether this will be followed in the collection, use, and retention of personal data). However, the analysis is limited by the fact that the project has not yet been deployed.

The study concludes with a set of recommendations to various stakeholders in their respective roles in order to ensure, among other recommendations, that citizens' rights are well taken care of during all phases of the project.

2. History of ID in DRC

In this section, I present the history of ID documents in the country from the colonial period until the introduction of digital-ID systems.

It is important to start by sharing that the history presented here is that of the country that is known as the DRC today, which has gone through a series of changes of name and leaders, starting with the period under Belgian authority (1908–60); then the period starting with independence (liberation from colonial rule) when the country was named Republic of Congo (1960–65); then DRC (1965–71); then the Republic of Zaire (1971–97); then back to DRC. Throughout these various stages in the country's history, there have been a range of IDs systems serving various purposes and interests, as will be seen in the following sections.

2.1 Colonial ID systems

According to Malonga (2020), under Belgian rule, the first ID document was the *Livret d'identité* (Identity Booklet, 1917–35). The second system was the *Certificat d'identité* (Identity Certificate, from 1935), which was issued to every Congolese person aged 16 years old at minimum. Three other important and very hierarchical systems are to be mentioned here: the *Carte de mérite civique* (Civic Appreciation Card), introduced in 1948, established by a decree of 12 July 1948 'recognising to some Congolese the right to a life similar to the one of the whites' (Malonga 2020 [author's translation]). This was followed in 1952 by the *Carte d'immatriculation* (Registration Card), something not all Congolese nationals had access to because it enforced racial hierarchy, awarding privileges for being part of the 'civilised' community. It only used to be accessible to Europeans living in the country from the early phases of the colonial period, then was extended to a few Congolese nationals, starting in 1952, who were now holders of both the Civic Appreciation Card and the Registration Card. This same category of Congolese nationals also had access to the 'Colonial Passport', the actual Belgian passport, because colonial authorities did not issue passports for their colonies.

In 1953, two new ID systems were issued: the *Carte d'identité inaltérable* (Unalterable Identity Card) which was laminated and imposed on adult male Congolese natives, followed by the *Certificat d'identité* (Certificate of Identity) (7sur7.cd 2014).

2.2 Post-independence ID

At independence on 30 June 1960, the country did not have a national identity card. Immediately after independence, the country entered a period of political tension, leading to the secession of some regions whose local political leaders rebelled against the national powers in place. As an example, in the regions controlled by Leopoldville (the capital city) an Identity Certificate was used, mentioning the name of the province of the holder. In Stanleyville, they had *attestations d'immatriculation* (registration certificates), while in the Katanga region (1960–63) they had their own ID as well as a local passport (Malonga 2020). As a result, each region had its own ID system whose security features and identity data were revised periodically, until the point where all citizens were able to access a laminated picture ID, as will be explained in the sections that follow.

According to Malonga (*ibid.*), the first identity card for Congolese was issued nine years after independence, on 25 February 1969. The government decided to abandon the use of Certificates of Identity, which were seen as a colonial relic. The new identity card contained all the essential information about the holder: names; place and date of birth; parents' names; sex; marital status; spouse's names; fingerprints; place of residence; origin (village, community, zone, and region); and occupation.

Definitions

According to the Word Bank's Identification for Development (ID4D) Initiative, an ID system can be considered a 'legal ID system' to the extent that it enables a person to prove who they are using credentials recognised by the law or regulation as proof of legal identity (i.e. most foundational ID systems) (World Bank n.d.).

Foundational vs functional ID systems

The CIS defines 'foundational ID systems' as those that are general-purpose systems that can be used for many different purposes, whereas 'functional ID systems' are those designed and built for a specific purpose. These ID systems are used for conducting the processes of identification, authentication, and authorisation (Katira 2019). The National Identity Management Commission of Nigeria shares that a foundational ID helps explain 'who you are' while a functional ID helps explain 'whether you are eligible for a specific benefit' (NIMC n.d.).

2.3 Foundational ID systems in DRC

According to Article 82a of the DRC Family Code: 'All births, marriages and deaths are recorded in the form of certificates in a separate civil status register, known as a birth, marriage and death register' (Leganet 2017b). This study does not speak about the death certificate since it is not a document used by the owner as a form of an ID.

Birth certificate

The birth certificate is an important document that serves as the primary and first ID document each Congolese citizen is supposed to have at their birth. Declaring and registering a child at birth establishes, per the law, the existence of the child. Registering them officially in the civil status register is an important act that grants them rights including their civil, political, social, economic, and cultural rights. The birth certificate received is the proof of their citizenship (SOS Enfants n.d.). In practice, I can say that this is the document that grants access to other forms of functional ID at a later stage.

Marriage certificate

Articles 390–392 of the Family Code introduce this document. It is issued by the Officer of Civil Status and signed by both the officer and the spouses during the celebration of their marriage, and then handed to the married couple as the official document attesting their union. Among the elements present on this certificate are the names, sex, place and date of birth, occupation, nationality, and domicile or residence of each of the spouses; the names, sex, profession, nationality, and domicile or residence of the father and mother of each of the spouses and matrimonial witnesses as required by law; the choice of matrimonial property regime adopted by the spouses, etc.

2.4 Functional ID systems in DRC

DRC officially entered the era of digital-ID systems through the arrival of the Voter Card in 2004. In addition to the card, the country has various other functional ID systems, some of which are provided by the state, such as driving licences and the national passport, while others are provided by private entities for internal use. The latter include student IDs (for high-school and college students), employee IDs (for employees of various entities), and so forth.

In this section, only state-delivered IDs will be presented, starting with the national passport, then the driving licence, and finally the Voter Card. From 1997 until 2004, there was no national ID in DRC and up to the time of writing of this report, the Voter Card has acted as the *de facto* national ID.

National passport

In DRC, there are three types of passports: diplomatic passports, used by diplomats and certain categories of government officials such as ministers; duty passports, used by public servants; and regular passports, used by citizens. According to Jeune Afrique (2017), DRC introduced semi-biometric passports in April 2009, which were supposed to be valid until December 2015 and the introduction of the fully biometric passports. Both are digital (or electronic) passports but the latter is more secure, with an embedded microchip (in a small, gold camera logo at the bottom of the cover) containing biometric information that can be used to authenticate the identity of the passport holder.

On 27 May 2025, the DRC government, through the Ministry of Foreign Affairs, International Cooperation and Francophonie announced a new Congolese passport would be introduced that '[aimed] to respond to the major concerns of the Congolese population regarding the security of travel documents abroad and the simplification of the acquisition of this essential document' (MINAFFET 2025). The press release further announced that the new passport (which would contain 38 pages, up from 32) was in response to Norm 39794 of the International Civil Aviation Organization and included the following features:

- A contactless radio frequency identification microchip.
- A polycarbonate data page offering greater resistance to falsification.
- Holograms and watermarks to make counterfeiting more difficult.

What is interesting about this new passport is the simplified and direct mode of application, which it was announced would be partly online,[10] starting 5 June 2025, while new centres to collect biometrics were to be deployed across the country, as a way to ensure national coverage and accessibility, which was a big challenge under the current system.

In addition to the national passport, whose primary use is for international travel, the DRC Immigration Office (DGM) issues other forms of travel documents, which are mainly used for regional trips (within specific subregions of Africa). These, however, need to be presented alongside the Voter Card (or the national passport) in order to serve to identify the holder, and to be stamped to authorise entry into or exit from the relevant subregion.

10 Via a passport **registration and payment website**.

Driving licence

The driving licence is a functional ID document that is used mainly for driving purposes. It was instituted in December 1997 by ministerial decree. The entity responsible for issuing driving licences in DRC, CONADEP (Leganet 2017a), issued various forms of driving licences until the announcement in early March 2012 of the first digital driving licence with a microchip, which was designed to prevent the document being issued to those with no proper driving knowledge and to ensure mastery of the driving code (Agence Ecofin 2012).

For reasons that remain unclear, in September 2017 the government suspended the delivery of this driving licence; it took nearly seven years before a new, more secure biometric driving licence (with a microchip) was announced in November 2024. According to the minister responsible for transportation, the objective was to 'modernize and secure the process of obtaining a driving licence by introducing biometric features that will make it possible to combat fraud and forged documents more effectively' (Radio Okapi 2024).

Voter Card

The Voter Card was introduced by law in 2004 as an ID document meant to serve for the 2006 election cycle. Per the law, to be eligible for ID, and therefore to have access to the Voter Card, one has to be of Congolese citizenship; to be at least 18 years of age on the date of completion of all identification and enrolment operations; to be on DRC territory at the time of identification and enrolment; and to be entitled to civil and political rights (CENI 2016).

In order to have access to a Voter Card, one has to provide a document proving Congolese citizenship, which includes a birth certificate, a previous Voter Card (when one is renewing the card), a national passport, a driving licence, etc. According to the electoral body (CENI n.d.), if applicants cannot provide any of the above they are required to obtain a letter from a local authority attesting to their citizenship, and to come to the registration office accompanied by three witnesses who have already received their Voter Cards. Because the country did not have an official national ID, the Voter Card (in all its various iterations, per electoral cycle) was used for both purposes – for the elections and as a provisional national ID for Congolese citizens until this function was officially removed by law in 2016. But since there is no official national ID, the practice of using the Voter Card has continued to date.

On this note, Jordan Tshilombo Kabamba, the principal information communication and technology advisor at the electoral body CENI, shared the following during an interview as part of this study:

> *No article of Law No. 16/007 of 29 June 2016 which is an amendment of Law No. 04/028 of 24 December 2004 explicitly states that the electoral card no longer serves as an identity card. In fact, the explanatory memorandum to the 2004 Act acknowledged that, but the one of the 2016 Act has no such mention. It completely refocuses the electoral card on its electoral role, with no administrative status.*

He further shared that the current Voter Card was produced to a low quality because CENI thought that it would be used solely for the December 2023 elections, since deployment of the digital-ID project had been announced as imminent. But, two years later, citizens are seeing their Voter Cards deteriorate and CENI is obliged to produced new cards as citizens need to carry a form of ID.

The Voter Card, as the source of legal identity, is the primary document that grants access to the other existing ID systems across the country and across sectors, as well as being used to access government services. The Voter Card used for the 2018 election cycle was a laminated, paper-based ID with a digital photo and a barcode. The most recent one, used for the 2023 election cycle, is similar, but the barcode has been replaced by a QR code. The latter is the one being used currently as the *de facto* national ID.

2.5 Towards a national digital-ID

DRC has been in the process of sourcing the right approach to provide its citizens with a national digital-ID with the objective of replacing the Voter Card. It is for that reason that a new entity, the National Office for Population Identification (ONIP), was created in 2011 with the mandate of conducting a population census, as well as delivering a national ID to Congolese citizens.

Eleven years later, in 2022, the prime minister signed the Decree on the Creation of a National Identity Card (CIN) in DRC (the 2022 Decree) through ONIP, a digitalised card using biometric data, which would be mandatory for all Congolese citizens aged 18 and over. According to Article 4 of the 2022 Decree (ONIP 2022), the card would contain personal information, including the following: the card number (unique identifier); the holder's full name; their place and date of birth; their sex; their (digital) photograph; their physical address (of residence); their signature; the signature of the authority that delivered the card; the place and date of issue; and the validity of the card; as well as fingerprints and/or iris scan.

With that in place, and as a way to show that the process had started and that it would be the case for the whole population in the days or months to come, on the 63rd anniversary of the country's independence,

on 30 June 2023 the president was presented holding the first copy of the national digital-ID card delivered by ONIP (Presidence.cd 2023).

But since that event, a number of issues have arisen that have made it hard to issue Congolese citizens with their digital CINs. These include acts of corruption, and lack of proper and sound management of the process, coupled with logistical issues due to the size of the country that make it hard to deploy the necessary equipment and materials. According to German media (Deutsche Welle 2024), the agreement between the government and the two companies hired to work with ONIP to manage this process was cancelled 'in good faith' after an alert from a national financial control entity that revealed that the project's cost had risen from US$400 million to US$1.2 billion, which was either because of overpricing or corruption involved in the system.

As presented in the previous sections, the CIN is yet to be deployed across the country. The 2022 Decree that created it aimed to set the tone, while at the same time announcing a subsequent ministerial order (from the Ministry of the Interior). This was the Ministerial Order signed on 15 November 2023 (the 2023 Ministerial Order) on practical aspects regarding the creation and deployment of the CIN (ONIP 2023).

It is also important to note the creation, under the ONIP's supervision, of the General Population Register (FGP) by Decree No. 22/07 of 2 March 2022 (Leganet 2022), which is the initial and unique register of reference, collecting, according to Article 2, 'biographical and biometric information regarding the identity of natural persons and information regarding marital status' pertaining to every Congolese citizen (in and outside of the country), as well as all foreigners who have permanent residency in DRC. After registration, a unique National Identification Number is issued. The register is updated regularly, serves as the basis for the CIN, and is managed according to the data protection law (the Congolese Digital Code). According to Article 13 of the 2023 Ministerial Order, whenever data is updated or modified in the FGP, this will result in the CIN being updated and replaced as necessary.

In the following sections, these legal instruments will be examined in light of the three tests in the CIS framework: the rule of law test, the rights-based test, and the risk-based test. It is therefore important to note that these tests will be based on the mentioned pieces of legislation rather than actual practice in the field because the process has not started yet. Finally, since it is about personal data, the 2023 Digital Code will also be examined in order to present a picture of what legal instruments say with the hope these prescriptions will be followed in the deployment of the digital-ID project in DRC.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

The digital-ID in DRC is not backed by a validly enacted law but rather by the 2023 Ministerial Order on applicable measures about the creation of the CIN, which implements the 2022 Decree on the creation of the CIN, as presented in the previous sections. However, under Article 183 of the 2023 Digital Code (Droit Numérique 2024a), personally identifiable data includes a person's full name and their official ID document (the CIN falls into this category). That means, the collection, treatment, transmission, storage, and the use of personal data by the state should be carried out in accordance with the provisions of the Digital Code.

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Article 1 of the 2022 Decree states that: 'The DRC has created an ID document for Congolese citizens, known as the *Carte d'identité nationale* (CIN). The CIN certifies and establishes the Congolese identity of its holder.' This can be considered as the statement of the aim of the card, which I personally consider as legitimate.

That being said, this is the legal and official document that establishes the Congolese identity of its holders, a role currently being played by the Voter Card, though no longer legally. The CIN is meant to be a digital-ID with a chip that allows those with authority to check and confirm the validity and accuracy of the data it contains, and serves for many other purposes as a true foundational ID. As in many other countries that have implemented such initiatives, this initiative will ensure the digital registration of citizens, which is an improvement on manual data collection, which presents many risks, such as data loss and loss of confidentiality. Collecting the population's vital statistics allows decision makers to have an understanding of the real number of humans in the territory at a given point in time, for better service delivery.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

Important aspects of data governance are addressed in Article 6 of the 2023 Ministerial Order, which limits which actors are permitted access to ID data. However, the categories of actors are imprecise and too broad to act as guard-rails for data governance. Article 6 provides that only 'relevant security service personnel, civil servants or public agents, as well as private individuals, in accordance with the regulations in force' are authorised to access 'non-apparent data contained in the CIN'. This statement in itself is something that can be considered to be overly broad since it is not clear about who exactly the actors are, and could potentially lead to various interpretations, and therefore potential violations of citizens' privacy.

According to Article 4 of the 2022 Decree, the data to be collected in the process of obtaining the CIN falls within two main categories: **apparent data** (a list of 16 items is provided in the legislation), as well as **non-apparent data** (a list of ten items is provided in the legislation). The spirit of this text is that non-apparent data refers to data that can be read electronically using digital technology, which includes fingerprints, iris scan, the signature of the holder, the validity of the card, etc.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

The 2023 Ministerial Order speaks about sanctions (through the Congolese Penal Code), mostly against CIN holders who misuse their card, although many of the cases mentioned and which lead to sanctions could have their source in or be facilitated by the entities that govern the use of the CIN. For example, Article 11 of the 2023 Ministerial Order states that sanctions will be directed towards anyone who receives a CIN based on false declarations, holds two CINs in their own name, uses a counterfeit CIN, or is at the origin of altering a CIN.

According to Article 4 of the 2023 Ministerial Order, the CIN is mandatory for every citizen aged 18 years in or outside of the country, and can be granted to anyone who is below 18 per a request through their legal custodian. Per Article 13, holders of the CIN have the possibility to have their data edited or modified, and this will result in the delivery of a new CIN; but since this ID is

mandatory for citizens over 18, there is no possibility to opt out. In case of loss, citizens have the possibility to request another card through a clear process.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

No independent regulatory mechanism has been put in place to ensure accountability in the administration of the CIN as a form of specific personal data. All operations pertaining to the collection and maintenance of data, as well as the delivery of the CIN, are the responsibility of ONIP, which is an entity under the Ministry of the Interior, Security and Customary Affairs.

However, because the CIN is a form of personal data, Article 186 of the Digital Code states that the processing of such data has to be done after a prior declaration to the Data Protection Authority (DPA). The current reality is that DRC does not have a proper DPA to deal with this, but responsibility has provisionally been given to the telecoms regulator, the ARPTC, which has raised some questions, including over the lack of separation of powers, and the legality of the decision to hand over responsibility to the telecoms regulator (Droit Numérique 2024b).

On whether it is possible for citizens (data subjects) to gain access to the data held about them, Brozeck Kandolo, a Congolese technology law expert shared the following during an interview as part of this study, citing Article 209 of the Digital Code: 'The Digital Code does indeed provide for a right to rectification (in the event of incorrect identity, for example); this is known as the exercise of rights, or the rights of data subjects'. He further shared that the administrators of the CIN are required, per the law, to make sure the people working under their leadership have access limited to the type of data necessary for them to deliver their work, therefore limiting the possibility of a data breach or even sale of data to third parties. The principle of necessity is therefore enforced by the Digital Code, in Article 209. Mr Kandolo concluded by sharing the following:

> *In the event of a breach, the data controller (here, the CIN administrator) may be penalised if their responsibility is proven, particularly if they have collected data unfairly or illegally, or if the use of the data infringes fundamental rights. The penalty is then imposed by the Data Protection Authority [now the ARPTC], as per Articles 255 to 257.*

4. Rights-based tests

4.1 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

According to Ireland's Data Protection Commission, the principle of data minimisation means that 'processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed' (Data Protection Commission n.d.). The next section will respond to the question of whether data minimisation is followed in the process of obtaining the CIN.

Based on the above definition, it is worth reminding the reader of the FGP which was established by Decree No. 22/07 of 2 March 2022 (Leganet 2022). The FGP is meant to serve as the basis for the CIN because, per Article 7 of the 2023 Ministerial Order, 'the CIN is requested after the first registration in the FGP'; this means that each citizen or alien must provide the following data if and where relevant for their registration into the FGP:

> first name, surname, middle name, other names, place and date of birth, birth certificate number, place and date of death, death certificate number, sex, height, eye colour, occupation, marital status, nationality, national ID number, digitised image of their face and fingerprints, digitised image of their signature, home or residence address, data relating to parentage (names, national ID number, place and dates of birth of parents or guardians, and their nationality), the composition of the household, the date of transcription of a decision declaring a person's absence or disappearance (if applicable), details of the registration numbers of the person's various civil status documents, the foreign national's administrative situation, the date and number of the act recognising or acquiring Congolese nationality, the place where the refugee is located, the province of origin, the territory, the sector or chiefdom, the group and the locality, the email address and/or telephone and/or postal contact details. (Decree No. 22/07, Article 9)

A unique National ID Number is given to each physical person after their first registration into the FGP (Article 8). Now, let us look at the type of data needed during the process of obtaining the CIN.

According to Article 4, the CIN contains personal information, some of which is visible to the naked eye (apparent), and some of which can be read electronically or digitally (non-apparent):

- **Apparent personal data**, to be displayed and visible to anyone on the ID, includes the following: the name of the Democratic Republic of Congo, the name of the Ministry of the Interior and Security, the card's name, the card's number, the bearer's first name, their last name, their middle name, their place and date of birth, their sex, their photograph, their domicile and/or residence, the signature of the bearer, the signature of the authority issuing the card, the place and date of issue of the card, the validity of the card and the coat of arms of the Republic.
- **Non-apparent personal data**, to be read electronically, includes the following: National ID Number, fingerprints and/or iris, identity keys, other names, marital status, province of origin, sector and/or chiefdom, group and locality, family composition, occupation, parents' names, nationality and other information authorised by the Ministry of the Interior and Security.

With the above explanation, it is safe to say that the principle of data minimisation is followed because the FGP collects all data and only what is necessary to fulfil the legitimate aim of the ID project is used for the CIN, in addition to a few other elements of data relevant to the CIN.

4.2 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

The current legislation provides no clarity on this. It is therefore very important to point out the necessity for ONIP to deploy this project by making sure the service is accessible across the country, which will require a lot of resources to reach the entire population in urban and non-urban settlements (challenges will include access to electricity and to the internet since this is a digitally led process); if this is not done properly, this could be yet another act of discrimination and would cause trouble and inconvenience. So far, no legislation has spoken about this, but given that the project has not yet been deployed, we hope concrete mechanisms will be put in place to prevent exclusion, and that alternative data collection methods such as unstructured supplementary service data[11] (and any other offline method) could be envisaged, that people living with various forms of disabilities are considered and special provisions made for them, etc.

11 A communication protocol used by GSM cellular phones to interact with their service provider's computers.

Considering the importance of having a national ID, which is the foundational ID system (a very important role as currently played by the Voter Card), Congolese citizens will do whatever it takes to get a CIN in order to avoid facing the inconveniences that come with not having one. Remember, this national ID will be the basis for access to other various functional IDs, and to access various services such as banking, employment, insurance, travel within the country, etc. The Voter Card should not be banned until every citizen has received their CIN.

4.3 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

The relevant legislation presented in the above sections does not provide the justification for the mandatory acquisition of the digital-ID of majors aged 18 and over (per Article 4 of the 2023 Ministerial Order); moreover, as mentioned above, it does not even say much about the legitimate aim of that project other than the fact that it 'establishes the Congolese identity of its holders' (per Article 1 of the 2022 Decree).

However, Article 6 of the 2022 Decree on the FGP speaks about the role of the FGP, which includes the fact that it helps the state to have 'better knowledge of the Congolese population and the foreign population resident in DRC, ensuring the exchange of information on the population with the various government departments, preventing and combating identity fraud and all forms of crime, etc.' That being said and because the FGP and the CIN are linked, this would justify the necessity for every individual to consider registration into the FGP and for Congolese citizens to also obtain their CIN. The relevant legislation does not speak of any fines or penalties against anyone who does not register into the FGP or seek to obtain a CIN.

5. Risk-based tests

At this point in time, it is not possible to assess the risks associated with the deployment of the CIN in DRC since it is the first time it has been tried and we have no knowledge of any risk assessment being conducted prior to the adoption of the regulations in place. However, if possible, a proper risk assessment should be conducted at some point after the effective deployment of the project across the country in order to balance the benefits and the risks associated with its use in a country such as DRC, which is the size of a continent. At the very least, past experiences of the deployment of similar projects, such as the process of registration for the Voter Card, should provide enough knowledge and therefore inform this new project in terms of the logistical aspects, as well as the inclusion of every citizen, as applicable.

6. Conclusion

DRC has not deployed an integrated foundational digital system but the process has started, the president of the country having symbolically received his own digital CIN, as a sample, on 30 June 2023. The CIN project was introduced by the prime minister's 2022 Decree, followed by the 2023 Ministerial Order from the Ministry of Internal Affairs with implementing measures. This project therefore needs to be rolled out by strictly following the Digital Code, which covers data protection legislation in DRC and provides measures to ensure personal data is protected and is managed in a legal, necessary, and proportionate way, as encouraged by international best practices in the sector.

This study notes the interest and the willingness of the various actors involved in progressing with the implementation of a national digital-ID system, and therefore encourages them to ensure the country finally has a foundational ID that will replace the *de facto* ID, the Voter Card, which is no longer legal under the law but is still being used by citizens as the document proving their legal citizenship. This report makes it clear that due to the existence of the many actors involved at national and local levels, as well as foreign contractors or investors, coordination and sound leadership must establish a holistic vision of the project.

There is need for further research, especially when deployment at the national scale starts to better assess the risks associated with this implementation vs the benefits citizens are receiving, and then to suggest improvements, as the deployment continues.

In light of that, the following specific recommendations are made to the various stakeholders:

To parliament (policymakers)

- Ensure there is a proper and specific law that governs the creation, deployment, and use of digital-ID for better regulation rather than leaving it to be governed by a decree or a ministerial order.
- Ensure the deployment is done according to the best practices in the sector, taking into account the size of the country, the preservation of citizens' personal data, etc.
- Measures should be taken to control the actions of the government and, in particular, of foreign actors involved in the project, to ensure all operations are done in citizens' best interests.

- Ensure the creation of an independent body to monitor, regulate, and lead on accountability of all operations related to the deployment of this project. This body should be independent from government, the private sector, and civil society.

To the government (the executive branch)

- Provide the necessary resources to ONIP to ensure the proper deployment of the CIN across the country by making sure no one is left behind.
- Ensure there is clarity and accountability about the various actors (administrators) who will be in charge of accessing and processing the data related to the CIN.
- Internet connectivity and electricity will be essential to ensure coordination of operations across all the offices that will be in charge of the various phases of this project; therefore, there is a need to speed up the deployment of connectivity initiatives across the country.

To civil society (the end users or data subjects)

- Continue playing the role of watchdog by being alert and asking the right questions to the entities in charge of the overall management of this project – because citizens' personal data is at stake.
- Work with the parliament to channel local issues to the legislature for policy updates and better regulations by ensuring digital rights, and the rights of disabled people and rural populations, are protected throughout the process.
- Be prepared and support the process to ensure the national ID card project reaches all corners of the country, so that no one is left behind.

7. Bibliography

7sur7.cd (2014) ***Lumanu recherche un demi-milliard de dollars pour l'ONIP***, 24 November (accessed 12 October 2025)

Agence Ecofin (2012) ***RD Congo: lancement du permis de conduire biométrique***, 2 May (accessed 12 October 2025)

CENI (n.d.) ***FAQ*** (accessed 12 October 2025)

CENI (2016) ***Journal Officiel de la République Démocratique du Congo***, 22 July (accessed 12 October 2025)

Data Protection Commission (n.d.) ***Principles of Data Protection*** (accessed 12 October 2025)

Deutsche Welle (2024) ***En RDC, le feuilleton sans fin des cartes d'identité***, 4 September (accessed 12 October 2025)

Droit Numérique (2024a) ***Ordonnance – loi No 23/10 du 13 mars 2023 portant Code du numérique*** (accessed 12 October 2025)

Droit Numérique (2024b) ***ARPTIC/ARPTC investie des missions de l'Autorité de Protection des Données en RD Congo*** (accessed 12 October 2025)

Jeune Afrique (2017) '**RDC : l'annonce de l'invalidation des passeports semi-biométriques crée la polémique**' , 16 September (accessed 12 October 2025)

Katira, D. (2019) ***Technological Design Choices***, The Centre for Internet and Society, India (accessed 12 October 2025)

Leganet (2022) ***Décret n° 22/ 07 du 02 mars 2022 portant création d'un fichier général de la population en République Démocratique du Congo*** (accessed 12 October 2025)

Leganet (2017a) ***Arrêté ministériel n° 050/CABNPM/MIN/TC/ 2017 du 16 novembre 2017 modifiant et complétant l' Arrêté ministériel n° 409/CABNPM/MIN/TC/ 072/1997 du 31 décembre 1997 portant création de la Commission Nationale de Délivrance des Permis de conduire*** (accessed 12 October 2025)

Leganet (2017b) ***Code de la famille de la République Démocratique du Congo*** (accessed 12 October 2025)

Malonga, S. (2020) ***Titres d'identité du Congo belge à la RDC***, Mbokamosika blog, 2 September (accessed 12 October 2025)

MINAFFET (2025) '**Communiqué de presse**'

NIMC (n.d.) ***Other NIMC Services***, National Identity Management Commission (accessed 12 October 2025)

ONIP (2023) ***Arrêté ministériel No25/CAB/VPM/MININTERSECAC/PKK/255/2023 du 15 Nov 2023 portant mesure d'exécution du Décret No22/08 du 02 Mars 2022 relatif à la création d'une carte d'identité nationale en République Démocratique du Congo*** (accessed 12 October 2025)

ONIP (2022) ***Décret No 22/08 du 02 Mars 2022 portant création d'une Carte d'Identité Nationale en République Démocratique du Congo*** (accessed 12 October 2025)

Presidence.cd (2023) ***Le Président Felix Tshisekedi reçoit sa nouvelle carte d'identité nationale***, 30 June (accessed 12 October 2025)

Radio Okapi (2024) ***Le Gouvernement valide la relance du processus d'obtention du permis de conduire 'biométrique sécurisé' avec 'puce'***, 2 November (accessed 12 October 2025)

SOS Enfants (n.d.) ***État civil en RD du Congo*** (accessed 12 October 2025)

World Bank (n.d.) ***Practitioner's Guide – Types of ID Systems*** (accessed 12 October 2025)

Digital-ID in Egypt: Country report

Afef Abrougui and Mohamed Farahat

 DOI: 10.19088/IDS.2025.057

1. Introduction

With a population of over 116.5 million people, Egypt is the third most populous country in Africa (Galal 2025a) and the second largest economy on the continent (Galal 2025b). It has, over the past years, been pushing a digital transformation strategy to advance economic development and streamline government services (Ministry of Planning and Economic Development 2023). While the adoption of digital identification (digital-ID) is a key element of this transformation plan, as of May 2025, Egypt had still not adopted a national system of biometric digital-ID. In 1996, the national ID card became machine readable, with the addition of a digital barcode (Yosri Ahmed 2012), and the government contracted a French company to produce the biometric ID card (EuropaWire 2014). Government and non-government entities started integrating biometric digital-ID into their services and operations such as in finance, travel, and the voting process.

This push for biometric digital-ID in Egypt is taking place despite a regulatory framework that lacks safeguards to ensure the programme does not infringe on people's privacy and fundamental rights, and exclude their access to essential services. In particular, regulations to ensure protection of people's privacy and data in the biometric digital-ID system, independent oversight over how their information is handled, and the availability of adequate redress and accountability mechanisms are lacking. This report sets out to address the following questions:

- What is the current state of the national ID system and digital-ID in Egypt?
- What is the existing legislative framework relevant to digital-ID in the country and to what extent it is in line with international human rights standards?

The report was compiled using desk research based on reports from civil society groups, media reports, and a review of government documents and regulations. The assessment was based on parameters set by the Centre for Internet and Society for assessing digital-ID programmes against rule of law, rights-based, and risk-based tests.

The first section provides a historical overview of ID systems in Egypt and which groups and communities it excludes. It also delves into preparations for digital-ID in the country and drivers behind it. The second section reviews the legislative framework for digital-ID, to assess to what extent preparations for the digital-ID programme are mandated by law, serve a legitimate aim, and further citizens' ability to access information held about them and to obtain redress. The third section conducts the rights-based tests and assesses

the necessity and proportionality of privacy violations, and provisions for data minimisation and redress. The fourth section reviews whether the existing legislative framework provides appropriate risk assessment.

2. History of ID in Egypt

2.1 Pre-digital-ID era

The identification and registration system in Egypt has undergone several developments from the royal era in the 1920s to date.

Royal era (1922–52)

Carrying ID cards became mandatory for the first time in Egypt in 1944. The law in respect of personal ID cards (Law No. 123 of 1944) applied only to workers in commercial and industrial places, and any other persons as determined by the minister of social affairs. According to Article 3 of the above-mentioned law, an ID card had to contain the name of the holder, and their nationality, religion, age, profession, address, and electoral data.

Republican era (1955–94)

After the transition to the republican era following the 1952 'revolution', holding ID cards became mandatory for all 'residents' over 16 years old in Egypt, with the exception of unemployed women and foreigners, according to Article 1 of Law No. 181 of 1955 relating to personal ID cards. However, unemployed women and foreigners could get a ID card upon request.

In 1960, the Civil Status Authority at the Ministry of Interior was established in accordance with Law No. 260 of 1960 in respect of civil status. It was responsible for issuing civil and ID documents, and keeping citizens' civil records.

Modern era (1994–present)

According to Article 48 of the Civil Status Law (Law No. 143 of 1994), amended by Law No. 165 of 2022, all Egyptian citizens who are 15 years old have to apply for ID. Article 2 of the law tasks the Civil Status Authority with establishing a national database for citizens' data. Citizens are allocated an individual number that stays with them for the duration of their lives (and, indeed, after their deaths). In 2018, the Civil Status Law was amended by Law No. 8 of 2018 by adding a new Article 2(bis) based on which the collection of national ID numbers from beneficiaries by governmental entities became mandatory.

Before addressing the situation of digital-ID in Egypt, it is worth giving a brief overview of the digital landscape in the country. There were 110.41 million mobile (cell) phone subscriptions at the middle of 2024 (MCIT 2024: 2), which

constituted 94 per cent of the total population. In the beginning of 2024, there were 82.01 million internet users in Egypt, when internet penetration was 72.2 per cent (DataReportal 2024). In terms of internet connectivity, the percentage of internet penetration increased in 2024; 83.02 per cent of the population were connected (Statista 2024).

2.2 Current state of national ID and the populations it excludes

As mentioned in the previous section, under the national ID system, each Egyptian is assigned a national ID number at birth. Once they reach the age of 15, all citizens are required to obtain and carry a physical ID card with them. Failure to show an ID card at the request of authorities can result in a fine (Refworld 2016). The card contains a photo, the holder's full name, address, date of birth, religion, gender (male or female), and job (Debch and Taha 2022). A range of data and documents are needed to obtain an ID card, which include a photo, a birth certificate, verification of address by means of lease agreement or an electricity, gas, or water bill, a certificate proving academic qualifications or a letter from the applicant's current employer or, for students, educational institution at the time of application, and for those who are married, a copy of their marriage certificate (Refworld 2016). In 1996, a barcode was added to the card (Yosri Ahmed 2012).

Egyptian authorities have been taking steps to address forms of exclusion in the national ID system (for instance, discrimination on the basis of gender or religion); however, exclusion still persists (Creech, Modugno and Pitarra 2022). In 2006, amendments to the nationality law made it possible for women to transmit citizenship to their children, paving the way for children born to foreign fathers to obtain an ID number and exercise political rights, access a wide range of services, and benefit from government welfare programmes (*ibid.*). Nonetheless, those born to an Egyptian mother and a foreign father before 2004 – when Nationality Law No. 26 of 1975 was amended – were not automatically granted citizenship and continue to face burdensome procedures to apply for Egyptian nationality (*ibid.*).

Those not affiliated with the three Abrahamic religions (Judaism, Christianity, and Islam), particularly Bahá'ís, have for years struggled to obtain an ID, and despite a 2009 government decree to issue them an ID by leaving the religion line empty, they still face discrimination in the national ID system (Minority Rights Group 2025). For instance, they still face obstacles in obtaining marriage certificates, which are necessary for obtaining an ID for married people, and for registering the birth of a child (Creech *et al*. 2022). A birth certificate is a key document to obtaining an ID.

The ID system further excludes refugees and asylum seekers. The main path for an ID document for these groups is through registration with or recognition by the United Nations Refugee Agency (UNHCR), a complicated and burdensome process requiring travel to UNHCR offices in Cairo or Alexandria, and provision of ID documents, which some refugee groups – such as stateless refugees – commonly lack (Ayoub and Twefik 2021). Even for registered refugees, their UNHCR-issued identity card is not always recognised by government officials, making it difficult for them to travel, work, and access services (Creech *et al*. 2022).

Bedouin populations, particularly those living outside urban areas, lack ID documents, exposing them to increased risks of statelessness and marginalisation. For instance, for those living in remote areas in Sinai, travelling to civil registration offices to register births in time is costly (Minority Rights Group 2025), and it can be dangerous because of security checkpoints and conflict in North Sinai (Creech *et al*. 2022).

2.3 Preparations for biometric digital-ID

In its current state, the national ID card is not suitable for recording biometrics (Privacy International 2019). However, the government has been laying the groundwork for a biometric digital-ID system for over a decade. In 2014, it signed a multi-year contract with French company Morpho, a subsidiary of Safran, to produce a new national biometric digital-ID, embedded with a smart chip (EuropaWire 2014). While it remains unclear why 11 years later biometric digital-ID has not been implemented, Egypt has faced challenges with its national ID system, including registration of citizens, particularly women and those living in rural areas. With a population that is expected to surpass 120 million in 2025, and projected to continue to grow beyond 2050, the system could face increased pressures, particularly in registering new births in densely populated areas (Abdelghany 2025).

In the meantime, biometric digital-ID has been rolled out for specific areas such as voting and travel. During the constitutional referendum and presidential election of 2014, (EuropaWire 2014) and parliamentary elections of 2015 (Identity Week 2015), the state deployed French multinational Safran's MorphoTablet, for enrolment and registration of voters, using touchscreen tablets to capture facial biometrics and fingerprints.

In December 2016, the Egyptian civil aviation authority started implementing a biometric ID system at airports 'to better monitor the activities of employees, and automate their entrance and exit of the airport' (Privacy International 2019). Cairo International

Airport also installed e-passport gates that used facial recognition technology to authenticate the identity of travellers (Lee 2015).

Table 4: The road to biometric digital-ID in Egypt

Year	Milestones
1940s	First paper personal ID cards issued in Egypt; carrying an ID became mandated for workers (Bab Masr 2020)
Early 1950s	The look of the paper personal ID cards changed when Egypt became a republic in 1953 and additional data about the holder's religion was added (*ibid.*)
1990s	The Civil Status Law (Law No. 143 of 1994) was adopted in 1994; the first cards with a barcode were issued in 1996 (Yosri Ahmed 2012) – these are the same cards that remain in use today
2010s–2020s	The Egyptian government contracted a company for a biometric digital-ID card equipped with a smart chip in 2014; it also started implementing biometric digital-ID in specific areas such as for elections and in airports*

Source: Author's own; * EuropaWire (2014).

In finance, the Financial Regulatory Authorities issued a number of decisions in 2023 to regulate the use of digital-ID in non-bank financial services provided by fintech companies (Masaar 2025). Decision 140 of 2023, for example, mandated the use of biometrics such as facial recognition or fingerprint scanning by customers seeking to create a digital-ID to access non-bank fintech services and conduct transactions (*ibid.*). As of May 2025, it did not appear that customers of banks needed digital-ID to conduct banking transactions or open accounts; however, the Central Bank of Egypt in 2024 established the Digital Financial Identity Company, tasked with enabling digital-ID for banking purposes, including opening accounts without visiting a physical branch (Arab Finance 2024).

In November 2024, the traffic department at the Ministry of Interior announced the issuance of a new digital driving licence (Alayam 2024).

For years, the government has been implementing mandatory SIM card registration that makes the provision of a person's national ID a precondition of mobile phone use. In late January 2025, in a meeting between the parliamentary telecommunication commission and the National Telecommunications Regulatory Authority, a member of parliament said 'that no phone will be activated until the ministry of interior verifies the identity of the user and their data and that there will not be a phone we don't know its owner' (Ghareeb 2025). There is an existing digital-ID app allowing Egyptians to access government services. To register, users need their ID number and

mobile number linked to their ID. The Ministry of Finance and the Ministry of Communications and Information Technology also launched a system for Egyptians travelling back to Egypt with imported phones to register the phones within three months using an app called Telephony (Nawar 2025).

2.4 Drivers of digital-ID

The push for the adoption of biometric digital-ID comes as part of Egypt's digital transformation strategy, a key component of the country's Vision 2030 (Ministry of Planning and Economic Development 2013) and Egypt ICT 2030 Strategy (Ministry of Communications and Information Technology n.d.b).

At first glance, digital transformation, including the adoption of digital-ID, may be seen as an entirely positive step towards improving efficiency in administration and citizens' access to public services, combating corruption and security threats, preventing fraud, and promoting good governance. However, there are also political drivers in President Abdel Fatta El-Sisi's Egypt, where advanced technologies such as smart city tech and facial recognition have become essential elements in the country's surveillance apparatus to help maintain regime power, and crack down on dissent and early signs of civic action such as protests and strikes (Abrougui 2025).

With digital-ID linked to SIM cards, and potentially bank account numbers at a later stage, it will be even easier for the regime to track citizens and their data. This potentially includes tracking sensitive data about their health and finances that can be weaponised against them; for instance, by denying them access to services, or to persecute them. The authorities keep an eye on the finances of non-governmental organisations and their workers, with repercussions for their human rights work – several human rights defenders have had their personal assets confiscated in the past, (Amnesty International 2016). A 2023 report by Human Rights Watch (2023) found that: 'The Egyptian authorities in recent years have systematically refused to provide or renew the ID documents of dozens of dissidents, journalists, and human rights activists living abroad… The refusal is apparently intended to pressure them to return to near-certain persecution in Egypt'.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

According to Article 48 of Civil Status Law, all Egyptian citizens who are 15 years old have to apply for an ID. Under Article 2 of the same law, the Civil Status Authority maintains a national database of citizens' data based on their individual ID numbers. The law was amended by Law No. 8 of 2018, which obligated government entities to obtain the data of linked to the national numbers of beneficiaries of government services, in accordance with Article 2(bis). However, each entity would only see data relevant to providing that particular service; they would not have access to all of the data about an individual citizen. Article 13 of the same above-mentioned law states:

> Data and information related to the civil status of citizens contained in records, books, computers, or attached storage media are considered confidential, and their data may not be viewed or obtained except in the cases stipulated by the law and in accordance with its provisions.

The same article adds that the collected information and data are considered a national secret.

Article 76 of the law mentions that: 'Anyone who breaches or attempts to breach the confidentiality of data, information or statistics collected in any way shall be punished with temporary hard labour.'

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Although, the law does not explicitly contain a specific legal provision stating its aim, the legitimate aim could implicitly be derived from some specific provisions. Article 2 of the Civil Status Law mandates the Civil Status Authority to establish a national database for citizens' data based on their individual ID numbers. A legitimate aim is to ensure the validity of the ID data and information when dealing with different entities, in accordance with Article 12 of above-mentioned law. This article states that 'the recorded data is considered correct unless proven otherwise, and all governmental and non-governmental agencies have

to recognize this data'. In addition, Article 50 clearly states that 'ID cards are a proof of the accuracy of the data they contain when they are usable and valid' and that 'governmental or non-governmental entities should not refrain from using them to prove the identity of the holder.'

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law clearly define the nature of data that can be collected? Do individuals have rights to access, confirmation, correction and opt out?

Articles 1, 2, and 13 of the Civil Status Law state that all civil status databases including the national ID database are considered confidential national secrets. Only the Civil Status Authority at the Ministry of Interior has the power as specified by the law to use, manage, and connect to ID databases. According to Article 13, on permission from the head of the Civil Status Authority the national ID database may be 'viewed and published' for academic purposes and in the national interest; otherwise, private actors or other government actors may not access, use, manage, or connect to the database.

Does the law clearly define the nature of data that will be collected?

In principle, collecting data and information related to political tendencies, beliefs, or criminal records is prohibited except in cases specified by law, in accordance with Article 64 of the Civil Status Law. Article 33 of the executive regulation states that The ID card contains the following information about each citizen: issuing office; national ID number; full name (first four names, at least); place of residence; gender; religion; occupation; spouse's name (for married women); and card expiration date. This means that all collected data should reflect the data that appears on the ID card. In practice, according to the ID application form and in addition to the above-mentioned data, the authorities collect data and information linked to the marital status, parents' names, parents' birthdays and place of birth, and academic background data. According to the same Article 33 of the executive regulation, civil registration offices collect biometric data such as fingerprints and a photo of the applicant, and save them in the computer system.

Do individuals have rights to access, confirmation, correction and opt out?

Regarding ID data, individuals do not have any right to access the information and at the same time they have no right to opt out of providing the information because the data and information are submitted to

the authorities to establish their national identity and nationality for the purpose of issuing the mandatory national ID card. However, individuals do have a right and obligation to make sure that the collected data is up to date. According to Article 53 of Civil Status Law 143. If any of a citizen's ID card data or their civil status data changes, within three months from the date of the change, they must apply to the Civil Registry Department of the district where they reside to update this data. In some cases, the ID card may contain inaccurate information or data due to incorrect information or data in one of the supporting documents such as the birth certificate, marriage certificate, or academic certification. In this case and according to Article 46 of the Civil Status Law, individuals have a right to submit a request to correct or change the incorrect data and update the ID data after the correction has been processed.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

Personal Data Protection Law No. 151 of 2020 (PDPL) enshrines the right of data subjects to complain and seek compensation in cases of data protection violations. Article 33 of the PDPL states that data subjects can resort to the judiciary in cases where 'their right to personal data protection has been violated or breached' and they have been prevented from 'fulfilling their rights'. Moreover, Article 35 of the same law stipulates that 'without prejudice to the right of the injured party to compensation, the crimes stipulated in the following articles shall be punished with the penalties prescribed for them'. However, Article 2 of the PDPL states that its provisions do not apply to national security authorities, which include the Ministry of Interior (Fatafta 2020). Since the Civil Status Authority is a Ministry of Interior unit, this can complicate citizens' ability to seek and obtain redress for privacy-related violations in the digital-ID system.

In addition, although there is no specific law regarding violations or harm specifically for digital-ID systems, according to Egyptian civil law and in accordance with rules of tort, a person has the right to seek compensation against harm they have incurred. Article 163 of the Civil Code states that:

> Any fault which causes damage to another obliges the person who committed it to make compensation. A damaged person has to file a lawsuit asking for compensation. To be eligible for redress and compensation the damaged person has to establish 1. the fault and violation has occurred 2. the damages and harms that a person suffers from 3. the causality between the harm and damages.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

In terms of accountability mechanisms, Article 74 of Civil Status Law No. 143 of 1994 states that:

> anyone who accesses, attempts to access, obtains, or attempts to obtain data or information contained in records, computers, or storage media attached to them, or changes them by adding, deleting, cancelling, destroying, or tampering with them in any way, or broadcasts or discloses them in circumstances other than those stipulated by law and in accordance with the procedures stipulated therein, shall be punished by imprisonment for a period not exceeding six months and a fine not exceeding five hundred pounds, or by either of these two penalties. If the crime is committed against collected data, information, or statistics, the penalty shall be imprisonment.

Article 75 further states that:

> anyone who disrupts or damages the civil status information network – ID system is included – , or any part thereof, due to negligence, recklessness, lack of caution, or failure to comply with laws, regulations, and executive regulations shall be punished by imprisonment for a period not exceeding six months and a fine of not less than two hundred pounds and not more than five hundred pounds, or by either of these two penalties.

Article 76 adds that: 'Anyone who breaches or attempts to breach the confidentiality of collected data, information, or statistics in any way shall be punished by temporary hard labour'.

Furthermore, Article 23 of Anti-Information Technology Crimes Law No. 175 of 2018 states that:

> Anyone who uses the internet or any information technology device to unlawfully access bank numbers, data, cards, services, or other electronic payment tools shall be punished by imprisonment for a period of no less than three months and a fine of no less than 30,000 Egyptian pounds and no more than 50,000 Egyptian pounds, or by either of these two penalties. If the person uses the internet or any information technology device to unlawfully access bank numbers, data, cards, services, or other electronic payment tools, the penalty shall be imprisonment for a period of no less than 50,000 Egyptian pounds and no more than 100,000

> Egyptian pounds, or by either of these two penalties. The penalty shall be imprisonment for a period of no less than one year and a fine of no less than 100,000 Egyptian pounds and no more than 200,000 Egyptian pounds, or by either of these two penalties, if the person thereby seizes, for himself or for another, those services or the property of others.

The above-mentioned criminal accountability mechanism does not prevent individuals from seeking available redress mechanisms, in particular, their right to compensation according to Civil Code and Article 35 of the PDPL.

While the law establishes penalties for unauthorised access to data and networks, independent oversight of governing bodies is lacking. In particular, the PDPL provides for the future establishment of a data protection authority, the Personal Data Protection Centre. However, the centre will lack the independence required for it to achieve its mandate, including overseeing the law's implementation and investigating complaints. In fact, its board will be appointed by the minister of communication and information technology and will include representatives from the Ministry of Defence, Ministry of Interior, and intelligence services (Fatafta 2020).

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

As the governing law of national IDs was issued in 1994 and before the strategies and processes of digital transformation, consequently the Civil Status Law of 1994 did not explicitly specify the proposed purposes of the digital-ID. The current situation in Egypt shows a lack of regulation of digital-ID, in spite of digital-ID becoming a fact and existing in people's daily practices, especially for online banking, use of digital wallets and money transfer apps, and accessing government services platforms such as Digital Egypt.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

The range of data and documents collected to issue an ID card, including about applicants' religion and profession, are neither necessary nor proportional, as they are not necessary for issuing an ID card and can even pose risks of discrimination. For instance, Egyptian authorities only provide three possible options for religious data, which are Jewish, Christian, and Muslim. All other religious groups or those not affiliated with any religion in effect had to input incorrect data (Egyptian Initiative for Personal Rights 2022) in order to be issued an identity card. But since 2009, those not belonging to the three Abrahamic religious groups recognised by the state have been able to be issued identity cards with a dash ('–') to indicate they do not belong to any of these groups (Refworld 2016).

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

As mentioned above, collection of data and documents is not minimised; indeed, the collection of certain kinds of data (such as about one's profession and religious affiliation) does not serve a legitimate purpose. No clear limitations in the Civil Status Law and no data retention periods have been established.

A 'Secured and Smart Documents Complex' at the Ministry of Defence, established by a decision by the president (Decision number 232 of 2021), is tasked with preserving biometric data 'from destruction and illegitimate processing' (Manshurat 2021). The complex is tasked with securing official documents 'pertaining to natural persons' civil, social and financial situations from birth until death' and biometric data defined as 'data that identifies a person in a way that distinguishes his/her identity from others and guarantees non-repetition' (*ibid.*). This civil data, financial data, social data, and biometric data are all processed by the complex; however, no limits for data minimisation are in place (*ibid.*). The decision, further, does not specify data retention periods (*ibid.*).

While the government plans to integrate fingerprints into the national ID system (El-Din 2021), it is unclear what other biometrics will be collected to issue the biometric ID card. Biometric data is also collected for single functions such as to obtain a new driving licence (Alayam 2024), for non-bank financial transactions, and to vote in elections.

Finally, while Egypt has a data protection law that establishes limits for data processing and retention, the law's provisions do not apply to national security authorities (Fatafta 2020), which means that they do not apply to the Civil Status Authority at the Ministry of Interior or the Secured and Smart Documents Complex at the Ministry of Defence.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

There is a lack of adequate limitations on access to personally identifiable information.

Article 11 of the Civil Status Law grants access to 'directors of civil status service, and their auxiliaries from officers, heads of departments, and civil servants' to civil registers to implement the provisions of the law, without specifying each purpose. Article 13 of the same law states that civil status information and databases are 'considered a national security secret and should only be viewed or published for national or scientific interests and after written consent from the director of the civil status service or his deputy'. These exceptions are vague, particularly when it comes to national security, a pretext often used by the authorities to infringe on fundamental rights, including the right to privacy.

While the Secured and Smart Documents Complex is tasked with 'securing' official documents, biometric data, and the digital-ID system, it is unclear what measures it has in place (if any) to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors. Additionally, as mentioned above, the data protection law does not apply to the complex and the Civil Status Service at the Ministry of Interior.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

It is unclear if the government will make access to entitlements or services dependent on digital-ID in the future. However, several marginalised groups already face obstacles to obtaining a national ID, which is fundamental to daily life in Egypt (Creech *et al*. 2022).

As explained previously, exclusion particularly affects refugees, asylum seekers, and their descendants, those with an Egyptian mother and a foreign father, Bedouin and rural populations, and Bahá'ís, all of whom face obstacles in obtaining an ID (*ibid.*).

Bahá'ís and those belonging to religions not recognised by the state have a dash ('–') for religion on their ID cards. Further, Egypt does not recognise conversion from a recognised religion to another religion such as the Bahá'í faith, which can complicate applicants' ability to enrol in the ID system or obtain a card (Minority Rights Group 2025). Bedouins who live in very remote areas, with no close access to civil registration offices, and stateless tribes both face challenges to enrolling in the national ID system and accessing essential services (*ibid.*).

The national ID card offers only two options when it comes to gender (male or female), excluding gender non-binary people from listing the gender they identify with. According to Minority Rights Group (*ibid.*), 'transgender individuals struggle to get their national ID cards corrected with their new gender' and the approval of the Egyptian Medical Syndicate's Sex Reassignment Committee is required prior to changing their gender on the card.

Additionally, the authorities in Egypt have weaponised the national ID system against dissidents in the diaspora and their families. For instance, Egyptians living in Türkiye, even those not part of the opposition, said they were asked to provide their social media accounts and explain why they had left the country, in order to receive official documents such as birth certificates, IDs, and passports (Mahmoud 2023). In some cases, authorities stripped dissidents of their nationality, rendering them stateless (Egyptian Front for Human Rights and Egyptian Human Rights Forum 2024).

The government has attempted to close the gender gap in ID enrolment. In 2022, a joint government campaign was launched by the National Council for Women and the United Nations, with the aim of enrolling 2 million women in the national ID system (UN Women 2012). The initiative at that time estimated that 4 million women – specifically those living in poverty, with disabilities,

and in rural areas – did not have an ID card (*ibid.*). The council continued to register women and issue them ID cards in 2025 (Al-Sharqawi 2025).

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

The mandatory use of national ID is based on the Civil Status Law (Law No. 143 of 1994). In 2022, the parliament amended Article 48 to lower the minimum age required for obtaining an ID card to 15 years from 16 (Nawar 2025). As a result, under Article 50 of the same law, everyone aged 15 and older is required to carry their ID with them and to show it to representatives of public authorities when asked to do so. Article 56 further requires those representing government and non-governmental entities not to provide services or receive anyone as an employee, consumer, worker or student unless they provide a valid identity card. While the mandatory nature of ID is justifiable in some cases such as to obtain a passport and travel abroad, and to conduct large financial transactions, Egyptian law sets very broad conditions that make it impossible for people, including children who have not reached the age of majority of 18, to access a wide range of basic services and exercise fundamental rights without an ID. This includes enrolling in an education programme, moving freely within the country, obtaining a job, and conducting basic administrative and financial transactions (Egyptian Initiative for Personal Rights and Human Rights Watch 2007).

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

Egypt's Personal Data Protection Law No. 151 of 2020 (PDPL) establishes a legal framework for conducting risk-based assessments of digital-ID systems. While the law provides neither specific provisions addressing digital-ID nor a detailed methodology for such assessments, it outlines several principles and requirements that align with risk-based testing approaches. The PDPL includes provisions on 'Licensing Requirements for Data Controllers and Processors', an 'Obligation to Implement Appropriate Technical and Organizational Measures', 'Data Protection Officer (DPO) Appointment', and 'Breach Notification Requirements', in addition to provisions that emphasise legitimacy and proportionality in the collection and processing of personal data, including digital-IDs.

The Parliament of Egypt promulgated the PDPL in 2020. According to Article 4, the minister of communication and information technology was due to issue the executive regulation within six months; the executive regulation has not been issued yet. Article 19 of the law provides for the establishment of the Personal Data Protection Centre, which would be responsible for protecting personal data. The centre had not been established at the time of writing. Despite the PDPL being in place, it is not effective due to the lack of both executive regulation and the authority responsible for protecting personal data.

5.2 Differentiated approach to risk

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

The PDPL incorporates several privacy-by-design principles governing personal data, including digital-IDs, aimed at minimising the risks and potential harms associated with data breaches. According to Article 2 of the law, collecting, processing, and disclosing personal data shall only be done with the explicit consent of the data subject. Articles 3 and 6 emphasise the legitimacy of collecting and processing personal data; processing is lawful if it takes place with the consent of the data subject. Article 4 ensures that the data controller is obligated not to take action that leads to personal data being publicly accessible, and to take technical and

organisational measures to protect personal data. According to Article 4, the data controller is obligated to erase personal data after the legitimate purpose of its use comes to an end. If any breach occurs to personal data, the controller and processor shall notify the Personal Data Protection Centre within 72 hours, in accordance with Article 7. To minimise the harms from data breaches, Article 8 states that the controller and processors are obligated to hire a DPO; among other responsibilities, according to Article 9 the DPO is responsible for periodically monitoring and evaluating data protection systems and preventing data breaches. According to Article 19, the Personal Data Protection Centre is responsible for issuing licences, permissions, and measures related to protecting personal data. According to Article 26, collecting, processing, and keeping data should be licensed.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

While a specific law on digital-ID does not exist, the PDPL is used to regulate some aspects of digital-ID. The PDPL includes a specific provision that emphasises the proportionality principle in relation to the collection and processing of personal data. According to Article 4 of the PDPL, personal data must be collected for specified, explicit and legitimate purposes, and not processed in a manner inconsistent with those purposes. The same article adds that personal data must be adequate, relevant, and limited to what is necessary in relation to those purposes. However, the PDPL does not include provisions for either data classification or risk categorisation.

6. Conclusion

As of May 2025, Egypt had still not implemented a biometric digital-ID programme. However, digital-ID is becoming increasingly integrated into single functions such as finance, banking, and access to government services. In the meantime, authorities are taking steps to pave the way for the adoption of biometric digital-ID; for instance, through the introduction of amendments to the Civil Status Law and the establishment of the Secured and Smart Documents Complex to store biometric data. The rule of law tests, rights-based tests, and risk-based tests identified shortcomings in Egypt's national ID system, which could lead to privacy violations and exclusion as the government moves ahead with the implementation of its digital-ID programme.

A comprehensive regulatory framework is lacking to prevent mission creep, and while the law defines a range of data that can be collected as part of the national ID system, citizens lack rights to access their data and opt out of data collection. The Civil Status Law further establishes criminal punishments for unauthorised access to civil data or which causes damage to the civil information network. Furthermore, the incomplete personal data protection framework has directly adversely affected the digital-ID system.

The programme in its current state does not pass the test of necessity and proportionality as the collection of a range of data such as about people's religion and profession in order to issue an ID does not serve a legitimate aim. Additionally, there is a lack of adequate limitations on access to personally identifiable information collected for civil status purposes. While ID is mandatory under the Civil Status Law to access a wide range of services and entitlements, several groups and populations, including refugees and asylum seekers and their descendants born in Egypt, Bahá'ís, people with an Egyptian mother and a foreign father, and Bedouin and rural populations, face obstacles in obtaining official documents such as birth certificates and IDs, putting them at risk of exclusion. Yet, there is no evidence the government is putting adequate mechanisms in place to address and prevent such exclusion in relation to digital-IDs.

Finally, while the PDPL establishes a legal framework for conducting risk-based assessments, it does not provide specific provisions addressing digital-ID or a detailed methodology for such assessments. Additionally, the legislative framework remains largely silent on other potential risks to accessing welfare and other socioeconomic rights, and the right to non-discrimination.

Policy recommendations for government

- Issue the executive regulation of the PDPL, which will include more details about implementation.
- Establish an independent data protection authority to oversee processing of personal data, and provide redress mechanisms for those enrolled in the digital-ID programme.
- Amend Personal Data Protection Law No. 151 of 2020 and Civil Status Law No. 143 of 1994 to add a specific provision on digital-ID.
- Include safeguards for the processing of data by government entities including in relation to the digital-ID programme. These safeguards should include minimisation of data collected, limits on data sharing and retention, and options for data subjects to control and access their data.
- The government should refrain from launching a biometric digital-ID programme until it has conducted a robust and comprehensive risk assessment to understand the negative impacts of such a programme on fundamental human rights, including the rights to privacy and the right to non-discrimination. The assessment should also review potential impacts on the most vulnerable groups in Egypt, including minorities, women, and those living in poverty and in rural areas.

Recommendations for civil society

- Civil society should raise societal awareness about digital-ID and its impacts.
- It should also monitor current efforts to introduce digital-ID in Egypt by producing policy briefs and research papers on its deployment and impacts.

7. Bibliography

Abdelghany, A. R. A. (2025) ***Strategic Planning and Future Projections for Reforming Egypt's National Identification Number Registration System (2025–2050)***, DOI: 10.13140/RG.2.2.22878.34886 (accessed 12 October 2025)

Abrougui, A. (2025) '**Phishing, Spyware, and Smart City Tech: Surveillance in Sisi's Egypt**', in T. Roberts and A. Mare (eds), *Digital Surveillance in Africa: Power, Agency, and Rights*, London: Zed Books, DOI: 10.5040/9781350422117.ch-3 (accessed 10 February 2025)

Alayam (2024) '**بحاص ةيوه فشك ت ةينورتكلإ ةحير ش .2025 ةديدجلا ةصاخلا ةدايقلا ةصخر لكش ةرايسلا**' [*The Look of the New Driving Licence 2025*] (accessed 9 February 2025)

Al-Sharqawi, N. (2025)'**ةديس 127 ـل نانجرملاب يموقلا مرقلا تاقاطب جارختسا . «كقوقح كتقاطب» نمض (روص) ةيردنكسإلا يف ةزتنمرلا ـب**' ['As Part of 'Your Card, Your Rights', 127 National Number Cards Issued for Free for 127 Women in Al-Montazah in Alexandria (Images)'], *Almasry Alyoum* (accessed 29 May 2025)

Amnesty International (2016) ***Egypt: Planned Asset Freezes are Government's Latest Tool to Eradicate Civil Society***, 18 March (accessed 29 May 2025)

Arab Finance (2024) ***CBE to launch Digital Financial Identity Company in H2 2024***, 5 August (accessed 15 May 2025)

Ayoub, M. and Tewfik, N. (2021) '**Preventing Statelessness Among Migrants and Refugee Children in North Africa: The Case of Egypt**', *Cairo Studies on Migration and Refugees* 15 (accessed 1 June 2025)

Bab Masr (2020) '**مرلا عرلا يف ةيلئاعلا قاطبلا اومدختسا نمر لوأ ءامدقلا نوي رصملا**' [*Old Egyptians the First in the World to Use Family Cards*], 28 July (accessed 29 May 2025)

Creech, C.; Modugno, H. and Pitarra, R. (2022) ***The Campaign to End Statelessness in Egypt***, Boston University School of Law (accessed 16 May 2025)

Data Reportal (2024) ***Digital 2024: Egypt***, 23 February (accessed 12 October 2025)

Debch, H. and Taha, M. (2022) '**تاوطخلاو راعسألا .يموقلا مرقلا ةقاطب نأشب ةيلخادلا نمر ديدج رارق طورشلاو**' ['A New Decision from the Ministry of Interior about the National Number Card Prices, Steps and Procedures'], *Almasry Alyoum* (accessed 13 May 2025)

Egyptian Front for Human Rights and Egyptian Human Rights Forum (2024) ***Transnational Repression: Targeting Egyptian Human Rights Defenders In The Diaspora*** (accessed 29 May 2025)

Egyptian Initiative for Personal Rights (2022) ***Citizens Without Valid Identity Papers, Marriage Certificates, or Burial Places*** (accessed 29 May 2025)

Egyptian Initiative for Personal Rights and Human Rights Watch (2007) ***Prohibited Identities: State Interference with Religious Freedom*** (accessed 9 February 2025)

El-Din, M. (2021) 'Efforts to Link Egypt's National ID System With Finger-Vein Recognition Technology', *Daily News Egypt*

EuropaWire (2014) ***Morpho (Safran) Signs Multi-year Contract with Arab Organisation for Industrialisation Electronics to Produce the Egyptian National eID Card***, 3 December (accessed 9 February 2025)

Fatafta, M. (2020) ***Egypt's New Data Protection Law: Data Protection or Data Control?***, Access Now (accessed 12 October 2025)

Galal, S. (2025a) ***African Countries with the Largest Population as of 2024***, Statista (accessed 21 April 2025)

Galal, S. (2025b) ***African Countries with the Highest Gross Domestic Product (GDP) in 2024***, Statista (accessed 21 April 2025)

Ghareeb, M. (2025) '**القومي للاتصالات»: تفعيل تطبيق «الهوية الرقمية» خلال شهر ولن يكون لدينا تليفون لا نعرف مالكه**' ['Telecom Regulator: Digital ID App Will Be Implemented Within a Month and There Will Not Be a Phone We Wouldn't Know Its Owner'], *Almasry Alyoum* (accessed 9 February 2025)

Hamdy, N. N. (2004) '**The Internet and Egypt's National Development**', *Global Media Journal* 3.5 (accessed 12 October 2025)

Human Rights Watch (2023) ***Egypt: Dissidents Abroad Denied Identity Documents***, 13 March (accessed 9 February 2025)

Identity Week (2015) ***MorphoTablet Deployed for Egyptian Elections***, 17 December (accessed 9 February 2025)

Kame, S. (2001) 'The Information Society in Egypt', in G. Nulens, N. Hafkin, L. Van Audehove and B. Cammaerts (eds), *The Digital Divide in Developing Countries: Towards as Information Society in Africa*, 1st ed., Brussels University Press

Katira, D. (2019) ***Technological Design Choices***, The Centre for Internet and Society, India (accessed 10 May 2025)

Lee, J. (2015) ***Cairo International Airport Installs Epassport Gates***, BiometricUpdate.com, 18 May (accessed 9 February 2025)

Mahmoud, S. (2023) '**Depriving Dissidents of Identity Documents: Egypt's Latest Chapter in Rights Violations**', *Raseef22*, 31 March (accessed 12 October 2025)

Manshurat (2021) ***Decision Number 232 of 2021 by President of the Republic on Establishing a Secured and Smart Documents Complex***

Masaar (2025) ***Privacy Rights in the Fintech Era: Examining the Egyptian Legal Framework And Its Implementation Hurdles***, 15 April (accessed 16 May 2025)

MCIT Egypt (2025) **مصر الرقمية عن الإدارة** [*Digital Egypt*] [mobile app] (accessed 16 May 2025)

Migration and Passport and Nationality Department (n.d.) **عن الإدارة** [*About Management*], Ministry of Interior (accessed 12 October 2025)

Ministry of Communications and Information Technology (2004), ***ICT Indicators Bulletin***, June, (accessed 12 October 2025)

Ministry of Communications and Information Technology (n.d.a) ***Digital Egypt*** (accessed 9 February 2025)

Ministry of Communications and Information Technology (n.d.b) ***Egypt ICT 2030 Strategy*** (accessed 9 February 2025)

Ministry of Planning and Economic Development (2023) ***The National Agenda for Sustainable Development: Egypt's Updated Vision 2030*** (accessed 9 February 2025)

Minority Rights Group (2025) ***MRG Urges Action on Minority and Indigenous Rights in Egypt***, 20 January (accessed 12 October 2025)

Nawar, B. (2025) '**Egypt Imposes New Rules on 'Importing' Mobile Phones**,' *Egyptian Streets*, 2 January (accessed on 9 February 2025)

Privacy International (2019) ***State of Privacy Egypt***, 26 January (accessed 8 February 2025)

Refworld (2016) ***Egypt: Information on National Identity Cards Including Appearance; Requirements and Procedures to Obtain the Card, and Whether Documents Required to Apply for a Card Can Be Obtained by a Proxy (2010-June 2016)***, 26 May (accessed 12 October 2025)

Statista (n.d.) ***Digital and Connectivity Indicators – Egypt*** (accessed 12 October 2025)

UN Women (2012) ***The Women Citizenship Initiative Will Ensure Citizenship Rights to Two Million Women in Egypt***, 10 July (accessed 21 April 2025)

Yosri Ahmed, A.M. (2012) '**The Egyptian Machine Readable Passport and ID Card: Evaluation of Their Compliance to ICAO and ISO/IEC Standards**', *Keesing Journal of Documents & Identity 37* (accessed 29 May 2025)

Digital-ID in Tunisia: Country report

Yosr Jouini

 DOI: 10.19088/IDS.2025.058

1. Introduction

This report assesses the current state of Tunisia's digital identification (digital-ID) by examining its legislation and governance, evaluating its alignment with the rule of law, and conducting rights-based and risk-based analyses. Specifically, it addresses: what the current state of digital-ID in Tunisia is; what legislative framework and governance mechanisms exist; and how these elements satisfy rule of law, rights-based, and risk-based tests.

In recent years, Tunisia has been actively digitising public services, driven by political, societal, and economic interests (Paradigm Initiative 2025). This is evident in national strategies and budgetary support for projects such as the digital-ID, promising to modernise identity verification and service access. Developed during significant political shifts – including political regime change, a new constitution, and ongoing instability – the digital-ID project has sparked debate regarding privacy, surveillance, and exclusion (Access Now 2023). As the project unfolds, it is becoming increasingly important to understand how political dynamics influence its governance and legal framework. Although planning is advanced and enabling legislation is in place at the time of writing (May 2025), the first biometric digital-ID card has not yet been issued.

The report relies on the Centre for Internet and Society (CIS)'s framework for the evaluation of digital-ID (Bhandari, Trikanad and Sinha 2020). It is structured as follows. First, context is provided by examining the history of ID systems in the country, assessing the current level of digital penetration and the existing ID system overview. Next, an evaluation of the preparatory digital-ID law is conducted through three key lenses: examining the clarity and comprehensiveness of governing legislation using rule of law tests; analysing the impact on citizen rights using rights-based tests; and identifying potential risks and mitigation responses using risk-based tests. The report concludes by presenting concluding observations and recommendations.

1.1 Pre-digital-ID era

The foundation of Tunisia's modern ID system dates back to the early twentieth century, before French colonial rule, when the Beylical Decree of 28 December 1908 – issued by the Bey of Tunis (a title designating the monarchical head of state in Tunisia from 1705 to 1957) – made registration of births and deaths mandatory for all Tunisians. This measure laid the groundwork for the civil registration system, which was further expanded after independence (UNFPA 2021).

Post-independence (1956), Tunisia established a legal framework for civil status, starting with Law No. 1957-3 (Republic of Tunisia 1957), which reorganised civil registration and set recording guidelines. Subsequently, several amendments have been made to modernise the system, including efforts to digitise civil registration processes.

Tunisia's National Identity Card (CIN) was first introduced with the adoption of Law No. 68-24 (Republic of Tunisia 1968). Initially a paper document that included a photograph, a unique ID number, and personal information such as name, date and place of birth, parents' names, and address, in 1993 the CIN became mandatory for citizens aged 18 and over under Law No. 27 of 1993, requiring them to present it to security officers upon request in public spaces, with non-compliance punishable by imprisonment (Republic of Tunisia 1993).

In the 2000s, the system underwent modernisation with the introduction of machine-readable cards incorporating a photograph, fingerprint, and signature, alongside enhanced verification features such as barcodes and UV-fluorescent features (Council of the EU 2021).

1.2 Digital penetration in the country

The digitalisation of social, economic, and political spheres in the country is mirrored by the digitalisation of its national ID system. In Tunisia, whose population was roughly 12 million in January 2024 (INS 2025), individual internet usage stood at approximately 74 per cent, while household internet access was estimated at 57.0 per cent (ITU 2024). Furthermore, mobile connectivity is widespread, with 15.7 million cellular mobile connections active in early 2025 (DataReportal 2025). Data traffic reached 93.77 terabytes in January 2025, with smartphones accounting for a substantial 87.4 per cent of total traffic (INTT 2025).

1.3 Current state of the digital-ID project

The current Tunisian digital-ID landscape is built on three foundational ID systems (Clark, Ben Ghachem and Okamura, 2019): the Civil Register; the CIN, which is expected to be replaced by a biometric version under Law No. 2024-22; and the Unique Citizen Identifier (IUC), which may be further integrated into the digital-ID system in the future. The digital-ID system was further complemented by the introduction of the Mobile ID in 2022, which allows for digital authentication and access to online public services. The system also incorporates an interoperability framework. These interrelated components together form the infrastructure for digital identification and authentication. In addition to the Civil Register and

sectoral ID databases, these components collectively contribute to Tunisia's digital-ID ecosystem, but they vary in their levels of implementation.

It is important to distinguish between Tunisia's biometric card system established by Law No. 2024-22, which amends Law No. 93-27 of 22 March 1993, relating to the CIN and the Mobile ID project launched in 2022 by the Ministry of Communication Technologies. While both initiatives fall under the broader umbrella of digital identity, they are not synonymous. The biometric ID is a mandatory, state-issued ID based on biometric data, and is physically embedded as a microchip in the CIN. In contrast, the Mobile ID is a voluntary, digital authentication platform designed to enable citizens to access online services using their national ID credentials. Although the two systems may become integrated in the future, they currently serve distinct functions and are governed by different policy frameworks. The Mobile ID is currently the only digital-ID accessible in Tunisia.

Civil Register

The Civil Register – the MADANIA system, whose name derives from the Arabic word for 'civil' (مدنية) – is a digitised civil registration system, which serves as a centralised database to manage the civil status records of all Tunisian nationals and foreigners with registered civil status. It covers events such as births and deaths, which come under the authority of the Ministry of Interior, and marriages and divorces, under the Ministry of Justice (UNFPA 2021).

Unique Citizen Identifier

As part of Tunisia's National Strategic Plan for Digital Transformation, the IUC was introduced under Decree-Law No. 2020-17 and Decree No. 2020-312 (hereafter referred to as the IUC decrees). The IUC assigns a unique 11-digit number to Tunisian nationals at birth or upon acquiring nationality, based on civil registration records, requiring no additional documentation for enrolment. No biometric data is stored. It applies to all registered Tunisian nationals, with the civil registration system achieving a 99 per cent birth registration rate (*ibid.*).

CIN

In 2024, the Tunisian parliament enacted Law No. 2024-22 (Republic of Tunisia 2024), which mandates a biometric ID card for all citizens aged 15 and above.

Law No. 2024-22 (Republic of Tunisia 2024) modifies and complements Law No. 93-27 of 22 March 1993, concerning the CIN. It introduces the integration of an electronic chip on the card, and an electronic authentication certificate for digital-ID verification and electronic signatures, and revises requirements for card renewal and expiration.

A first draft of this law was proposed by the Ministry of Interior in 2016, and discussed at the parliamentary commission for rights and freedoms and external relations, but faced broad criticism from civil society organisations and the National Authority for the Protection of Personal Data. The Ministry of Interior consistently resisted significant alterations of the draft, which led to its withdrawal by the ministry on the same day as its submission to a vote in plenary session in 2018 (Benzid 2022). The ministry's fourth draft was approved by parliament, with limited public consultation in early 2024 (Access Now 2024).

To obtain the biometric ID card, applicants must provide a valid CIN and/or a recent birth certificate, proof of residence, and recent photographs. During the application process, the Ministry of Interior's specialised services capture the applicant's fingerprint and photograph.

The biometric ID contains an electronic chip storing personal information including the cardholder's address and date of birth, and biometric data, including their photograph and fingerprint, an electronic authentication certificate for identity verification, and digital signatures. The data stored in the chip is encrypted. Access to this data is authorised for the specialised services of the General Directorate of National Security, agents of the National Guard, and Customs, within their respective areas of responsibility. As of May 2025, the Ministry of Interior had yet to begin issuing these biometric ID cards; consequently, no Tunisian citizen possesses the new biometric card.

Functional ID systems

In addition to foundational IDs, Tunisia employs several functional ID systems designed for specific sectors, including social security, taxation, health care, and education. These functional IDs require the CIN and/or birth certificate for enrolment and pre-transaction authentication.

Key stakeholders responsible for these functional IDs include the Ministry of Social Affairs, which manages identifiers for social security and health care; the Ministry of Finance, which administers the taxpayer ID number (*matricule fiscal*), a mandatory identifier integrating data from diverse sources such as employers; the Ministry of Interior, for traffic violations; and the Ministry of Labour, for labour infractions. The Ministry of Communication Technologies often provides technical oversight for these systems.

Mobile ID

Tunisia's Mobile ID system was launched in 2022, following Circular No. 007 of 20 June 2022 by the minister of communication technologies. It is available to citizens aged 18 and above with a valid CIN (MTC 2022). Mobile ID holders can access a selection of public and private e-services, including electronic document signing. Additionally, citizens can create an electronic wallet on the Mobile ID platform and request an electronic payment card, which allows various financial operations such as payment of administrative fees and withdrawal of money (*ibid.*).

The Mobile ID is available in two types. The first, linked to a mobile device, is accessible to both residents and non-residents (*ibid.*). The second, linked to a phone number, uses SMS (text message) verification and is available only to residents. To note, mobile phone SIM card registration is mandatory in Tunisia. Telecoms operators are required to keep records of customers' data, including identities, dates of birth, postal addresses, and CIN numbers (Privacy International 2019).

The registration process for the Mobile ID requires submitting an online request through the mobile app or official website, including the unique CIN number, date of birth, phone number, email address, and acceptance of the terms of service. Verification involves a physical visit to a telecoms operator agency (for residents), or a virtual video call (for non-residents), with a CIN or passport. All three existing mobile telecoms providers in Tunisia – Ooredoo Tunisia, Orange Tunisia, and Tunisie Télécom – are partners in the Mobile ID project. Upon verification, the digital-ID and electronic signature (numeric identifier and PIN) are activated (MTC 2022).

As of January 2025, there were 142,772 Mobile IDs linked to phone numbers (relying on phone numbers linked to pre-registered SIM cards), 21,941 Mobile IDs linked to mobile devices, and 12,434 Mobile IDs issued to citizens abroad.

Circular No. 007 of 20 June 2022 by the minister of communication technologies identified the purpose of the Mobile ID project, listing the actors involved and their roles (*ibid.*).

The development of the Mobile ID project, the IUC system, and related e-government initiatives are financed through a combination of domestic allocations and international loans, notably, a €71.56 million loan from the African Development Bank, approved in November 2017 (AfDB 2017), and an €89.2 million loan from the International Bank for Reconstruction and Development, approved in January 2020 (Republic of Tunisia 2020e).

2. History of ID in Tunisia

Tunisia's digital-ID system is driven by internal and external pressures. Internally, pre-digital administrative inefficiencies forced citizens to navigate bureaucratic hurdles, often requiring them to travel long distances for physical documents. A 2017 survey among a sample of 500 operational small and medium-sized enterprises across 24 governorates in Tunisia revealed that a significant majority (76.3 per cent) of the participating enterprises perceived the public administration as a major, moderate, or severe obstacle to their operations (CJD, Konrad Adenauer Stiftung and One to One 2017). The Covid-19 pandemic exposed these weaknesses, particularly in social aid distribution, demonstrating the perceived need, according to authorities, for a unified, real-time data system for equitable resource allocation. This need became a key driver for the rapid development of the IUC (INPDP 2020).

Beyond these immediate concerns, Tunisia's broader push for digitalisation, fuelled by public and private investment in information and communications technology, has created fertile ground for digital-ID. The Ministry of Information Technology initiated the unique identifier system's design in 2015, with early involvement from the Strategic Council for the Digital Economy. While the National Authority for the Protection of Personal Data (INPDP) was initially involved, its influence has diminished in recent projects. Lack of parliamentary oversight and the unilateral actions of the president since 2021, such as the dismissal of the government, and the dissolution of the elected parliament and high judicial council (Amnesty International 2023), raise concerns about the potential misuse of data and impact on civil liberties.

Having established the historical context of identification in Tunisia, the next section will transition to an analysis of the enabling legislation for the future biometric digital-ID, evaluated using the 2020 CIS framework.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

The biometric digital-ID project in Tunisia is backed by a validly enacted law but has not yet been implemented. On the other hand the Mobile ID is being implemented, but lacks a validly enacted law.

The biometric ID card law was passed by the parliament, fulfilling the requirement of being enacted by a competent legislative authority. The law establishes the legal basis for the biometric ID card system, including the collection of biometric data and integration of an encrypted electronic chip. However, it also delegates substantial powers to future executive decrees, such as the specifications for keeping personal data secure and protecting it from misuse. This framework introduces the risk of excessive executive delegation.

In contrast, the Mobile ID project is only backed by executive decrees and ministerial orders. The project was launched by Circular No. 007-2022 from the minister of communication technologies, following a series of government decrees related to data interoperability and the IUC (Republic of Tunisia 2022). These texts (Decree No. 31-2020 and Order No. 777-2020 on data interoperability, as well as the IUC decrees) establish foundational legal provisions (*ibid.*). However, the reliance on an executive circular for policy matters of collection, storage, use, and the sharing of personal information raises concerns about legality and the risk of executive overreach.

All texts are publicly accessible digitally and, in some cases, physically. While generally clear, technical terminology presents comprehension challenges for the average citizen.

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

The Mobile ID circular defines its purpose as enabling secure and reliable access to online services, while facilitating the gradual transition away from administrative processes requiring physical presence (Republic of Tunisia 2022). The data interoperability decrees define its scope as establishing a framework for electronic data exchange between entities,

with the explicit exclusion of national defence, diplomatic, and security data (Republic of Tunisia 2020c). The IUC decrees establish five explicit purposes; namely, facilitating inter-organisational information exchange, minimising citizen information requests, automating legal public register updates, streamlining sectoral register management, and simplifying administrative procedures (*ibid.*). Overall, while each of these regulations sets out legitimate aims, their effectiveness in upholding proportionality varies.

In contrast, Law No. 2024-22 on the biometric ID card does not explicitly articulate a legitimate aim for the adoption of mandatory biometric ID. The law merely defines the ID card as a 'personal document certifying the identity of its holder' (*ibid.*).

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

No. The current legislation is overly broad in defining who may have access to citizens' personal data and for what purposes that data may be used.

Tunisia's digital-ID framework is governed by multiple legal instruments, each defining the actors involved and the purposes for which the data may be used. However, the level of specification varies widely. For instance, the biometric ID card law vaguely assigns the Ministry of Interior responsibility for issuance of the ID cards and data management, and lacks clarity on private sector and government access (including law enforcement) to the biometric infrastructure and database. The law broadly mandates Ministry of Interior specialised services to implement data security safeguards and adherence to data protection laws, while granting law enforcement access to the electronic chip. Furthermore, while the law mentions the general purpose of the biometric ID card as a personal document certifying the identity of its holder, it lacks detailed specifications of limitations on the use of the data collected, and requirements for user consent regarding changes in data applications (Republic of Tunisia 2024).

The Mobile ID circular outlines the roles of: telecoms operators (identity verification, service integration, agreement compliance); the National Agency for Electronic Certification (certificate issuance, service oversight); and the National Informatics Centre (CNI) (platform development, hosting, process digitisation). In 2022, a partnership agreement for implementation of the Mobile ID was signed between these actors and the telecoms ministry, but remained undisclosed to the public (THD 2022).

Additionally, the Mobile ID project's functionality is closely linked to the data interoperability platform. Understanding its actors is crucial. They include the interoperability operator that manages the system (CNI), public and private legal entities tasked with a mission of public interest or managing a public utility, which are required to provide the CNI with available data stream lists and authorisations, alongside strategic and technical advisory committees. As of 2024, four ministries were operating with the interoperability platform (Interior, Education, Transport, and Social Affairs) with plans to expand its use to all other ministries and administrations(THD 2024).

The IUC system, which may be further integrated within the digital-ID in the future, has clearly defined actor roles and detailed responsibilities: a dedicated register management unit, the CNI (technical operations in coordination with the INPDP), and a multi-representative council for monitoring compliance and access. The IUC decrees also specify that private entities managing public services may also access the database under specific conditions, subject to a ministerial decree and INPDP approval.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use the digital-ID and govern its use?

While the overall digital-ID framework provides some administrative redress mechanisms, such as the ability to report discrepancies and access usage records, it falls short of ensuring adequate civil and criminal redress.

Mobile ID authentication requires identification via an SMS-based, one-time password received via SMS, or acceptance of device notifications. However, the circular lacks provisions for real-time notifications regarding data usage, access, or breaches.

The Mobile ID is optional, offering options for opting out and for the deletion of mobile data. The platform's privacy policy affirms data subject rights to access, correction, deletion (upon objection), and withdrawal of consent (MTC 2022). However, it lacks provisions for subject access to logs and metadata related to digital-ID usage.

In contrast, the biometric ID card is mandatory for all Tunisian citizens residing in the country aged at least 15 years. Its governing law, however, lacks several critical components necessary for establishing adequate redress mechanisms. There are no clear legal obligations outlined in the law for the relevant authorities to promptly notify individuals in the event of a data breach involving their personal data. Given the sensitive nature of stored biometric and demographic information, timely notification

would be essential to allow individuals to take measures to mitigate potential harms related to identity theft or misuse of personal data. The law only mentions notification of the cardholder in case of expiration of the electronic authentication certificate. However, this is limited to a specific technical aspect of the card and does not cover broader uses of the data or potential security breaches. While cardholders can legally access their encrypted chip data and track access, the undefined process makes this right unenforceable until a complementing decree is adopted. Furthermore, the law fails to establish clear rights for data correction or a grievance redress framework, potentially leaving individuals without recourse.

The IUC system and interoperability platform do not provide the right to opt out. The IUC decrees establish the mandatory inclusion of all Tunisian nationals in the system, whether through civil status records, or naturalisation. Individuals are not explicitly granted the right to directly access their personal data as it is stored in the IUC register or the interoperability platform. Instead, they may review information about the usage of their data, including the date and nature of operations performed on their data, and the identity of the entity that accessed their data. These mechanisms are still not publicly available. Individuals must rely on the IUC Register Management Unit or related service provider for corrections and to ensure alignment with original records. While this provides a degree of transparency and accountability, the right is limited to monitoring usage rather than direct access to the stored data itself. Additionally, access to this information is limited to a one-year period after the operations occur, requiring individuals to proactively check within this timeframe.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

Both the biometric ID card system and Mobile ID platform governing texts lack defined oversight and grievance mechanisms. The absence of a clear separation between the administrators of the system and independent regulators (assigned to the Ministry of Interior and Ministry of Communication Technologies, respectively) weakens accountability and opens avenues for conflicts of interest. Additionally, the biometric ID card law's reliance on future decrees leaves a significant gap in holding actors accountable, given that there is no mention of an independent body to handle complaints, nor are there detailed processes for individuals to challenge unlawful access or use of their data. Overall, the biometric ID law fails to establish the necessary accountability mechanisms as it lacks oversight and transparency mechanisms, and effective grievance redress procedures.

Conversely, the IUC system employs a multi-stakeholder oversight model comprising the IUC Register Management Unit, the INPDP, which ensures data protection and is empowered to revoke access to IUC data, and the Council for Monitoring the Use of the IUC, which supervises usage and access approval (Republic of Tunisia 2020a).

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

The digital-ID framework provides limited safeguards against mission creep. Although the IUC decrees mandate that access to the digital-ID database is subject to approval by a supervisory council and oversight by the INPDP, the data interoperability platform lacks public consultation or legislative scrutiny for expanded data exchange. Similarly, the biometric ID card law is vague regarding permitted uses, and lacks review procedures for new uses, and any independent oversight mechanism. This absence of safeguards risks unauthorised functional expansion, potentially leading to surveillance or profiling by the authorities.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

The biometric ID card law also does not demonstrate that the privacy violations arising from the designed system are necessary and proportionate to achieve a legitimate aim. The law does not demonstrate that the biometric ID system – specifically, the design choice to use a centralised database – is the least restrictive means of achieving its unstated aims. Additionally, the law does not address data retention policies, leaving open the possibility of excessive and unjustified data storage.

The personal data protection policy for the digital-ID platform states that processing is limited to the issuance of the ID, based on the data subject request, and respecting the principles of necessity and proportionality. Additional data usage requires explicit user consent.

However, the current platform enables excessive data collection and broad metadata retention, and lacks strict access controls with clear legal mechanisms for challenging misuse, making it difficult for individuals to enforce their right to privacy. Some safeguards exist, including the National Personal Data Protection Authority's role of oversight, review, and consultation, and receiving user complaints (MTC 2022). However, it lacks enforcement power for its decisions.

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

The data protection policy restricts data usage to digital-ID and electronic authentication certificate creation and delivery, requiring explicit consent for other purposes. However, the national personal data protection law exempts public authorities from standard data-processing obligations, including consent requirements (Republic of Tunisia 2004). The policy for the digital-ID platform specifies that the collected and processed data include the holder's name, birthdate, CIN number, phone number, and a copy of the CIN, but lacks prohibitions against future expansion into additional categories, including biometrics or metadata (MTC 2022).

The policy does not state specific time frames for data retention, but rather uses vague terms such as 'only as long as necessary', and permits controllers to anonymise or destroy data once they have fulfilled their purpose. Data transfer to third parties necessitates user consent or anonymisation/encryption; however, the policy fails to specify the applied level of anonymisation, thereby leaving potential vulnerabilities (MTC 2022).

The biometric ID card law also lists the data collected (both on the card and in the chip), but it still falls short in several critical areas regarding data minimisation: the absence of clear limitations on purpose, retention, processing, and the reliance on future decrees to define critical aspects of data protection. Overall, it lacks the specificity and safeguards necessary to ensure appropriate data limitations.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

The Mobile ID privacy policy mandates data security measures but lacks specificity regarding authentication logs and metadata handling. Data transfer requires consent or anonymisation/encryption, with undefined anonymisation standards.

The IUC decrees restrict data access to authorised entities for legal purposes. The federated system avoids central storage, using identifiers for controlled exchange. Access logs are maintained and are accessible to individuals for one year. The INPDP can also suspend the access of entities that violate the law

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

No. Neither the biometric ID law nor the data protection law has adequate mechanisms to prevent exclusions.

While a unique identifier is automatically assigned, Mobile ID access depends on mobile phone ownership and connectivity. This may exclude individuals without access to mobile devices or telecoms services. However, no formal studies have been conducted to assess the inclusivity of the system.

Data accuracy is maintained via mandatory controller updates and subject access rights for correction and cancellation.

However, the system lacks explicit appeal mechanisms for enrolment exclusions or authentication failures.

Similarly, the biometric ID law does not establish adequate mechanisms to prevent exclusion or restriction of access to entitlements or services resulting from the adoption of the biometric ID card. No provision is included on what happens if biometric verification fails, or on accountability for failures that lead to exclusion.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

The national biometric ID card is mandatory for all citizens aged 15 and over under Law No. 2024-22 (Republic of Tunisia 2024). Additionally, its use is mandated for the provision of several services and administrative procedures, including accessing public services, opening bank accounts, and participating in elections. Lacking a national ID card could significantly hinder an individual's ability to engage in civil life and access fundamental rights, potentially leading to difficulties in employment, housing, and legal matters.

In contrast, the Mobile ID is optional. Mainly, it can be used to authenticate and access electronic administrative services, but other authentication options are usually offered.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

The development and approval of digital-ID legal texts lack documented risk assessments. Authorities did not respond to a joint request by five civil society organisations for additional clarification on several key elements of the Mobile ID project, and whether any impact assessments were conducted (Access Now 2023). The IUC decrees stand as the only instance where the INPDP's involvement and consultation on data protection safeguards were communicated and supported by public opinion and media engagement with the INPDP president (INPDP 2020).

Furthermore, civil society organisations have raised concerns that the current data protection framework, Law 63-2004, fails to fulfil Tunisia's international obligations under Council of Europe Treaty 108 and Protocol 181, and requires revision. The INPDP's perceived lack of independence, documented non-enforcement of the law by both public and private sectors, and lack of inclusion of the specificity of biometric data, further underscore the framework's inadequacy (Access Now 2023).

5.2 Differentiated approach to risk

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

The digital-ID legal framework lacks a differentiated governance approach for digital-ID usage based on the risks it entails. While the biometric ID law mandates Ministry of Interior data integrity measures and relies on general data protection legislation, it contains no mention of conditions, consent requirements, or alternative verification mechanisms to prevent exclusion. The IUC decrees assign responsibility to the INPDP and the Council for Monitoring the Use of the IUC for addressing grievances and ensuring compliance with regulations, including those related to inclusion and access.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

The governance envisaged in the biometric ID law is not proportionate to the evident risks. Centralised storage of immutable biometric data, which is highly vulnerable to identity theft in the event of a data breach, is particularly concerning. While Ministry of Interior officials cited identification of victims of road traffic accidents as justification, this rationale fails to outweigh the substantial risk to millions of citizens, especially given alternative identification methods (Benzid 2022).

Despite referencing security measures (encryption, secure readers), the biometric ID card law lacks concrete technical specifications and data security protocols. Critically, the law does not disclose the electronic chip's nature. In a previous announcement, Ministry of Interior officials stated that the electronic chip would be contactless (i.e. readable remotely), which raises significant concerns regarding potential surveillance and remote intrusion vulnerabilities (*ibid.*). The law's reliance on a general reference to 'personal data protection legislation' is inadequate. This is particularly problematic given the referenced legislation's lack of specific provisions addressing the unique security and privacy risks associated with biometric data. Furthermore, the law lacks a comprehensive data breach response plan, notification procedures, redress mechanisms, and independent oversight. It also fails to address authentication inaccuracies, potentially leading to exclusion errors, and lacks a clear separation of responsibilities for collection/identification and authentication.

The texts governing other components of the digital-ID infrastructure such as the Mobile ID and the IUC platform offer improved governance, but shortcomings persist. For instance, the Mobile ID's privacy policy acknowledges data subject rights, yet lacks appeal mechanisms for authentication errors (MTC 2022). The IUC register's correction procedures, which the managing unit implements, exclude explicit access rights for individuals to their stored data (Republic of Tunisia 2020a).

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

While Tunisia's digital-ID initiative began with a draft data protection law aimed at harmonising the data protection ecosystem with international commitments and introducing a privacy-by-design IUC system, the subsequent implementation deviated significantly. The separate adoption of IUC decrees, the blocked data protection law revision, and subsequent enactment of the biometric ID card law and Mobile ID circular without sufficient risk mitigation, have resulted in a system that lacks essential safeguards. Notably, these two texts fail to mandate data breach notification to affected individuals, and lack provisions for a dedicated cybersecurity oversight body to prevent and investigate cyber-threats.

6. Conclusion

In conclusion, this analysis of Tunisia's digital-ID landscape highlights critical shortcomings in governance and implementation. While the country aims to enhance its digital-ID capabilities through a multi-layered system, the research reveals a mixed picture. The legal framework exhibits excessive delegation of authority to the executive, lacking clarity in purpose and limitations, while responsibilities across various legal instruments and components of the system vary considerably. Safeguards against mission creep and mechanisms for redress remain insufficient, raising concerns about data-handling practices and the protection of individual rights. These findings highlight the urgent need for improved legal clarity, stronger independent oversight, and robust risk management to ensure appropriate use of the digital-ID system and protection of individuals' rights.

Recommendations for different stakeholders include those listed below.

For civil society organisations

- Civil society organisations should advocate for greater inclusivity and consultation throughout the design and development phases of digital-ID systems.
- These organisations should promote public awareness regarding the human rights implications of digital-ID systems, and ensure citizens are informed of their rights and available redress mechanisms.
- Civil society organisations should strengthen their monitoring and documentation of instances of exclusion or harm experienced by citizens as a result of digital-ID implementation.

For authorities

- Authorities should establish mechanisms for meaningful coordination and consultation with diverse segments of Tunisian society when adopting systems that affect their livelihoods.
- Authorities should prioritise the selection of designs and technologies that minimise infringements on the privacy of Tunisian citizens, and should disclose the rationale for these choices to civil society, independent experts, and the wider public.
- Authorities should conduct and publicly disseminate accessible risk assessment reports whenever digital-ID adoption has the potential to impact fundamental human rights.

For international funders and development agencies

- International funders and development agencies should prioritise and promote the publication of transparency and human rights risk assessment reports.

7. Bibliography:

Access Now (2024) ***Eight Years in the Making: Tunisia's Controversial Biometric ID and Passport Bills Risk Rights***, 7 March (accessed 13 October 2025)

Access Now (2023) ***Tunisia's Government Must Open the Mobile ID Black Box***, 6 February (accessed 13 October 2025)

AfDB (2017) ***AfDB Approves €72 Million Loan For Radical Upgrade of Tunisia's Digital Capability***, African Development Bank, 10 November (accessed 13 October 2025)

Amnesty International (2023) ***Tunisia: The Abuse of Pre-Trial Detention to Silence Dissent***, 1 June (accessed 13 October 2025)

Benzid, H. (2022) ***Carte d'identité biométrique : Sacrifier la vie privée au profit de l'efficacité des services***, Inkyfada, 6 April (accessed 13 October 2025)

Bhandari, V.; Trikanad, S. and Sinha, A. (2020) ***Governing ID: A Framework for Evaluation of Digital Identity***, The Centre for Internet and Society, India (accessed 13 October 2025)

CJD, Konrad Adenauer Stiftung and One to One (2017) ***Enquête auprès des PME sur l'évaluation et les attentes des administrations publiques***, Konrad Adenauer Stiftung Tunisia (accessed 23 October 2025)

Clark, J.; Ben Ghachem, A. and Okamura, Y. (2019) ***L'Identification pour le Développement (ID4D): Diagnostic des systèmes d'identification en Tunisie***, World Bank (accessed 13 October 2025)

Council of the European Union (2021) ***Tunisia – National Identity Card (TUN-BO-01001)***, PRADO (accessed 13 October 2025)

DataReportal (2025) ***Digital 2025: Tunisia*** (accessed 13 October 2025)

INPDP (2020) ***النظام الوحيد للاعرف المرقمن*** [*L'identifiant unique citoyen*], National Authority for the Protection of Personal Data (accessed 13 October 2025)

INS (2025) ***Indicateurs clés***, Institut National de la Statistique (accessed 13 October 2025)

INTT (2025) ***Tableau de bord mensuel data mobile***, Instance Nationale des Télécommunications (accessed 13 October 2025)

ITU (2024) ***ICT Development Index 2024***, International Telecommunication Union (accessed 13 October 2025)

MTC (2022) ***FAQ – الهوية الرقمية***, [Mobile ID Tunisia FAQ], Ministry of Technologies and Communication (accessed 13 October 2025)

Paradigm Initiative (2025) ***Digital Rights and Inclusion in Africa Report*** (accessed 13 October 2025)

Privacy International (2019) ***Timeline of SIM Card Registration Laws*** (accessed 13 October 2025)

Republic of Tunisia (2024) ***Law No. 2024-22 of March 11, 2024, Amending and Supplementing Law No. 93-27 of March 22, 1993, Relating to the National Identity Card***, Legislation Sécurité (accessed 13 October 2025)

Republic of Tunisia (2022) ***Circular of the Minister of Communication Technologies No. 007 of June 20, 2022, Relating to the National Project to Focus Digital Identity on Mobile ID***, Minister of Communication Technologies (accessed 13 October 2025)

Republic of Tunisia (2020a) ***Decree-Law No. 2020-312 of 15 May 2020, Establishing the Content and Technical Specifications of the Unique Citizen Identifier and the Rules Governing the Maintenance and Management of its Register***, Legislation Sécurité (accessed 13 October 2025)

Republic of Tunisia (2020b) ***Decree-Law of the Head of Government No. 2020-17 of May 12, 2020, Relating to the Unique Identifier of the Citizen***, Legislation Sécurité (accessed 13 October 2025)

Republic of Tunisia (2020c) ***Decree of the Prime Minister No. 31 of 2020 dated 10 June 2020, Regarding the Electronic Exchange of Data Between Structures and their Clients and Between Structures***, Legislation Sécurité (accessed 13 October 2025)

Republic of Tunisia (2020d) ***Government Order No. 777 of 2020 dated 5 October 2020, Setting the Conditions, Formats, and Procedures for Implementing the Provisions of Decree No. 31 of 2020 of 10 June 2020, of the Prime Minister, Relating to the Electronic Exchange of Data Between Structures and their Clients, and Between Structures***, Legislation Sécurité (accessed 9 February 2025)

Republic of Tunisia (2020e) ***Law No. 25 of 2020 dated 28 May 2020, Concerning the Approval of the Loan Agreement Concluded on 30 January 2020, between the Republic of Tunisia and the International Bank for Reconstruction and Development to Contribute to the Financing of the e-Governance Program to Support the Digital Transformation of Administrative Services***, 9anoun (accessed 13 October 2025)

Republic of Tunisia (1993) ***Law No. 93-27 of 22 March 1993, on the National Identity Card*** (accessed 13 October 2025)

Republic of Tunisia (1957) ***Law No. 1957-3 of 1957, Regulating Civil Status***, Refworld, UNHCR (accessed 13 October 2025)

THD (2024) ***Deployment of the National UXP Interoperability Platform***, Tunisie Haut Debit (accessed 13 October 2025)

THD (2022) ***Mobile ID: Signing of a Partnership Agreement Between the Ministry of ICT and Operators***, Tunisie Haut Debit (accessed 13 October 2025)

UNFPA (2021) ***Knowledge Brief on Completeness of Birth Registration in Tunisia, 2000-2018***, United Nations Population Fund accessed 13 October 2025)

Digital-ID in Liberia: Country report

Peterking Quaye

 DOI: 10.19088/IDS.2025.059

1. Introduction

This research investigates the impact of biometric digital identification (digital-ID) systems on citizens' digital rights in Liberia. As the country rebuilds post-conflict institutions, the adoption of a national digital-ID – anchored in biometrics and managed by the National Identification Registry (NIR) – is central to modernising identity management and enhancing access to public services.

Supported by international partners such as the World Bank and the United Nations Development Programme (UNDP), Liberia's digital-ID rollout presents a unique case in sub-Saharan Africa, where infrastructure limitations, legal gaps, and social inequalities intersect with digital transformation. While digital-ID aims to improve service delivery and legal recognition, it also raises questions around inclusion, privacy, and governance. This study addresses the following core research questions: how does Liberia's biometric digital-ID system affect citizens' digital rights, and to what extent does it align with rule of law, rights-based, and risk-based principles? By focusing on Liberia, the study aims to contribute to the broader African discourse on responsible digital-ID development and digital rights protection.

The report is structured as follows: Section 2 traces the history and evolution of ID in Liberia, before the present digital-ID system is assessed using the three sets of tests in the Centre for Internet and Society (CIS) framework.

2. History of ID in Liberia

This chapter examines the development of Liberia's ID systems, from colonial-era practices to the current National Biometric Identification System (NBIS). It focuses on the country's transition to digital-ID, a process shaped by governance reforms, regional integration goals, and the need for inclusive public service delivery.

Digital-ID is particularly significant in Liberia, where decades of conflict and institutional fragility have left millions of people without official proof of identity. The government argues that the introduction of a biometric ID system – incorporating fingerprints and facial recognition – is a crucial step towards strengthening state–citizen relations, improving service delivery, and enabling financial and electoral inclusion. Yet, implementation faces challenges related to access, infrastructure, legal safeguards, and public trust. The researcher addresses questions including what the current state of Liberia's digital-ID system is, and how its legislative and institutional framework aligns with rule of law principles, human rights protections, and risk-based governance.

2.1 Colonial ID systems

Liberia, unlike most African nations, was never colonised by a European power but was founded in the early nineteenth century by freed African Americans under the American Colonization Society. This unique history shaped the country's early ID systems, influenced by the American Colonization Society's governance rather than European colonial models. The first ID documents were land deeds and citizenship papers issued to repatriated freed slaves, serving as proof of settlement and land ownership. These land deeds primarily benefited Americo-Liberians, while indigenous populations were often excluded from official records. By the late nineteenth and early twentieth centuries, ID systems expanded to include tax records, military registration, and labour documentation. However, these systems remained paper-based, decentralised, and prone to inefficiencies and corruption.

2.2 Post-liberation ID systems (pre-digital)

After gaining independence in 1847, Liberia's ID documentation was fragmented, with the Americo-Liberian elite controlling records, and indigenous populations facing barriers to obtaining birth certificates and passports. By the mid-twentieth century, voter registration cards

and passports were introduced due to urbanisation and the needs of a growing civil service. However, incomplete birth registration, inefficient record-keeping, and restricted rural access limited the ID system. The civil wars (1989–2003) further devastated the system, and were accompanied by lost records, identity theft, and fraud. Post-war efforts focused on rebuilding civil registration and identity management.

2.3 Digital penetration in Liberia

As of mid-2025, Liberia's digital-ID initiatives are advancing, yet infrastructure and policy challenges persist. Internet penetration has increased to 32.4 per cent, with 1.84 million users, while mobile connections have reached 90.1 per cent of the population, totalling 5.11 million active lines (DataReportal 2025). Liberia's digital-ID rollout, supported by the World Bank and UNDP, seeks to improve governance and service delivery through the NIR. However, rural populations still depend on paper-based documents due to limited internet connectivity, infrastructure gaps, funding constraints, and data security concerns. These factors hinder widespread adoption of digital-IDs in remote areas. According to the World Bank, inadequate broadband access, digital infrastructure, and affordability challenges are major barriers to digital inclusion across sub-Saharan Africa, including Liberia (World Bank 2023). Bridging the digital divide is therefore critical for ensuring an inclusive and effective digital-ID system.

2.4 Introduction of the digital-ID system

Liberia's digital-ID system is grounded in the NIR Act of 2011, enacted on 1 August 2011, which established the legal framework for creating and managing a biometric national ID system. Liberia launched its National Biometric Identification Card programme in October 2016, establishing the foundation for its national digital-ID infrastructure. By December 2024, approximately 740,000 individuals – less than 15 per cent of the estimated 5.2 million population – had been registered. To address this gap, the government, through the NIR, aims to achieve 80 per cent national coverage (around 4.2 million people) by 2027. Strategies include deploying mobile registration units, partnering with mobile network operators, and focusing on hard-to-reach populations. The National Biometric Identification Card serves as an official ID for accessing government services, banking, elections, and digital platforms.

2.5 Registration requirements and process

Liberia's NBIS, overseen by the NIR, issues secure ID cards using biometric data such as fingerprints and facial recognition to strengthen identity verification and access to services. However, the system faces key challenges. Applicants must present official documents such as a birth certificate or passport, while community attestation is accepted for those without formal records; however adoption is uneven due to limited internet and digital literacy.

The NIR Act of 2011 mandates the NIR to design, implement, and manage Liberia's NBIS, including biometric data collection (Section 3.1). It also grants authority to collect data and issue ID cards (Section 4). However, the Act does not specify procedural details such as required documents, acceptance of community attestation, offline registration, issuance timelines, mobile teams, or urban/rural access differences. These operational specifics are covered in NIR policies, guidelines, and public communications from the NIR and development partners such as the World Bank and UNDP.

2.6 Adoption and inclusivity

As mentioned above, as of December 2024, the NIR had enrolled less than 15 per cent of the population. This low adoption reflects challenges including limited public awareness, logistical constraints, and poor accessibility, especially in rural areas. Urban centres such as Monrovia show higher registration rates, while rural regions face inadequate infrastructure and literacy barriers. Vulnerable groups – women, elderly people, people with disabilities, and undocumented individuals – face further difficulties such as mobility limitations and lack of birth records. To improve coverage, expanding outreach, adopting inclusive policies, and boosting public awareness are critical (NIR Act 2011; NIR Annual Report 2019; World Bank 2023).

2.7 Biometric and technological features

The NBIS uses biometric technologies – including all ten fingerprints and facial recognition – to ensure secure and unique identity verification. The system employs an automated fingerprint identification system to prevent duplicate registrations, while facial recognition serves as a secondary verification method when fingerprints are unclear (NIR Annual Report 2019). The NBIS integrates with key government and private sector databases, enabling access to essential services such as health care, banking, social welfare programmes, and electoral voting. For example, biometric ID cards are mandatory for enrolling in the National Health Insurance Scheme, opening bank accounts, and voter registration (World Bank 2023;

Government of Liberia 2011; NIR 2019). Telecoms providers such as Orange Liberia also require biometric verification for mobile money transactions to comply with know your customer (KYC) regulations (OMEA 2024).

However, a significant portion of the population – particularly in rural and vulnerable communities – remains excluded from these services, exacerbating inequality and limiting social and economic participation. To mitigate this, mobile registration teams and outreach initiatives supported by development partners aim to expand coverage, especially in underserved areas (UNDP 2023).

The NBIS's biometric infrastructure also allows for potential future enhancements, such as iris scanning, to improve security, and accuracy in identification.

Data storage and security

Liberia's digital-ID system uses a centralised biometric database with encryption, restricted access, and backup measures to protect personal data. Multi-factor authentication strengthens security, but the lack of a stand-alone data protection act raises privacy concerns, emphasising the need for stronger cybersecurity laws.

Integration with government services

Liberia's digital-ID system, established under the NIR Act of 2011, supports governance, service delivery, and financial inclusion. The act mandates the NIR to design and manage the NBIS.

In partnership with the Civil Service Agency, the NIR uses national ID numbers on government employee ID cards to eliminate 'ghost' names and improve payroll efficiency. A memorandum of understanding allows the Civil Service Agency access to the NIR's e-verification portal.

Telecom firms such as Orange Liberia use digital-ID for KYC-compliant mobile money services, ensuring secure transactions. Orange also supports digital inclusion through its Orange Digital Center at Tubman University. Public–private collaboration is key to driving Liberia's digital transformation and expanding citizen access to secure services.

Government agencies involved

Liberia's biometric ID system is supported by multiple government agencies to ensure comprehensive integration across sectors. The NIR issues biometric IDs and manages data verification. The Ministry of Internal Affairs oversees civil registration, providing foundational ID records. The Liberia Immigration Service applies the system for border control and migration

management. The Liberia Revenue Authority links biometric IDs to taxpayer records to improve revenue collection. The National Elections Commission incorporates the IDs into voter registration to enhance electoral integrity. The Central Bank of Liberia promotes financial inclusion by endorsing biometric ID use in banking services, while the Liberia Telecommunications Authority regulates biometric ID use for SIM card registration and mobile banking compliance (NIR 2019; Ministry of Internal Affairs 2025; LRA 2024).

International support for Liberia's digital-ID system

Liberia's digital-ID development is strongly backed by international partners contributing to its infrastructure, governance, and interoperability. The World Bank committed US$30 million in 2025 under the Government Resource and Economic Advancement of Transformation (GREAT) project to support Liberia's digital public infrastructure. The initiative targets the enrolment of at least 2 million Liberians into the biometric ID system managed by the NIR.

The African Development Fund approved a US$8 million grant in 2023 to support the Unique Bank Identification and Digital Interoperability Project across four West African Monetary Zone countries, including Liberia. The initiative, led by the West African Monetary Institute, promotes harmonised banking ID frameworks. In 2017, the NIR signed a US$5.9 million deal with Techno Brain Global FZE to develop a biometric civil registry and issue 1 million ID cards, including 50,000 ECOWAS-compliant cards. While funding details remain undisclosed, UNDP and ECOWAS have provided vital technical assistance for digital registry improvements, digital inclusion, and deployment of ECOWAS Biometric Identity Cards to ensure regional interoperability. Together, these partners help ensure Liberia's digital-ID system is secure, inclusive, and regionally integrated.

Private sector role

The private sector supports Liberia's digital-ID system by providing biometric technology, securing data, and integrating services. The private sector is key to Liberia's digital-ID rollout – supporting biometric tech, data security, and service integration.

Telecoms
Lonestar Cell MTN and Orange Liberia use biometric ID for SIM card registration, in line with Liberia Telecommunications Authority rules, enhancing national security and reducing fraud. Their mobile money services also employ biometric KYC for secure transactions and regulatory compliance.

Banking and fintech

Banks and fintech firms use national biometric ID for KYC and anti-money-laundering compliance, per the Central Bank's Financial Inclusion Strategy. They also enable digital onboarding using biometric verification, improving access to secure financial services. These partnerships are critical for advancing digital infrastructure, financial inclusion, and digital rights protection in Liberia.

Drivers of development

While Liberia's digital-ID growth is publicly framed around goals such as strengthening e-governance, improving electoral integrity, advancing financial inclusion, and enabling digital economy expansion, it is important to recognise that not all motivations are purely driven by public interest. The role of private vendors, international funders, and even state actors may also reflect interests in profit generation, data control, or surveillance expansion. Vendors stand to benefit commercially from long-term contracts for biometric systems and infrastructure. Governments may view digital-ID systems as tools for enhancing administrative control, while donors align support with global ID frameworks that often reflect broader geopolitical or strategic interests. As such, beyond the stated benefits, it is crucial to critically assess the balance between inclusion, rights protection, and potential risks of centralised data collection and misuse of personal information.

Opportunities and risks

Digital-ID enhances financial access, governance, and cybersecurity, but poses risks such as privacy violations, exclusion of vulnerable groups, identity theft, and cyber-threats.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Yes. Liberia's digital-ID system is grounded in a valid legislative framework. The NIR Act of 2011, enacted by the Liberian legislature and signed into law on 1 August 2011, establishes the legal foundation for the country's biometric ID system. This act created the NIR as an autonomous agency within the executive branch, tasked with designing, implementing, and managing the NBIS. Key provisions of the act include:

- **Establishment of the NIR:** Section 1.1 of the act provides for the creation of the NIR, repealing the previous People's Redemption Council Decree #65 that had established the National Identification Card System.
- **Mandate and functions:** Section 3.1 outlines the general functions of the NIR, which include designing, establishing, maintaining, and administering the NBIS. Section 3.2(b) details responsibilities such as collecting, organising, storing, securing, and granting access to biometric data collected from individuals applying for national biometric ID cards and other key documents.
- **Issuance of biometric ID cards:** The act mandates the issuance of biometric cards, each with a unique identifying number to be called a social security number, serving as the primary government-approved ID number for various services, including registration of births and deaths, passports, immigrant documents, bank accounts, driver's licences, social security benefits, and other ID documents. These provisions ensure that Liberia's digital-ID system operates under a legislated mandate, providing a rules-based framework for its implementation and governance.

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Yes. Liberia's digital-ID system is grounded in a valid legislative framework. The NIR Act of 2011 provides the legal basis for Liberia's biometric ID system. It established the NIR as an autonomous agency to design and manage the NBIS. The act aims to enhance security, service delivery, and financial inclusion but lacks clarity on the specific scope and

limits of ID usage. While it mandates biometric IDs for services such as passports, bank accounts, and licences, it does not clearly define how collected data may be used. This absence of detailed data protection provisions raises concerns about potential misuse and highlights the need for stronger safeguards to protect citizens' digital rights.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

The NIR Act specifies that the NIR is responsible for managing the digital-ID system, including data collection and storage. However, it does not comprehensively define all actors permitted to access or use the ID data. As the legal framework on digital-ID data governance and individual rights, the NIR Act of 2011 establishes the NIR as the sole authority responsible for managing Liberia's digital-ID system, including the collection, storage, and administration of biometric and demographic data (NIR Act 2011, Sections 3.1 and 4).

While the act mandates the collection of comprehensive biometric identifiers such as fingerprints and facial recognition data, it lacks detailed provisions on data minimisation principles or the categorisation and protection of sensitive data, which are critical for privacy compliance. Crucially, the act does not explicitly define all third-party actors authorised to access or use the digital-ID data, creating potential ambiguities in data sharing and governance.

Furthermore, it does not grant individuals explicit rights to access their data, to seek confirmation or correction of inaccuracies, or to opt out of the system, which are fundamental rights under international data protection standards such as the African Union Convention on Cyber Security and Personal Data Protection (AU 2014) and the General Data Protection Regulation (EU 2016).

Additional reports from the World Bank and UNDP highlight these legal gaps, emphasising the need for complementary data protection legislation to safeguard individual privacy and enhance trust in digital-ID systems (World Bank 2023; UNDP Liberia 2023). Liberia's ongoing efforts to draft a dedicated data protection and privacy act may address some of these deficiencies, aligning national laws with global best practices (Ministry of Justice 2024).

Assessment

While Liberia's NIR Act provides a foundational mandate for digital-ID management, the absence of clear legal safeguards on data access, user rights, and data minimisation presents significant challenges. Strengthening the legal framework through explicit definitions of authorised actors, detailed data governance policies, and recognition of individual rights is essential to ensure transparency, protect citizens' privacy, and foster inclusive digital-ID adoption.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

Liberia currently lacks a dedicated data protection law or regulatory authority to oversee digital-ID data use or address related grievances. While the Constitution of Liberia guarantees a general right to privacy (Article 15), the NIR Act of 2011 does not explicitly provide individuals with a right to redress or specify mechanisms for contesting misuse or abuse of digital-ID data. A detailed review of the act reveals no mention of complaint procedures, data protection oversight bodies, or legal recourse for affected persons (NIR Act 2011).

This legal gap leaves individuals vulnerable, as there are no formalised channels to challenge inaccuracies, unauthorised access, or other violations involving biometric and personal data collected by the NIR. The absence of such protections contrasts with international standards on digital-ID governance, which emphasise accessible redress mechanisms as critical to upholding privacy and fostering public trust (UNDP 2023; World Bank 2023).

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

No. Liberia does not have an independent data protection authority (DPA) to oversee the operations of the NIR or ensure accountability in the management of the digital-ID system. The lack of such a regulatory body means there is minimal oversight, increasing the risk of data misuse and undermining public trust in the system.

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

The NIR Act (2011) defines the digital-ID system's primary purposes (Sections 3.1 and 4) but does not explicitly limit its use to these functions. Recent measures, such as an executive order requiring biometric ID for banking, telecoms, health care, education, and immigration, show an expansion beyond the original scope.

This absence of clear boundaries risks mission creep and possible rights infringements. To address this, Liberia needs stronger legal and institutional frameworks, including comprehensive data protection laws, independent oversight, and clear limits on digital-ID use to safeguard individual rights and ensure transparency.

Rights-based tests assess the extent to which Liberia's digital-ID system aligns with international human rights principles – namely, inclusivity, accessibility, non-discrimination, and data privacy. These tests evaluate whether digital-ID policies uphold fundamental rights, particularly for vulnerable and marginalised populations. In Liberia, applying a rights-based framework is essential to ensure that digital-ID serves as a tool for empowerment rather than exclusion.

Liberia's 1986 Constitution, alongside its commitments under international instruments such as the African Charter on Human and Peoples' Rights (OAU 1981) and the International Covenant on Civil and Political Rights (UN 1966), provides a normative foundation for assessing digital-ID systems. The right to identity is fundamental for accessing essential services, including health care, education, banking, and democratic participation (OAU 1981; UN 1966).

Exclusion from digital-ID registration or access to identity credentials can violate constitutional guarantees, including equal protection under the law and the right to participate in public life. These risks disproportionately affect vulnerable groups such as rural populations, people with disabilities, women, and ethnic minorities, who face systemic barriers to accessing public services (Government of Liberia 1986; OAU 1981; UN 1966).

A rights-based approach to digital-ID systems mandates inclusivity by design, ensuring:

- Universal coverage, including of rural and remote residents;
- Affordability, with no financial barriers to obtaining or renewing IDs;
- Cultural and linguistic sensitivity, providing multilingual services that reflect Liberia's ethnolinguistic diversity; and

- Physical accessibility, with disability-friendly registration processes (Government of Liberia 1986; OAU 1981; UN 1966).

Rights-based testing must assess whether exclusions – intentional or unintentional – are occurring, and whether there are mechanisms to prevent them and provide redress. Currently, there are no comprehensive safeguards in place to ensure that people who cannot access or authenticate through digital-ID are not denied entitlements such as health care, pensions, or education.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

The use of biometric and personal data must meet the principles of necessity and proportionality. Liberia's current ID system lacks adequate legal checks to ensure that collection of data such as fingerprints or facial scans is justified for specific services and not excessive (Government of Liberia 2011; World Bank 2016). Without independent oversight, it is impossible to guarantee that data use aligns with legitimate aims such as fraud reduction or service efficiency. This raises serious human rights concerns under both national and regional frameworks (Government of Liberia 2019; Human Rights Watch 2021).

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

Liberia's current digital-ID practices do not adhere to the principle of data minimisation. There is no clear guidance on what data is required, how long it is retained, and under what conditions it can be accessed or shared. Rights-based assessments must ensure that only necessary data is collected, that it is stored for clearly defined and lawful purposes, and that it is deleted after its utility expires. In the absence of a comprehensive data protection law, there is no legal mandate enforcing minimal, purpose-specific data collection, nor provisions for data subjects to access, correct, or erase their data.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

Access to the digital trail created by digital-ID systems – such as transaction histories or authentication logs – must be strictly controlled. In Liberia, no clear legal safeguards exist to limit how state or private actors' access or use this data, increasing the risk of surveillance, profiling, or unauthorised data sharing. This lack of statutory protections is

inconsistent with Economic Community of West African States and African Union data privacy standards (ECOWAS Commission 2010; OAU 1981).

Recommendation

Introduce robust access control mechanisms, including role-based restrictions, logging, and independent audits, to prevent misuse and protect user privacy. Judicial or DPA oversight should be mandatory for access to sensitive personal data.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Liberia's digital-ID system lacks adequate safeguards to prevent exclusion from essential services. The absence of alternative enrolment methods for individuals without formal ID, coupled with biometric dependency, creates barriers for marginalised populations – especially in rural, informal, and stateless communities (World Bank 2017; AfDB 2022).

Moreover, access control mechanisms remain weak. There are no binding rules on:

- Role-based data access;
- Agency data-sharing protocols; or
- Independent oversight of breaches or profiling.

Existing laws, such as the Freedom of Information Act, do not address biometric data protection or digital surveillance. This regulatory vacuum risks both service exclusion and rights violations due to misuse of personal data (NIR Act of 2011; Human Rights Watch 2021).

A comprehensive data governance framework is urgently needed to:

- Define who can access ID data;
- Establish inclusive registration paths; and
- Protect against systemic exclusion and misuse.

Another critical gap is limited public awareness and engagement around digital-ID policymaking. Most Liberians are unaware of their data rights, how their data is used, or how to seek redress in case of a breach. A rights-based framework emphasises:

- Public consultations in the design and rollout of digital-ID systems;
- Civic education to inform citizens of their rights and responsibilities; and

- Human rights impact assessments, conducted periodically to evaluate effects on civil liberties and data privacy.

To realise a secure, inclusive, and rights-respecting digital-ID system, Liberia must embed rights-based principles into every stage of its digital-ID ecosystem – legal design, technological architecture, implementation, and governance. This includes:

- Enacting a comprehensive data protection law;
- Establishing an independent oversight body;
- Ensuring that digital-ID systems are not used for unlawful surveillance or discrimination; and
- Guaranteeing legal pathways for redress and enforcing the principle of non-exclusion.

By balancing security objectives with the protection of civil liberties, Liberia can build public trust in its digital-ID system and ensure that no one is left behind in the country's digital transformation journey.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

As of now, Liberia lacks legislation that explicitly mandates enrolment in or use of the NBIS. However, recent government directives and administrative practices – such as requiring biometric IDs to access banking, telecoms, or public services – suggest a growing shift towards making digital-ID effectively compulsory.

From a rights-based perspective, any move towards mandatory use must meet key legal criteria:

- **Legality:** A clear legal basis must exist that is grounded in formal legislation, not administrative discretion.
- **Necessity and proportionality:** The mandate must serve a legitimate aim and be proportionate to that aim.
- **Safeguards and oversight:** The law must allow for judicial review and provide avenues for redress.
- **Inclusion:** Alternatives or exemptions must be available for individuals unable to enrol due to barriers such as disability, lack of documentation, or geographic isolation.

At present, Liberia has not established:

- A statutory obligation requiring mandatory use;

- Defined penalties for non-enrolment; or
- Legal provisions ensuring alternative identification pathways for marginalised or excluded groups.

The absence of a comprehensive legal framework governing mandatory use raises concerns about potential rights violations and exclusion. Legal clarity and safeguards are essential to ensure the system respects individual freedoms and promotes inclusive access to services.

5. Risk-based tests

Contextual overview of risk in Liberia's digital-ID system

Liberia currently has no comprehensive data protection law in force, though relevant provisions exist across sectoral regulations (DLA Piper 2025). Liberia's biometric digital-ID system, established under the NIR Act of 2011, was envisioned as a transformative tool to streamline governance, enhance service delivery, and foster financial and social inclusion. Designed as a foundational ID, it is intended to underpin identity verification across key sectors such as health care, voting, education, financial services, and social welfare programmes.

However, the implementation of this system has unfolded in a post-conflict environment characterised by weak institutional frameworks, low public trust, and a lack of robust legal safeguards. Liberia's fragile socio-political context heightens the potential for rights violations, systemic exclusion, and misuse of digital-ID data. The absence of a comprehensive data protection framework and independent oversight exacerbates these vulnerabilities, leaving biometric and demographic data at risk of unauthorised access, profiling, or surveillance – without mechanisms for redress.

Global best practices, particularly those outlined in the CIS risk-based approach to digital-ID governance and the World Bank's Principles on Identification, emphasise that a rights-respecting and inclusive digital-ID ecosystem must be guided by a risk-based governance framework. This means that risks must be assessed, mitigated, and monitored across the entire ID lifecycle – from enrolment to data use to redress – especially for high-risk use cases and vulnerable populations.

Yet, Liberia's digital-ID system lacks a structured approach to risk governance. It does not incorporate privacy impact assessments (PIAs), proportional safeguards, or tiered data access frameworks. Additionally, there are no legal or institutional mechanisms to recalibrate or suspend ID system operations in cases of abuse, mission creep, or systemic failure. The absence of an independent DPA further compounds this, leaving citizens – particularly rural dwellers, undocumented individuals, and minority groups – exposed to harm without recourse.

Against this backdrop, the CIS framework proposes four critical risk-based questions for evaluating digital-ID systems. These serve as a diagnostic lens for assessing Liberia's system and identifying pathways for reform.

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

Liberia's NIR Act of 2011 does not mandate structured risk assessments such as PIAs, data protection impact assessments (DPIAs), or human rights impact assessments. Consequently, the current digital-ID governance framework lacks mechanisms to evaluate potential risks such as surveillance, exclusion, and data breaches.

This omission contrasts with international best practices. The Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD 2025) emphasise the necessity of risk assessments and privacy management programmes to ensure data protection and accountability.

In the context of Liberia – characterised by limited digital literacy and institutional capacity – the absence of mandated risk assessments heightens vulnerabilities. To align with global standards and safeguard individual rights, it is imperative for Liberia to legislate formal, recurring risk assessment mechanisms throughout the digital-ID system's lifecycle, especially concerning biometric data and third-party access.

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

Liberia's digital-ID legal framework – principally governed by the NIR Act of 2011 – does not incorporate a differentiated or risk-based approach to governing the use of digital-ID data. The act applies uniformly across all use cases, without distinguishing between low-risk activities (such as school enrolment or civil registration) and high-risk applications (such as law enforcement or financial surveillance).

This lack of nuance fails to account for the varying degrees of sensitivity and potential harm linked to different uses of personal and biometric data. As noted by the World Bank's Identification for Development Principles on Identification, robust digital-ID systems must implement risk-based safeguards that reflect the specific threats to individual rights in each context (World Bank 2020b; World Bank 2024).

In contrast, countries such as Canada and Estonia have adopted tiered digital-ID governance models, where higher-risk applications (e.g. national security, criminal justice) are subject to stricter legal thresholds, oversight,

and data protection mechanisms (Government of Canada 2022).[12] These frameworks include mechanisms such as judicial authorisation, purpose limitation, and restricted third-party access based on risk severity.

Moreover, biometric identifiers – such as fingerprints and facial images – are particularly sensitive due to their permanence and potential misuse. International standards, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD 2025), recommend that systems handling such data apply heightened safeguards, especially when used for surveillance or profiling.

Liberia's legal framework currently lacks:

- Legal differentiation between routine vs sensitive use cases;
- Oversight mechanisms for security or law enforcement access; and
- Special protections for vulnerable groups, such as women, children, displaced people, and ethnic minorities.

To align with international best practices, Liberia should embed risk-tiered safeguards into its legal framework. This includes requiring PIAs for high-risk applications, and legally mandating greater protections for biometric data and sensitive demographic categories.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

Liberia's legal framework for digital-ID, primarily the NIR Act of 2011, lacks explicit provisions ensuring that data collection and processing are proportionate to the intended purposes and associated risks. The act mandates the collection of biometric data, such as fingerprints and facial images, and their centralised storage without offering individuals meaningful choices, opt-out options, or clear purpose limitations.

Furthermore, Liberia does not currently have a dedicated data protection law or an independent authority to oversee data governance and address grievances related to digital-ID usage.

This absence of a comprehensive data protection framework means there are no mandated requirements for data minimisation, decentralised storage, or role-based access controls – measures that are standard in jurisdictions upholding data protection and privacy rights.

12 See also ID4Africa (2022).

The lack of proportionality in governance structures raises concerns about potential violations of fundamental rights, including the right to privacy and protection against arbitrary interference, as enshrined in international instruments such as the International Covenant on Civil and Political Rights and the African Charter on Human and Peoples' Rights.

To align with international best practices, Liberia should consider:

- **Enacting comprehensive data protection legislation** that incorporates principles of proportionality, data minimisation, and purpose limitation.
- **Establishing an independent DPA** with the mandate to oversee digital-ID systems, conduct PIAs, and enforce compliance.
- **Implementing oversight mechanisms** to assess the proportionality of data use and to issue binding directives when overreach is identified.

By adopting these measures, Liberia can ensure that its digital-ID system operates transparently, respects individual rights, and is governed in a manner proportionate to the risks involved.

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

Currently, Liberia lacks an independent oversight body specifically mandated to monitor the digital-ID system in alignment with legal and human rights standards. The NIR Act of 2011 establishes the institutional framework for identity management but does not provide for an autonomous authority to oversee data processing, privacy protection, or redress mechanisms (see also LRC 2021).

This gap contradicts regional and international best practices, including the ECOWAS Supplementary Act on Personal Data Protection (2010), which recommends the establishment of independent supervisory authorities (ECOWAS Commission 2010), and the African Charter on Human and Peoples' Rights (OAU 1981), which obligates states to uphold privacy and due process. Moreover, Liberia's draft Data Protection and Privacy Policy (2019) also emphasises the need for independent enforcement mechanisms (Government of Liberia 2019).

In contrast, countries such as Ghana and Senegal have established data protection authorities that oversee digital-ID systems and ensure compliance with privacy laws and human rights obligations (UNECA 2020).[13]

Recommendation

Liberia should urgently establish a legally mandated, independent DPA with the power to audit, investigate, and halt digital-ID operations where rights violations are found. This body should also report transparently and work in coordination with civil society and international human rights bodies (UNDP 2023; ITU 2021).

13 See also UNECA (2023) and ECDPM (2023) for broader discussion of risks and challenges in African digital-ID systems).

6. Conclusion

This report examined whether Liberia's digital-ID system, as currently governed by the NIR Act of 2011, meets the principles of a rules-based, rights-respecting digital governance framework as defined by the CIS and Research ICT Africa (RIA). Using the six test questions from the CIS/RIA assessment framework, the analysis revealed substantial governance gaps and institutional weaknesses that undermine the effectiveness, legality, and human rights compliance of the digital-ID system.

Key findings by test area

1. **Legislative mandate:** While Liberia's digital-ID system is backed by the NIR Act of 2011, this law is outdated and lacks alignment with contemporary data protection and human rights standards. It does not mandate core safeguards such as DPIAs or privacy-by-design principles.
2. **Legitimate aim:** The stated goals of enhancing service delivery and security are broadly legitimate, but the NIR Act of 2011 lacks specificity in defining the precise and limited purposes for which digital-ID data may be used. This opens the door to potential mission creep.
3. **Defined actors and purposes:** The law does not clearly define the full set of actors who can access or use ID data. Nor does it provide adequate protections for individuals – including the right to access, correction, or to object to data processing. High-risk uses, such as for criminal investigations or national security, are not treated with enhanced safeguards.
4. **Redress mechanisms:** There is a lack of meaningful grievance redress mechanisms. No independent oversight body exists to receive complaints or investigate harms caused by the misuse of ID data, leaving affected persons – especially from marginalised communities – without avenues for remedy.
5. **Accountability:** Liberia does not currently have an independent and adequately resourced DPA with powers to regulate, audit, or enforce rules related to the use of digital-ID data. This severely limits institutional accountability.
6. **Mission creep:** The law does not impose clear limitations on the expansion of digital-ID use cases. The absence of a purpose limitation clause or periodic review processes makes it difficult to monitor or prevent function creep, particularly in politically sensitive areas such as voter registration or surveillance.

Policy and practice recommendations

To align Liberia's digital-ID ecosystem with international human rights and data governance standards, the following actions are recommended.

1. **Enact a comprehensive data protection law**
   - Pass a dedicated data protection law that mandates PIAs and DPIAs.
   - Establish risk-based usage tiers, data minimisation principles, and legal bases for processing personal data.
   - Include rights for individuals (access, correction, objection, and erasure), and mechanisms for effective remedy.
2. **Establish an independent DPA**
   - Create a legally empowered, independent DPA with the capacity to conduct audits, issue penalties, and oversee digital-ID operations.
   - The DPA should monitor compliance with proportionality, necessity, and purpose limitation principles.
3. **Amend the NIR Act of 2011 to reflect rights-based principles**
   - Explicitly define high-risk use cases, such as biometric data usage, law enforcement access, or cross-border data sharing, and subject them to heightened legal safeguards.
   - Clarify the specific, legitimate purposes of digital-ID use and introduce a purpose limitation clause to prevent mission creep.
4. **Introduce emergency contingency protocols**
   - Develop a legal framework to pause or modify ID operations in response to technical failures, data breaches, or mass exclusion events.
   - Include public reporting obligations when emergency powers are triggered, to maintain transparency.
5. **Expand public transparency and engagement**
   - Publish regular transparency reports, including statistics on ID issuance, data-sharing practices, breach incidents, and redress. As of now, Liberia does not have an independent oversight body specifically mandated to monitor the digital-ID system. The NIR Act of 2011 lacks provisions for such a body to ensure the system operates in line with legislation and Liberia's human rights commitments. This absence leaves gaps in accountability, transparency, and redress.
6. **Improve accessibility and inclusion measures**
   - Enable alternative registration mechanisms for individuals without standard documents (e.g. community attestations).

- Provide non-biometric fallback options (e.g. personal ID numbers or digital tokens) for individuals unable to complete fingerprint or facial recognition due to physical limitations.
- Implement mobile and rural registration teams to reduce geographic exclusion.

7. **Commission further research and evidence gathering**
   - Conduct a comprehensive audit of exclusion from digital-ID across Liberia, especially among rural, informal, stateless, or marginalised populations.
   - Study the impact of biometric failure rates and system downtimes on service delivery and citizens' rights.

Final reflection

A secure, inclusive, and rights-respecting digital-ID system is central to Liberia's digital transformation and governance reform. However, to move from aspiration to accountability, Liberia must build legal, institutional, and technical safeguards that balance innovation with protection. Enacting reform now – before the full scale-up of the ID ecosystem – will help ensure that Liberia's digital-ID system promotes dignity, access, and justice for all.

Recommendation

Liberia should urgently establish a legally mandated, independent DPA with the power to audit, investigate, and halt digital-ID operations where rights violations are found. This body should also report transparently and work in coordination with civil society and international human rights bodies (UNDP 2023; ITU 2021).

7. Bibliography

AfDB (2022) ***African Economic Outlook 2022***, Abidjan: African Development Bank (accessed 14 October 2025)

AU (2014) ***African Union Convention on Cyber Security and Personal Data Protection***, Malabo: African Union (accessed 14 October 2025)

DataReportal (2025) *Digital 2025: Liberia*, DataReportal, Kepios and We Are Social

DLA Piper (2025) ***Data Protection Laws of the World: Liberia***, DLA Piper (accessed 14 October 2025)

ECDPM (2023) ***Digital ID Systems in Africa: Challenges, Risks and Opportunities***, ECDPM Discussion Paper 360, Maastricht: European Centre for Development Policy Management (accessed 14 October 2025)

ECOWAS Commission (2010) ***Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS***, Thirty-seventh Session of the Authority of Heads of State and Government, Abuja, 16 February (accessed 14 October 2025)

EU (2016) '***Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)***', *Official Journal of the European Union*, 4 May (accessed 14 October 2025)

Government of Canada (2022) ***Digital Trust Series: Part 1 – Digital Identity*** (accessed 14 October 2025)

Government of Liberia (2019) ***Liberia Information and Communications Technology (ICT) Policy 2019–2024***, Monrovia: Ministry of Posts and Telecommunications (accessed 15 October 2025)

Government of Liberia (2011) **National Identification Registry (NIR) Act of 2011**, Monrovia: Ministry of Foreign Affairs (accessed 15 October 2025)

Government of Liberia (1986) ***An Act to Repeal PRC Decree #65 Establishing the National Identification Card System and to Establish in Lieu Thereof the National Identification Registry***, Monrovia (accessed 15 October 2025)

ID4Africa (2022) ***Identity in Context: The Digital Transformation Journey Begins***, Augmented General Meeting, Palais des Congrès, Mövenpick Hotel Mansour Eddahbi, Marrakesh, Morocco, 15–16 June (accessed 15 October 2025)

ITU (2018) ***Digital Identity Roadmap Guide***, Geneva: International Telecommunication Union (accessed 15 October 2025)

ITU-T (2021) ***Recommendation ITU-T X.1252: Baseline identity Management Terms and Definitions***, Geneva: International Telecommunication Union (accessed 15 October 2025)

LRA (2024) ***LRA 2023 Annual Report***, Liberia Revenue Authority (accessed 15 October 2025)

LRA (2022) ***LRA Interim Plan 2022***, Liberia Revenue Authority (accessed 15 October 2025)

LRC (2021) *Legal Implications of Digital Identity in Liberia: A Regulatory Review*, Monrovia: Law Reform Commission of Liberia

Ministry of Internal Affairs (2025) ***Annual Report 2024***, Monrovia: Ministry of Internal Affairs (accessed 15 October 2025)

Ministry of Justice (2024) *Annual Report 2024*, Monrovia: Ministry of Justice, Government of Liberia

NIR (2019) *Annual Report*, National Identification Registry

OAU (1981) ***African Charter on Human and Peoples' Rights***, Nairobi: Organization of African Unity (accessed 15 October 2025)

OECD (2025) ***Recommendation of the Council Concerning: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,*** OECD Legal Instruments, Organisation for Economic Co-operation and Development (accessed 15 October 2025)

Orange Middle East & Africa (2024) ***Cultivating Impact: Orange Middle East & Africa 2024 Corporate Social Responsibility Report***, Casablanca: Orange MEA (accessed 15 October 2025)

UN (1966) ***International Covenant on Civil and Political Rights***, New York: United Nations (accessed 15 October 2025)

UNDP (2023) ***Drafting Data Protection Legislation: A Study of Regional Frameworks***, New York: United Nations Development Programme (accessed 14 October 2025)

UNDP Liberia (2023) ***Strengthening Governance and Inclusive Green Growth: Liberia Annual Report 2023***, Monrovia: United Nations Development Programme Liberia (accessed 14 October 2025)

UNECA (2023) ***Africa Digital ID Landscape 2022***, Addis Ababa: United Nations Economic Commission for Africa (accessed 15 October 2025)

UNECA (2020) ***Regulating Digital Data in Africa***, Governance and the Digital Economy in Africa Technical Background Paper Series, Addis Ababa: United Nations Economic Commission for Africa (accessed 15 October 2025)

World Bank (2024) ***ID4D Global Dataset 2021: Volume 2 – Digital Identification Progress & Gaps***, Washington, DC: World Bank (accessed 15 October 2025)

World Bank (2023) *Digital Progress and Trends Report 2023*, Washington, DC: World Bank

World Bank (2020a) ***Liberia Digital Economy Assessment: Summary Report***, Washington, DC: World Bank (accessed 15 October 2025)

World Bank (2020b) ***Identification for Development (ID4D) 2019 Annual Report*** (accessed 15 October 2025)

World Bank (2016) ***ID4D Country Diagnostic: Liberia***, Washington, DC: World Bank (accessed 15 October 2025)

Digital-ID in Ethiopia: Country report

Helen Beny

 DOI: 10.19088/IDS.2025.060

1. Introduction

Ethiopia is the second largest country in Africa and has an ethnically diverse population of over 134 million people (DataReportal 2025). However, over the past decade there has been ethnic conflict, political instability, digital repression, and, most recently, civil war (Abebe and Ahadu 2020; Access Now 2022).

Leading up to peace talks, in 2022 Ethiopia introduced the first National Identification Program (NIDP), also known as Fayda (ፋይዳ), which means 'value' or 'importance' in Amharic (Mohamed and Santoro 2024). However, the NIDP has raised some concerns, since the government has engaged in digital repression and surveillance (Zelalem 2023). The digital identification (digital-ID) project is 'a process of using human data for authentication', which includes biometric data such as fingerprints and iris scans (Wodajo 2022: 1). It is pertinent to critically review the national digital-ID programme to ensure that it does not lead to 'dataveillance' – 'a systematic monitoring of people's actions or communication through the application of information technology' (Clarke 1991: 1). To address this concern, the report is guided by the following questions: what is the current state of digital-ID in Ethiopia? What legislative framework(s) are in place? And, if any, do they protect against all forms of dataveillance? To answer these questions, the report will use the Centre for Internet and Society framework for assessing digital-ID systems (Bhandari, Trikanad and Sindha 2020).

The remaining sections of the report will be organised as follows. The report will begin by providing a brief historical overview of Ethiopia's digital-ID systems and outlining the current state of the digital-ID project. It will include procedural information to highlight how ID can be obtained, what documents are needed for registration, who has funded the project, and what still needs to be done. The final sections analyse Ethiopia's legislative framework and assess it against the rule of law, rights-based, and risk-based tests (*ibid.*).

2. History of ID in Ethiopia

Ethiopia's ID history is well-documented since 1991; however, there is limited information that pre-dates this period. In 1907, Emperor Menelik II received the first driver's licence in the country, a paper-based functional ID that was available for anyone who passed their driving exam (Kebret 2008). Under the Derg military regime (1974–91), local administration, known as the *kebele*, was formalised in 1975 (HRW 2005). A *kebele* is a grouping of small communities, and the *kebele* official would assist with the implementation of various ambitious initiatives for rural development and land reform; however, it quickly became a tool for surveillance (Wiebel and Admasie 2019). *Kebele* officials were expected to monitor individuals in their community and report any anti-government behaviour (HRW 2005). During this period, if you required access to government services outside of your community, registration for school, or to visit a doctor, you would obtain a letter from a *kebele* official to verify your identity and place of residence (*ibid.*). At the age of 18 years and over, you would register for a *kebele* ID, a paper-based ID system, and it would include an individual's name, date of birth, address, and ethnicity. While there is limited official documentation of this ID system during the Derg era, Ethiopians confirm its existence and that the *kebele* ID was also used to monitor and surveil opposition groups, especially during the so-called 'Red Terror', a violent campaign of political repression launched by the Derg military regime to eliminate the opposition from 1976 and 1978 (Wiebel 2017).

Since 1991, Ethiopia has been an ethnic federalist state, composed of nine semi-autonomous regional states and two multi-ethnic cities (Addis Ababa and Dire Dawa) (Aalen 2006; Addis 2022). In 1994, the ethnic federalist system was adopted to address the country's long-standing ethnic grievances (Taye 2017). Regional governments were more representative of an individual's identity and a national-ID was unnecessary for domestic purposes (Addis 2022).

Under the Ethiopian People's Revolutionary Democratic Front (EPRDF), the ethnic federalist political coalition, the government continued to assign the *kebele* with the authority to provide foundational forms of ID such as birth certificates and universal regional identity cards called *kebele* ID, which also indicate the bearer's ethnic designation (Novogrodsky 1999). There are over 16,000 *kebele*s in the country; the system is decentralised and the registration process can vary between neighbourhoods (World Bank 2016). Applicants must be 18 years or older to apply for a card, and they are expected to pay 10–40 Ethiopian birr (equivalent to US$0.07–0.10) (Kitzmüller

2020). To register for the *kebele* ID, applicants must provide evidence in the form of a foundational ID, such as a birth certificate, vaccination card, or school certificates. However, many people are unable to provide sufficient evidence to receive a *kebele* ID. For instance, women were 15 per cent less likely than men to obtain a *kebele* ID in 2022 (Casher and Clark 2024).

The *kebele* ID is a foundational ID that legally confirms an individual's identity and residence at regional and local levels. However, there are additional details on the *kebele* ID: mother's name, date of birth, occupation, ethnic group, emergency contact details, date of issue, issuing offices, and a *kebele* stamp (World Bank 2016). This system is paper-based and decentralised, which leads to several issues surrounding authenticity and traceability because it lacks a central database. There are variations on the card: simple cards with a stamp, or folded booklets; some cards are pre-printed on paper, whereas others are filled in by hand at the *kebele* office (World Bank 2016). With a *kebele* ID you can obtain other forms of functional ID such as a tax ID number (TIN), driver's licence, and passport (Kitzmüller 2020). However, millions of Ethiopians lack any form of formal ID necessary to obtain a *kebele* ID such as, a birth certificate or local ID (World Bank 2023). Without a *kebele* ID you are unable to access services such as banking, loans, public health care, or education, to purchase a home, to vote, to participate in elections for public office (elections), or to obtain a passport (Casher and Clark 2024).

2.1 Digital penetration in the country

As Ethiopia digitalised aspects of social, economic, and political life, the government launched a national strategy in 2021 titled Digital Ethiopia 2025 (Aratek 2024), which includes the national digital-ID programme. The case for digitalising ID is often linked to the increased use of digital technologies in social, economic, and political life. Internet access is a challenge. As of 2025, internet penetration is 21.3 per cent, which translates to approximately 28.6 million internet users (DataReportal 2025). The proportion of cellular mobile connections is higher, at 63.8 percent, which accounts for 85.4 million people (*ibid.*). Studies also show that men aged 20–35 with a post-secondary education are more likely to be online than any other segment of the population (CARD 2018). Most internet users live in the metropolitan area of Addis Ababa, and individuals with higher incomes spend the most time online (*ibid.*; Ambelu 2024). This is alarming because only 23.9 per cent of Ethiopia's population live in urban centres, and 76.1 per cent live in rural parts of the country (DataReportal 2025). Furthermore, women, particularly in rural areas, face additional barriers to internet access due to lower incomes, cultural norms, and limited digital literacy (Ambelu 2024).

2.2 Current state of the digital-ID project

In 2021, Ethiopia officially launched the NIDP, also known as the Fayda Digital ID initiative, a foundational ID system for legal residents and citizens to connect to all public services. The project was piloted in 2022, and leading up to the pilot, 3.5 million people in Ethiopia registered (ID4Africa 2022). In 2023, the government enacted the Ethiopian Digital ID Proclamation to establish a legal framework for the digital-ID system. The provisions included parameters for data collection, storage, and usage (Proclamation No. 1284/2023). As of February 2025, 12.2 million individuals had a Fayda ID, and the government planned to reach 90 million registrations by 31 December 2026 (Macdonald 2025b).

2.3 What documents are needed to register?

The government has a clear objective to make registration simple and accessible. To further reduce any barriers, there are 33 acceptable registration documents, such as a *kebele* ID, passport, birth certificate, driver's licence, refugee ID, and bank book. In addition, should an individual not have access to any of the listed documents, they are also eligible to enrol if a current Fayda ID holder can attest to an applicant's identity (National ID 2025b). While the latter is helpful for displaced individuals, it is unclear whether this form of verification will be exploited.

To register for Fayda, applicants must pre-register online and submit their basic demographic data, including their current address, date of birth, and gender (Aratek 2024). Alternatively, in Addis Ababa's sub-cities (administrative zones), they can register in person at any of the Civil Registration and Residency Service Agency branch offices, service branches, or other designated registration centres such as branches of state-owned telecoms company Ethio telecom and select banks across the country (National ID 2025b). Once pre-registration is complete, applicants must visit any of the registration centres[14] across the country to provide their biometric data, which includes fingerprint scanning (all fingers), a facial photo, and iris scans of both eyes, and to have their ID documents verified (*ibid.*). According to the NIDP, Fayda uses local languages during the registration process to ensure informed consent (National ID 2025a). Following verification, applicants receive an SMS (text message) with their 12-digit Fayda ID number and they can access their code through the Fayda app. However, if an individual does not have access to a mobile (cell) phone or cannot receive an SMS, they can request a physical card for 350 birr that includes a 2D barcode and their Fayda ID number. The Fayda

14 See the network of Fayda registration centres.

ID programme therefore includes several key features: a unique 12-digit ID number; biometric data; a 2D barcode; a digital-ID, which is accessible through the Fayda mobile app; and a physical ID card (Awol 2025).

2.4 Who can register? What groups are included and excluded?

According to Ethiopia's Digital ID proclamation, residents who live in Ethiopia (with or without) proof of citizenship, and foreign residents who live or work in the country from the age of five years and up are permitted to register for Fayda. Individuals who do not have a proof of address can apply if they have formally declared their residence with the relevant authorities, such as the Civil Registration and Residency Services Agency. Furthermore, refugees and asylum seekers can also register for a Fayda ID through a new partnership between the NIDP, the government's Refugees and Returnees Services and the United Nations Refugee Agency (UNHCR) (Abdirahman 2024; UNHCR 2024). However, it is unclear how they will access a printed copy without an address, and/or a digital copy mobile device. Capturing fingerprints may be problematic for people who have disabilities, elderly people, and day labourers, who may be unable to provide this biometric data; for example, because 'their fingerprints may be faded and unreadable by the system' (Zelalem 2023).

2.5 Which government departments are involved?

Ethiopia's NIDP is led by the Prime Minister's Office through the National Identification Authority and, to launch the project, four government agencies agreed to integrate and assist in service delivery: the Ethiopian Artificial Intelligence Institute, the Information Network Security Administration, the Addis Ababa Civil Registration and Residency Service Agency, and the Addis Ababa Innovation and Technology Development Bureau. Over 33 integrated agencies and various organisations are assisting in rolling out the project, providing authentication services and issuing Fayda ID credentials. These partners[15] include public and private institutions such as Ethio telecom (29 locations), the Ministry of Revenue (25 locations), and nine banks including Hibret Bank, Nib International Bank, and Bank of Oromia (National ID 2025b). NIDP officials have indicated that banking is a key sector due to the low financial inclusion rate (ID4Africa 2022). For instance, as of January 2025, the government introduced a new policy for Addis Ababa, stating that all bank customers were required to link their bank account(s) to their Fayda ID, and that this policy would be rolled out across the country by 31 December 2026,

15 Partners are listed on the **National ID website.**

which could lead to economic exclusion (Kaberia 2025). Furthermore, the government has also integrated the TIN with Fayda to increase efficiency and strengthen the tax database (Mohammed and Santoro 2024).

2.6 Which funders are involved?

The NIDP is funded by the federal government; the World Bank committed US$350 million in December 2023 (World Bank 2023). The NIDP has also received a US$50 million grant from the World Bank International Development Association's Window for Host Communities and Refugees (National ID 2025b). The United Nations Economic Commission for Africa also supports the implementation of the Good Digital ID Framework Principles in Ethiopia (UNECA 2023). Laxton[16] is a data management company that specialises in proprietary software systems and has partnered with the NIDP to roll out the Modular Open-Source Identification Platform in Ethiopia – an open-source platform on which to build the digital-ID system (Macdonald 2024) Laxton is leveraging its identity registration expertise, and its equipment addresses the country's connectivity concerns because it can complete ID registrations with or without an internet connection or electricity (*ibid.*).

2.7 What still needs to be done?

From 2025 to 2030, the government and the NIDP seek to register 72 million people, and to reach 90 million (residents and non-residents) by 2030. However, it is worth noting that Ethiopia's population is projected to reach 150 million by 2030 (UNDP 2023). In 2025, the NIDP conducted a self-evaluation report, noting that it needs to address technical and environmental implications to achieve the projected growth (National ID 2025a). In particular, the system needs to expand to support additional use cases in a secure manner (*ibid.*). Furthermore, policies, processes, and procedures need to be reviewed to address potential changes in the digital ecosystem (*ibid.*). Other areas for improvement listed in the report include transparency, usability, and maintaining the biometric system (*ibid.*). To achieve its goal, the NIDP is also working on improving access and inclusion, and building trust, in rural Ethiopia (*ibid.*).

16 Laxton describes itself as an 'identity systems integrator'.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

On 18 April 2023, the government passed the Ethiopian Digital Identification Proclamation 1284/2023, approved as Proclamation No. 1284/2015, which is the legal basis for the national digital-ID project (Federal Democratic Republic of Ethiopia 2023).

On 24 July 2024, the government passed a more comprehensive Personal Data Protection Proclamation (PDPP) No. 1321/2024. The PDPP establishes a more uniform framework for protecting personal data; the regulatory institution is more clearly defined and addresses data localisation, privacy, and protections for citizens. As a result, the Ethiopian Communications Authority is the independent supervisory authority responsible for data processing in Ethiopia (Shemsu 2025).

The law is clear that registrants can update any data that is collected by the Digital Identification System (Federal Democratic Republic of Ethiopia 2023: Sec. 2). Relying parties, also known as partners, are institutions and persons that authenticate an individual's identity. Relying parties are broadly defined and citizens must go to the National-ID website to identify the relevant institutions and relying parties for registration (*ibid.*: Sec. 3). The law clearly states that all personal data that is collected belongs to the registrant, and any authentication requires the registrant's consent (*ibid.*: Sec. 4.17). In Ethiopia, personal data protection is more clearly defined under the PDPP than under the Digital Identification Proclamation.

Quality of the law

The law broadly outlines the procedure and details for appeals and sanctions, with minimal delegation to external courts. The law clearly outlines criminal liability and punishments for any person who refuses a digital-ID as a form of ID, who collects more data than needed, or who transfers the data collected to a third party.

Clarity and precision of the law

The law is published online, and the language is clear and understandable; terms are defined, but the language may still pose a challenge to the average citizen. There are several accessibility concerns relating to

technological access, literacy, and language. Based on Ethiopia's internet penetration rate of 23.9 per cent, 28.6 million individuals are using the internet, which is less than one in four individuals (DataReportal 2025). Furthermore, those who are predominantly online are men between the ages of 20 and 35 (CARD 2018). The literacy rate was 51.8 per cent as of 2017 (World Population Review 2017). Thus, only half of the population can read what is outlined and only a quarter of individuals can access the proclamation. The proclamation is written in Amharic and English: 29 per cent of the population speak Amharic and far fewer are proficient in English (World Bank 2007). Considering the linguistic makeup of the population, the proclamation should be translated into all local languages to ensure that citizens are informed of the process and the protections.

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

The governing law outlines clear objectives, stating that the purpose is to provide every Ethiopian and resident the right to be identified and to enhance their ability to exercise other rights. Prior to the digital-ID system, many Ethiopians lacked any form of foundational ID, and such records as existed were stored by each *kebele*.

The government's objective is that the digital-ID will support development and good governance, and build trust between service providers and service recipients. The government also suggests that establishing a nationwide digital-ID will enhance institutions, and contribute to building more reliable and secure systems that can ensure peace, security, and reinforce the justice system. Overall, the law broadly defines the purpose of the digital-ID, but it is unclear where registrants will use the ID.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

The proclamation outlines the legal relationships between various stakeholders in the digital-ID system: the registrant, the registrar, the relying party, the authentication service provider, and the digital-ID institutions. The proclamation defines these actors and institutions quite broadly. For instance, the proclamation does not name a clear

authority and, 'Institution' is defined as '[meaning] a Governmental Digital Identification entity that will implement the Digital Identification System and execute this Proclamation, or it may be an office established within a relevant Government body' (Proclamation No. 1284/2023: 3).

The proclamation outlines the nature of the data that is subject to collection during the registration process and what information will be visible on the digital-ID. The proclamation also outlines that the registrar is the operator that is entrusted by the 'Institution' to collect individuals' data. The registrant can modify the data if it is incorrect. They are also required to update any necessary information if the set information changes, or if it is lost or damaged due to disaster. However, it is unclear whether registrants can opt out or if they have the right to delete their data once they have registered.

Registrars are not listed in the proclamation, but the NIDP website provides more detail – it includes various ministries, financial institutions, and Ethio telecom. Registrars are permitted to access and use the data collected, but they are obligated to notify registrants and obtain their consent before processing it. Registrants receive a standard consent form that is prepared by the Digital Identification System, which describes these obligations, and it must be signed by the registrant as proof of consent; however, it is not clearly outlined how registrars will gather subsequent informed consent (Federal Democratic Republic of Ethiopia 2023: Sec. 4.16). Furthermore, personal data may be disclosed or transferred to a legal authority if it is subject to a court order. The proclamation also notes that anonymised data can be shared with legally authorised parties in the form of summarised demographic reports and statistical data. However, this data could be de-anonymised (Ohm 2010); if so, it could reveal the identities of individuals associated with the data, or it could be used to infer ethnicity or even behaviour, which poses greater privacy concerns.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

Section four of the proclamation outlines the avenue for grievances and complaint redress. Any person can file a complaint with the pertinent court if they are dissatisfied with the decision. Grievances need to be investigated and closed within 30 days even if the complaint is unresolved. There are no clear examples of the redress mechanism in practice. In addition, if registrants are still unsatisfied with the redress process, they can file a grievance with the World Bank Grievances Redress Service.

The institution tasked with developing a complaint department for grievances is under the Project Implementation Unit and the Ministry of Innovation and Technology. If the data is sold or shared beyond these groups the law outlines criminal penalties for various acts or grievances. These penalties can be applied if a service provider refuses a digital-ID as form of legal ID, if a registrar collects more data than needed, and/or if they transfer any data that is collected. Penalties are also categorised based on the actor, not on the offence.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

The NIDP is under the directive of the Prime Minister's Office. According to the Stakeholder Engagement Plan, the NIDP released an information disclosure plan, which states that to ensure accountability, information will be disclosed regarding data privacy and security, building an inclusive approach, emphasising consent and control, and upholding a pedigree of transparency by releasing findings through the NIDP website. In addition, stakeholder engagement meetings will be held, and printed copies of the findings will be published. The bodies that are responsible for the release of this information are the NIDP and the Ministry of Innovation and Technology. However, there does not seem to be an adequate system for accountability as there are no clear deadlines for these reports or mandatory updates to the public.

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

The law outlines the purpose of the digital-ID system, but does not clearly outline where the ID will be used, nor does it stipulate that the ID is mandatory to access public services. However, the NIDP has announced that it is 'going one step further' (National ID n.d.) and will be linking Fayda ID credentials with other essential services such as banking, telecoms, and medical records, which is a form of mission creep (National ID 2025a). For instance, Fayda ID has become mandatory for 'public servants, the tax system, government procurements, facilitation of domestic flights with Ethiopian airlines' (Macdonald 2025b). The Ethiopian government also released a policy that requires the use of Fayda for banking transactions (ID Tech 2025). The National Bank of Ethiopia (NBE) has mandated that as of 1 January 2025, individuals banking in Addis Ababa must register for the Fayda ID to open a bank account (Shega 2024). The NBE has provided a temporary

waiver for Ethiopia-born foreign nationals currently residing abroad, allowing them to continue to access their accounts (*ibid.*). These various policies and requirements strongly encourage citizens to register (Kaberia 2025; Macdonald 2025c), and failing to do so can lead to marginalisation (Kaaniru and Muindi 2024). Furthermore, a Fayda ID will also become a requirement for registration in schools by September 2025 (Macdonald 2025b). In the past, students registered for school using their birth certificate, but the new plan will require students aged five and above to provide their Fayda ID (*ibid.*).

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

The collection and use of data is defined under Section 2 of the digital-ID proclamation, Digital Identification System Principles Enrollment, and Service Provisions, which includes nationality, date of birth, gender, and domicile address. The government seeks to engage in data minimisation and the registrar is required to ascertain consent before using any data.

It is concerning that citizens will register with various public and private institutions, and that this data will be transferred to the Fayda portal, which could lead to privacy concerns. All data is currently stored locally, but the proclamation does not provide clear details surrounding future measures. For instance, there is a provision that permits cross-border data transfer for storage granted on the condition that the jurisdiction can demonstrate adequate data controls (Federal Democratic Republic of Ethiopia 2023: Sec. 2.18).

The proclamation protects citizens against data brokering (selling data) to third-party actors. Furthermore, the PDPP provides additional safeguards around data processing and sharing. However, there are some privacy violations that are not necessary to achieving the legitimate aim. For instance, partner organisations, which include Ethio telecom, financial institutions, and various ministries that are a part of the registration process, can store the information gathered in their own databases and use the information without violating its original purpose (*ibid.*: Sec. 17.8)

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

Data minimisation is listed as one of the principles in the proclamation. However, exorbitant amounts of data are collected beyond what is displayed on the digital-ID: The only personal data listed on the digital-ID is nationality, date of birth, gender, and residence address. However, at registration, the following personal information is also collected: mother's name, phone number, email address, and postal address (*ibid.*: Sec. 2.9).

Under the law, sensitive personal data is defined as the following:

> racial or ethnic origins, genetic data, physical or mental health or condition, political opinion, religious beliefs or other beliefs of similar nature, the commission or alleged commission of an offense, any proceedings for an offense committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court proceedings, any other personal data as the Institution or other authorised entities may determine to be sensitive personal data.
> (*ibid.*: Sec. 1.2)

The law states that this personal information requires protection and that it should not be collected in the digital-ID system (Yirga 2023).

The proclamation states that citizens are not required to register for a Fayda ID (*ibid.*). However, the government has already announced that a Fayda ID will be required for banking and school registration (Kaberia 2025; Macdonald 2025c). Furthermore, the NIDP has mentioned that it is working on linking Fayda ID credentials with essential services such as banking, telecoms, and medical records (National ID 2025b), which should be considered a form of mission creep. According to the proclamation, pending approval from the NIDP, partners (public or private institutions) such as the National Bank of Ethiopia, the Ministry of Revenue and Ethio telecom can require the use of the digital-ID to authenticate an individual to provide services. This has begun to take place – various reports mention that it is a government policy (ID Tech 2025), and procedurally, NBE has mandated the use of a digital-ID to access banking services (Shega 2024), which leaves room for mission creep.

Partner organisations may also receive a registrant's personal data from the NIDP or other authorised authentication service provider to authenticate the registrant's identity with their consent. However, if the partner organisation cannot obtain authentication from the NIDP, they can provide service(s) and use other methods for authentication. The NIDP still needs to outline how long the partner organisation can retain the registrant's personal data.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

According to the PDPP, when personal data relates to a subject, they have the right to be informed, which includes about: who has requested their data; the purpose of the processing; details of transfer; retention period;

right to withdraw consent; and details of the existence of automated decision-making, including profiling and more. Furthermore, the data subject has the right to obtain: confirmation of the processing of their data; communication in an accessible form of what data was processed; and the dates for which the data will be stored. Any other information that the data controller has must be shared to ensure transparency; it must be provided free of charge, at reasonable intervals, and without excessive delay (Federal Democratic Republic of Ethiopia 2024: Sec. 3.25). The PDPP provides better safeguards for citizens than the Digital Identification Proclamation does, and greater detail and nuance.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

If the registrant cannot provide biometric data due to disability, injury, or other reasons that affect their capacity, they are able to provide a photo for their ID instead. Furthermore, the registrar can issue a Fayda ID to an individual who cannot present themselves due to health, age, or other reasons beyond their control.

Government officials have said that Fayda ID will not display a person's ethnicity, to adhere to the data protection law, and an individual's consent is needed to reveal this information (Zecharias 2023). However, critics are still concerned that the implementation of the Fayda ID may lead to ethnic profiling of minority groups; this was also an issue in the case of Uganda's mandatory ID system (Kaaniru and Muindi 2024). The PDPP has some safeguards in place to protect the processing of data that may lead to ethnic profiling. However, it is unclear at this time how the PDPP will be implemented and, furthermore what shape prejudice might take. Critics say that despite these assurances a person's name can also be used to identify their ethnicity.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

In the initial stages, it was a voluntary project and the NIDP stated that citizens would be able to continue to use their *kebele* ID if they did not get a Fayda ID (Bosman 2023). Since December 2023, the TIN has been integrated into the Fayda ID to broaden the tax base, and increase monitoring and enforcement (Mohamed and Santoro 2024). This function was not listed in

the initial legislation. Since January 2025, the government has been moving towards mandatory requirements – for instance, a Fayda ID is needed for banking, education and potentially more services in the future (Kaberia 2025; Macdonald 2025c) – and this could lead to exclusion. There is no legitimate reason to mandate registration, but the government is increasingly taking this approach to reach the goal of 90 million registrations by December 2026.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

In 2021, the Ministry of Innovation and Technology undertook a broad risk assessment prior to the implementation of the digital-ID system. The government released the Environmental and Social Risk Screening Guideline for Partner/Beneficiary Institution and Technology (Ministry of Innovation and Technology 2021). It provides a broad assessment of Ethiopia's Digital Foundation Project, and within this plan the digital-ID system is listed as a central component to address the digital divide. Regarding digital-ID, the report identifies that marginalised communities could face a potential privacy risk and might unintentionally experience profiling (*ibid.*: 9). In 2023, the NIDP produced a stakeholder engagement report, briefly assessing the social risks and impact of the project, and reiterated this risk (National ID 2023). Lastly, in 2024 the NIDP and the government released the Environmental and Social Management Framework (National ID 2024). Overall, there is a chance of social exclusion if the digital-ID project is not distributed to underserved communities; however, no details have been provided about whether these groups were consulted (National ID 2023). It may also induce risk in the following areas: labour management, community health, and safety (National ID 2023: 3).

The Ethiopian government has identified the privacy risk and the risk source, and it has identified a way to avoid this risk through a call for representation during public stakeholder meetings during the rollout of the ID system, increasing accessibility and reducing barriers to ID verification. However, what is concerning is that it is unclear how the data or the digital-IDs will be used in practice, or how profiling will be mitigated. Furthermore, there is a growing risk of exclusion for individuals who do not register because the digital-ID is linked to education, and financial and other services. At this time, the government has not released a report to verify that these stakeholder meetings took place with historically marginalised groups.

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

The data collected for the digital-ID system is not harmful *per se* and the government has implemented provisions to refuse the use of the data for any reason other than for identification, taking a rights-based approach. To reiterate, the PDPP states that the data cannot be sold to or be used by third parties outside of partner organisations (Federal Democratic Republic of Ethiopia 2024). However, the law lacks strong limits around how partner organisations may use this data, which is concerning because if the registrant's data is used it would be considered harmful and potentially predatory. Citizens are required to register before 2026 to access basic services such as banking (ID Tech 2025), which is coercive because the government should not impose any conditions without demonstrating that they are legal, necessary, and proportionate. If an individual does not have a Fayda ID, they can register on the spot to receive those services (Yirga 2023). However, if a resident has not registered or refuses to register, it is unclear whether alternative ID can be used to access services despite initial promises that the *kebele* ID could still be used in its place (Zelalem 2023).

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

Currently, the government has not made provisions for independent governance in this area. However, it has made provisions for external participation by various stakeholders, including citizens, minority communities, and various institutions, to address potential risks.

In terms of risk and authentication errors, the system is designed to connect the identity of the individual to the unique 12-digit ID number. Thus far, Fayda has addressed identity theft issues, streamlined delivery of services, and increased efficiency in authenticating transactions (Macdonald 2025c). The government has a data protection law, but storage practices and data retention periods are not clearly outlined.

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

The government conducted an environmental and social risk assessment, and identified various ways to address this risk: increased involvement of stakeholders, a redress mechanism, and data protection law. However, it is unclear whether the government has enabled practices to mitigate risk. For instance, experts suggest that even traditional methods of verification are moving towards using digital methods to prioritise layered security, but these are not clearly defined (Macdonald 2025a).

6. Conclusion

Ethiopia's Fayda ID is the country's first national ID system, and it is increasingly integrated within society for services such as banking and taxation. The government has legislation to protect the personal data of its citizens, but there are concerns regarding implementation. Since the project is still in its early stages, little research has been conducted on its social impacts, and the legal provisions have yet to be tested in court.

This research focused on documenting the current phase of implementation and the legislation underpinning the digital-ID project in Ethiopia. It demonstrates that many actors are aware of the perceived benefits of the digital-ID system but are still concerned about the risks it poses to ethnic minority communities. The data protection laws and guidelines for redress indicate that the government has taken steps to address risks, but concerns around ethnic profiling are not clearly addressed.

According to the NIDP, the digital-ID system has increased efficiency, authentication, and integration of various ministries. Despite initial claims that the *kebele* ID could still be used, a Fayda ID will be mandatory to access banking, taxation, and education services, which is coercive (Kaberia 2025; Macdonald 2025c). This is an issue of mission creep. To address this, the government should allow individuals to access basic services using their *kebele* ID. Instead, the government is aggressively implementing the Fayda ID system, to support the government's goal of 90 million registrations. Since the project is in the implementation phase, it is unclear whether mass dataveillance is underway. However, there are some privacy concerns around data collection and the processing of this data. It will be critical for the NIDP to disclose how this data is processed and alert the public if any potential risks arise. The NIDP has released a self-evaluation report of the Fayda ID system (National ID 2025a), which provides limited insight and is marginally critical of its own efforts. However, it would have been more beneficial to the public if an independent body or the funding organisation had conducted an audit to ensure that the processes align with existing legislation, and that the data is not misused or transformed to augment mass surveillance repression.

7. Bibliography

Aalen, L. (2006) 'Ethnic Federalism and Self-Determination for Nationalities in a Semi-Authoritarian State: The Case of Ethiopia', *International Journal on Minority and Group Rights*, 13.2–3: 243–61

Abdirahman, M. (2024) ***Ethiopia Pioneers Inclusive Digital ID System for Refugees***, Identity Week, 8 March (accessed 6 February 2025)

Abebe, D. and Ahadu, E. (2020) 'Nexus Between Ethnic Federalism and Creating National Identity vis-à-vis Nation Building in Contemporary Ethiopia', *International Journal of Multicultural and Multireligious Understanding*, 71: 37–46

Access Now (2022) ***Two Years of Internet Shutdowns: People in Tigray, Ethiopia, Deserve Better***, Access Now, 4 November (accessed 30 March 2025)

Addis, A. (2022) '***The Unbearable Thinness of National Citizenship in a Country Organized as a "Nation of Nations": The Case of Ethiopia***', in A. Ibrahim and K. Wolde (eds), *Between Failure and Redemption: The Future of the Ethiopian Social Contract*, Evanston, Illinois: Northwestern Roberta Buffett Institute for Global Affairs and Northwestern University Libraries (accessed 17 October 2025)

Ambelu, A.A. (2024) ***Digital Divide in Ethiopia: The Struggle for Equitable Internet Access***, African News Channel, 29 June (accessed 8 February 2025)

Aratek (2024) ***National ID Ethiopia: A Gateway to Digital ID Empowerment***, 29 October (accessed 15 January 2025)

Awol, E. (2025) ***Ethiopia Launches Fayda National ID Mobile App***, Shega, 13 February (accessed 30 May 2025)

Bhandari, V.; Trikanad, S. and Sinha, A. (2020) ***Governing ID: A Framework for Evaluation of Digital Identity***, Centre for Internet and Society, 22 January (accessed 19 May 2025)

Bosman, I. (2023) ***Digital Identification and Biometrics in East Africa: Opportunities and Concerns***, Johannesburg: South African Institute of International Affairs (accessed 17 March 2025)

CARD (2018) ***Digital Divide in Ethiopia***, Center for the Advancement of Rights and Democracy (accessed 8 February 2025)

Casher, C. and Clark, J. (2024) ***Closing the Gender Gap in ID Ownership in Ethiopia***, Washington, DC: World Bank (accessed 17 October 2025)

Clarke, R. (1991) 'Information Technology and Dataveillance', in C. Dunlop and R. Kling (eds), *Controversies in Computing*, 14

DataReportal (2025) ***Digital 2025: Ethiopia*** (accessed 18 May 2025)

Federal Democratic Republic of Ethiopia (2024) ***Proclamation No. 1321/2024: Proclamation to Provide for Personal Data Protection***, (accessed 17 October 2025)

Federal Democratic Republic of Ethiopia (2023) ***Proclamation No. 1284/2023: Ethiopian Digital Identification Proclamation*** (accessed 17 October 2025)

HRW (2005) ***Suppressing Dissent: Human Rights Abuses and Political Repression in Ethiopia's Oromia Region: Mechanisms Used by the Ethiopian Government to Control Rural Communities in Oromia***, Human Rights Watch (accessed 29 May 2025)

ID Tech (2025) ***Ethiopia Mandates National Digital ID 'Fayda' for All Banking Transactions by 2026*** (accessed 8 February 2025)

Kaaniru, J. and Muindi, P. (2024) ***Ethiopia's Personal Data Protection Proclamation of 2024 and its Budding Digital Identity Regime***, Centre for Intellectual Property and Information Technology Law, Strathmore University (accessed 17 March 2025)

Kaberia, J. (2025) ***Ethiopia Unveils Mandatory Digital ID For Banks***, CIO Africa, 8 January (accessed 15 January 2025)

Kebret, N. (2008) ***Road Traffic Law Enforcement In Addis Ababa: The Law And Practice***, St Mary's University (accessed 17 October 2025)

Kitzmüller, L. (2020) ***Let's Get Digital? Policy Options for Ethiopia's ID System***, Medium, 12 December (accessed 9 February 2025)

Lawson, M.C. (2022) ***Business Models of ID Authorities (Nigeria, Pakistan, India)***, i-On-Ethiopia, Zoom hosted by ID4Africa, Episode 34, 28 September (accessed 9 February 2025)

Macdonald, A. (2025a) ***Ethiopia's Digital ID Proves Useful for Document Authentication, Fraud Prevention***, BiometricUpdate.com, *26 February* (accessed 17 Apr 2025)

Macdonald, A. (2025b) ***Ethiopia, UNICEF Look to Scale Up Birth Registration, Fayda ID Adoption***, BiometricUpdate.com, *12 February* (accessed 18 May 2025)

Macdonald, A. (2025c) **School Registration Adds Up to Expanding Use Cases of Ethiopia's Digital ID**, BiometricUpdate.com, 28 January (accessed 17 October 2025)

Macdonald, A. (2024) ***Laxton to Accompany Ethiopia on 90M Digital ID Target by 2030***, BiometricUpdate.com, *29 September* (accessed 5 February 2025)

Ministry of Innovation and Technology (2021) ***Digital Foundation Project: Environment and Social Impact/Risk Assessment Screening Guideline for Sub-Project Activities in all Beneficiary MDAs***, Addis Ababa: Ministry of Innovation and Technology (accessed 17 October 2025)

Mohamed, S.Y. and Santoro, F. (2024) ***Ethiopia's National Digital ID: A Breakthrough for Tax System Transformation?***, International Centre for Tax & Development blog, 9 May (accessed 15 January 2025)

National ID (n.d.) ***Authentication*** (accessed 17 October 2025)

National ID (2025a) ***From Insight to Impact. Ethiopia's National ID Program's Self-Evaluation of FAYDA*** (accessed 30 May 2025)

National ID (2025b) ***Fayda for Ethiopia*** (accessed 15 January 2025)

National ID (2024) ***Ethiopia Digital ID for Inclusion and Services (P179040): Environmental and Social Management Framework (ESMF)***, Addis Ababa: Office of the Prime Minister, Federal Democratic Republic of Ethiopia (accessed 30 May 2025)

National ID (2023) ***Ethiopia Digital ID for Inclusion and Services (P179040): Stakeholder Engagement Plan***, Addis Ababa: Office of the Prime Minister, Federal Democratic Republic of Ethiopia (accessed 17 October 2025)

Novogrodsky, N.B. (1999) '***Identity Politics***', *Boston Review* , 1 June (accessed 28 May 2025)

Ohm, P. (2010) 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review*, 57: 1701-1777

Shega (2024) ***NBE Sets One-Month Deadline for Digital ID Requirement to Open Bank Accounts in Addis Ababa*** (accessed 30 May 2025)

Shemsu, M. (2025) ***Data Center Oversight Mandate Shifts to Ethiopia's Communication Authority***, Shega, 26 January (accessed 17 March 2025)

Taye, B.A. (2017) 'Ethnic Federalism and Conflict in Ethiopia', *African Journal on Conflict Resolution*, 17.2: 41–66

UNDP (2023) *Ethiopia 2030: A Country Transformed? Options for A Next Generation of Reforms*, Working Paper Series, United Nations Development Programme

UNHCR (2024) **Ethiopia Launches Inclusive ID System for Refugees, Boosts Access to National Services**, United Nations Refugee Agency, 7 March (accessed 18 May 2025)

Wiebel, J. (2017) '**The Ethiopian Red Terror**', in *Oxford Research Encyclopedia of African History, Oxford University Press* (accessed 25 July 2025)

Wiebel, J. and Admasie, S.A. (2019) 'Rethinking the Ethiopian Red Terror: Approaches to Political Violence in Revolutionary Ethiopia', *The Journal of African History*, 60.3: 457–75

Wodajo, K. (2022) ***Digitalizing Identity: Precautionary Thoughts on Ethiopia's 'Fayda' Number***, Opinion Juris blog, 10 February (accessed 17 October 2025)

World Bank (2023) ***World Bank Supports Ethiopia's Digital ID Project to Increase Access to Services and Economic Opportunities***, World Bank, 13 December (accessed 15 January 2025)

World Bank (2016) **ID4D Country Diagnostic: Ethiopia**, Washington, DC: World Bank (accessed 17 October 2025)

World Population Review (2017) **Literacy Rate by Country 2025** (accessed 16 March 2025)

Yirga, B. (2023) 'National Benefits of Ethiopia's Digital ID Project and its Implementation', *Mizan Law Review*, 17.2: 457–78

Zecharias, Z. (2023) '**Ethiopia Digital ID Prompts Fears of Ethnic Profiling**', *Reuters*, 1 February (accessed 19 May 2025)

Zelalem, Z. (2023) '**Ethiopia Digital ID Prompts Fears of Ethnic Profiling**', *Context*, 1 February (accessed 19 May 2025

Digital-ID in Malawi: Country report

Jimmy Kainja

 DOI: 10.19088/IDS.2025.061

1. Introduction

This report examines the evolution and impact of Malawi's biometric identification (ID) system. Before 2017, Malawians relied on fragmented, function-specific ID such as driving licences, passports, and voter registration cards. These systems were limited in reach and lacked a unified framework for identification across sectors. The introduction of a centralised biometric ID in 2017 marked a major shift, enabling streamlined access to public services, voter registration, and digital platforms. However, it also raised critical questions about inclusion, surveillance, and rights. This report examines how identity is constructed and governed within this new system, and what that means for citizen agency and digital inclusion. It is structured around three guiding questions: Does Malawi's biometric ID system pass the rule of law test? Does it meet rights-based standards? And does it address potential risks? The analysis is presented in four sections: the first reviews the pre-digital-ID landscape; the second assesses the system against the rule of law principles; the third evaluates it through a rights-based lens; and the final section examines the risks centralised digital-ID poses.

2. History of ID in Malawi

Before the introduction of digital-ID in 2017, only a small percentage of Malawians had a functional ID, such as a driver's licence or passport. The digital-ID system was established to provide a universal form of ID. Malawians widely embraced its implementation, with 1.19 million people registering within 180 days (UNDP 2022; Citizens Rights in Africa Initiative 2017). Since then, the biometric-based ID has replaced fragmented identification methods and is now essential for accessing public services, including banking, voter registration, SIM card registration, passport applications, student loan schemes, and social welfare programmes. As of May 2025, 12.5 million Malawians had registered for the ID (Chitete 2025).

However, the system faces challenges. The IDs expire and require renewal; the first batch expired in 2021 (Bhatt, Moulton and Sutterlin 2021), and the National Registration Bureau (NRB) has struggled to process renewals efficiently. As a temporary measure, the government has permitted the use of expired IDs until January 2026 (Keesing Platform 2023). A data protection law was enacted in 2024, and the Data Protection Authority (DPA) was established. The country's telecoms regulator, the Malawi Communications Regulatory Authority (MACRA), is a designated policyholder (DPA n.d.).

2.1 Pre-digital-ID era

British colonial rule (1890s–1963)

During British colonial rule, Malawi (then called Nyasaland) lacked a formal civil ID system. Instead, identity verification was primarily based on administrative documents for taxation, labour control, and governance – these IDs were solely used to identify workers, not for citizens to carry and show to officials (Lovering 2002).

Hut tax registration and early passbooks (1890s–1930s)

The 'hut tax' was so called because African men were required to pay a tax for each hut they owned. Local chiefs and colonial authorities maintained manual registers of taxpayers, effectively serving as an early form of identity verification. According to Gwaindepi (2023), the system compelled many Malawians to engage in wage labour to afford tax payments; this increased labour migration.

Pass laws and labour identification (1930s–1950s)

According to Okia (2023), the growth of labour migration from Malawi to South Africa, Zambia, and Zimbabwe incentivised colonial authorities to introduce pass laws. These were implemented to regulate labour migration and ensure tax collection from African workers, primarily those migrating to work in Zambia and Zimbabwe.

Second World War military IDs (1940s)

Thousands of Malawians were recruited into the King's African Rifles during the Second World War and were issued military ID cards. However, Baker (1975) observes that these did not transition into a civilian ID after the war.

Federation of Rhodesia and Nyasaland (1953–1963)

Between 1953 and 1963, the British established the Federation of Rhodesia and Nyasaland, comprising Northern Rhodesia (now Zambia), Southern Rhodesia (now Zimbabwe), and Nyasaland (now Malawi). During this period, ID systems were primarily employed to manage **African labour, enforce racial segregation, and collect taxes**. Africans were obligated to carry **passbooks or ID documents**, typically issued through Native Authorities, to move within and between the three territories and to access employment in urban areas. Monahan (2019) notes that there was no national multi-purpose foundational ID, only various functional IDs for specific issues.

Post-independence identification systems (1964–2017)

Upon independence in 1964, Malawi lacked a national ID system. The country's first president, Hastings Kamuzu Banda, retained some colonial legal frameworks, which allowed him to consolidate his power and control. These included the 1930 Penal Code with vagrancy laws, but he did not introduce a universal ID system. The closest alternative was the membership card of the Malawi Congress Party (Banda's political party), which became mandatory to access markets, transport, and education. Banda's paramilitary groups enforced the card, and pregnant women were forced to buy extra cards for their unborn children (Hungwe 2000).

Beside the Malawi Congress Party card, formal ID was limited to functional IDs for specific purposes, including voter registration cards, passports, and driver's licences, which were expensive and inaccessible to most citizens, and employment IDs, issued mainly to urban workers, especially those in the civil service (Malik 2020).

Arguments for introducing a universal national ID were first raised in the aftermath of the 1994 general election, which removed Banda – the country's dictator of 30 years – from office. The NRB was established in 2007, and

the National Registration Act was passed in 2010, but the first attempt to implement a national ID in 2012 stalled due to funding constraints (Kubwalo 2012; Issue Lab 2012). It was not until 2017 that the NRB began its operations under the Ministry of Home Affairs and Internal Security (now the Ministry of Homeland Security), overseeing civil registration.

2.2 Introduction of the biometric national ID (2017–present)

At the launch of the biometric national ID registration in 2017, only 55,000 of Malawi's 9 million adults used different forms of ID such as a driver's licence, passport, or voter registration (Laxton 2017). By the end of 2021, 10.2 million people had registered for the biometric national ID (ID4Africa 2022), replacing the fragmented forms of ID. As of May 2025, 12.5 million people had registered (Macdonald 2025). The biometric national ID project was implemented with financial assistance from the United Nations Development Programme, World Bank, European Union, and Irish Aid (UNDP 2018).

The biometric ID, established under National Registration Act No. 13 of 2010 (subsequently referred to as the National Registration Act of 2010), is managed by the National Registration and Identification System (NRIS) within the NRB (*The Malawi Gazette* 2010). All indigenous Malawians and naturalised citizens must be 16 or older to be eligible. In addition, the following is also required as proof of their citizenship:

- Foundational ID (birth certificate);
- Two witnesses with national IDs;
- Biometrics (ten fingerprints, facial recognition, and an electronic signature).

In 2018, the Reserve Bank of Malawi, the country's financial sector regulator, announced that the national ID would be used for identity verification to open new accounts. Existing customers were required to undergo a know your customer verification process, linking all bank accounts to biometric IDs (Burt 2019). However, this is not specified as one of the uses for a national ID, therefore raising fears of mission creep. Providers of other services, including university student loans, social welfare, revenue collection, immigration services, and SIM card registration, followed the bank's lead. By 2020, almost 10.3 million people of an eligible population of 10.9 million had registered (Hersey 2022), and by May 2025, almost 100 per cent of the eligible population.

This shows that the registration exercise was well received. Yet, despite the attraction of the registration, not all eligible Malawians were able

to register because the process was not straightforward for them. Some groups, such as minority communities, naturalised citizens who arrived as refugees, for example, and Malawians of Asian descent, face challenges in proving their citizenship. Michael-Phiri (2017) highlights the case of Mussa Adam, a trader of Indian origin who had lived in Malawi his entire life but failed to register as he could not prove his 'Malawian-ness'. Those who are unable to register face difficulties accessing services that require the biometric ID card as proof of identity. This reflects the exclusionary effect of identity and belonging that complicate access to documentation for minority individuals (Bhatt *et al*. 2021).

2.3 Digital penetration in Malawi

There are various estimates of digital penetration, but this study relies on DataReportal, which has proved reliable over the years. According to its 2025 State of Digital report for Malawi (DataReportal 2025):

- 3.95 million internet users of the country's population of 21.9 million people were recorded at the start of 2025, with internet penetration at 18.0 per cent.
- 1.80 million active social media users were recorded in January 2025, representing 8.2 per cent of the total population.
- 13.2 million cellular mobile connections were recorded, covering 60.3 per cent of the population at the beginning of 2025.
- 18.0 million Malawians (80.0 per cent of the population) remained offline at the beginning of 2025.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Yes. Malawi's digital-ID project is primarily governed by the National Registration Act of 2010, which establishes the NRIS under Section 3. The NRIS establishes and governs the biometric national ID. It manages citizen registrations and forms the legal backbone of the country's digital-ID infrastructure.

However, the National Registration Act of 2010 does not elaborate on data protection, privacy safeguards, or consent, which has led to legal and ethical concerns, particularly with the increased use of identity data for multiple purposes – for example, banking, elections, and digital services. These gaps can be addressed through full implementation of the Data Protection Act No. 3 of 2024 (subsequently referred to as the Data Protection Act). However, Malawi's data protection framework remains underdeveloped.

Although the DPA now operates under MACRA, its activities are still in the early stages. For instance, the DPA has only recently initiated the registration of data controllers and processors (DPA n.d.). This limited progress reflects broader concerns noted by MACRA, particularly that the Data Protection Act has yet to be fully operationalised (Kasalika 2025). The absence of clear implementation mechanisms leaves room for legal ambiguity, and the potential for overreach in data management and delegation of authority.

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Yes. The law, the National Registration Act of 2010, provides the legal foundation for Malawi's digital-ID system, outlining five key objectives in official law and policy documents:

1. Facilitating access to public services;
2. Strengthening national security and law enforcement;
3. Supporting electoral integrity;
4. Improving financial inclusion and economic development;
5. Enhancing data-driven governance and planning.

However, eight years after implementation, there is little evidence that these objectives have been fully met. Instead, the ID system has sparked political controversy, particularly concerning its exclusive use for voter registration. Opposition parties have raised concerns that the ID could be manipulated to benefit the incumbent government by prioritising ID registration and issuing ID cards to voters in the government's stronghold areas, while depriving those in opposition party stronghold areas, casting doubt on the digital-ID's neutrality and integrity as the only acceptable form of ID for voter registration (Chitsulo 2024; Maulidi 2024; Malimba 2024).

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

No. The law establishing digital-ID in Malawi, the National Registration Act of 2010, does not clearly and comprehensively specify the actors involved in the digital-ID ecosystem or the full range of purposes that flow from its legitimate aim. While the act mandates the NRB as the authority responsible for civil registration and the issuance of national identity cards, it offers limited detail on which other public or private entities may access or use the digital-ID system.

Several institutions, including the Malawi Revenue Authority, financial institutions, telecoms companies, and social service agencies, rely on the national ID system for identification and verification. However, the law does not explicitly name these entities or provide a clear framework for their involvement. This lack of specificity raises concerns about data sharing, integration, accountability, and oversight.

While the act provides the legal basis for registration of citizens and the issuance of national identity cards, and outlines the types of personal information to be collected for registration purposes, it does not comprehensively address data protection principles or individual rights to access or correct personal information.

However, the law defines categories of personal data to be collected for national registration. According to the law, the NRB is supposed to collect the following information from applicants: full name, date and place of birth, gender, nationality, occupation, residential and postal address, and biometric data (fingerprints and facial images).

Furthermore, the National Registration Act does not explicitly grant individuals the right to access, rectify, or erase their personal information stored by the NRB. There is no defined mechanism within the act that allows citizens to request copies of their data, correct inaccuracies, object to processing, or be informed of how their data is used or shared.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

No. The legal framework governing digital-ID in Malawi, established under the National Registration Act of 2010, does not provide clear or comprehensive redress mechanisms for individuals whose rights may have been violated through the use or misuse of the digital-ID system. While the act outlines the responsibilities of the NRB and includes general provisions for the protection of personal data, it lacks explicit procedures for individuals to challenge decisions, correct errors, or seek remedies when their data is mishandled or misused by government agencies or third parties.

There is no dedicated and easily accessible avenue within the digital-ID framework to lodge a complaint, request an investigation, or obtain a timely resolution. The law also does not establish an independent oversight body with the mandate to monitor the digital-ID system, investigate grievances, or impose penalties on those who breach data protection principles. While the Data Protection Act provides some redress mechanisms, it has yet to be fully implemented (Kasalika 2025). This regulatory gap weakens the overall accountability of institutions that use or manage digital-ID data, and leaves individuals vulnerable to harm, without sufficient legal protections.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

No. There is no adequate regulatory mechanism or independent oversight body to ensure that digital-ID is managed under the law and Malawi's commitments to human rights. While the National Registration Act of 2010 establishes the NRB to manage the digital-ID system, the law does not provide an accountability framework that clearly defines the responsibilities of all actors involved, nor does it create robust mechanisms for monitoring compliance, investigating misconduct, or enforcing penalties.

The NRB operates under the Ministry of Homeland Security, meaning its actions are subject to internal government supervision rather than scrutiny

by an external, impartial body. This institutional setup raises concerns about conflicts of interest and insufficient checks and balances. No dedicated institutions or procedures are in place to systematically audit how digital-ID data is accessed, shared, or used across government departments and the private sector.

The multiple public and private agencies that integrate digital-ID into their operations without clear legal frameworks governing the integration contribute to the risk of misuse, overreach, and unauthorised access to personal information without consequence. Malawi has yet to fully implement the Data Protection Act, which would establish clear responsibilities for data controllers and processors, and provide a legal basis for holding actors accountable for breaches or abuse of personal information (DPA n.d.).

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

The law lacks a well-defined legislative mechanism to address mission creep. The law does not include detailed provisions that limit the use of identity to its original purpose, nor does it offer clear safeguards to prevent expansion into unintended or unauthorised areas of use, which exposes it to mission creep.

Parliamentary oversight exists in general terms, as the NRB falls under the purview of the Ministry of Homeland Security, which is accountable to Parliament. However, there is no dedicated parliamentary committee or legal requirement for regular reporting on the functioning of the digital-ID system, its integration into other sectors, or its impact on privacy and civil liberties. This lack of focused legislative scrutiny makes it difficult to detect, assess, or prevent mission creep.

Judicial oversight theoretically exists through Malawi's courts, which can hear cases involving violations of constitutional rights, including the right to privacy protected under Section 21 of the Constitution of Malawi. However, applying this provision may be limited in addressing cases of mission creep, which the law does not explicitly define or prohibit, and courts have limited statutory guidance to rely on when evaluating such claims.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

No. As much as the Malawi digital-ID system aims to enhance public service delivery, national security, and fraud prevention, its implementation has raised significant privacy concerns due to the extensive collection of personal and biometric data without robust data protection measures (Kasalika 2025; Kainja 2019).

In principle, a well-designed digital-ID system can streamline access to public services and support efficient, transparent state functions. However, the lack of clear legal provisions governing its extended use, especially in sensitive areas such as elections and financial institutions, raises questions about whether these applications are strictly necessary or whether less intrusive alternatives could achieve the same outcomes. Moreover, key objectives of the digital-ID remain unmet, suggesting that the system may not function in the least intrusive or most effective way.

The disproportionate reliance on the national ID for voter registration, amid unresolved concerns about political manipulation, may be excessive, especially given Malawi's lack of comprehensive data protection enforcement. Without strong safeguards, redress mechanisms, or oversight, the risks of exclusion, voter manipulation, privacy breaches, and abuse of power are heightened. The absence of clear boundaries around who can access and use digital-ID data further intensifies these concerns. While the system may have legitimate intentions, it lacks the legal and institutional safeguards necessary to pass a robust necessity and proportionality test, particularly in a politically polarised context.

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

No unnecessary data is collected. However, while Malawi has legal frameworks that establish the infrastructure for identity management, such as the National Registration Act of 2010, the broader data governance ecosystem remains underdeveloped. The DPA has only recently begun registering data controllers and processors, an

example of the Data Protection Act not being fully implemented. This regulatory gap exposes citizens to potential data misuse.

These concerns are amplified by the expanding and often legally ambiguous use of the digital-ID system beyond its original mandate, such as for SIM card registration and banking services. Initially intended to improve access to public services, security, and governance, the system is now increasingly used for politically sensitive functions such as voter registration.

Only data strictly required for specific and legally provided purposes must be collected. There must be clear boundaries around data access and usage. Strong legal safeguards, oversight, and redress mechanisms are essential to prevent abuse, protect individual rights, and ensure the digital-ID system serves the public good rather than becoming a tool for surveillance or exclusion.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

The law does not clearly articulate strong data protection principles or impose strict limitations on who can access, use, or share the digital-ID data generated through both public and private use. Additionally, no specific legal provisions define or regulate the creation of a digital trail or digital footprints when the digital-ID is used across various services such as banking, telecoms, voting, and social welfare.

Without a fully operational data protection law, there is no requirement for consent, no independent oversight of data-sharing practices, and no legal obligation for state or private entities to notify individuals about how their data is used or stored. This means that once a person's digital-ID is used for a government transaction or a commercial service, limited safeguards prevent access to or repurposing of that information without their knowledge.

Public and private entities extensively use Malawi's digital-ID system for identity verification. However, the lack of clear regulations and enforceable standards regarding data collection, storage, and sharing has resulted in significant legal and institutional deficiencies. Without sufficient safeguards, individuals are vulnerable to data breaches, profiling, surveillance, and discrimination (Kainja 2019). This highlights the urgent need for a comprehensive data protection framework to ensure privacy, transparency, and accountability in the use of digital-ID data.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Malawi lacks sufficient mechanisms to ensure that the adoption of digital-ID does not result in exclusion or restricted access to entitlements or essential services. Although the national ID system aims to enhance identification and service delivery, its mandatory use, especially in contexts such as voting, accessing public services, and mobile (cell) phone registration, presents risks of exclusion for individuals who do not have a digital-ID or face challenges in obtaining one.

According to Bhatt *et al*. (2021), rural populations, individuals living in poverty, people with disabilities, and those without supporting documentation often face challenges during the registration process. However, service providers and institutions frequently deny access due to the absence of a national ID. The lack of fallback options and accountability frameworks exacerbates the risk of systemic exclusion. This situation deepens existing social and economic inequalities, particularly for those unable to establish a mobile money account for business transactions or mobile cash transfers.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

No. However, Section 14 of the National Registration Act of 2010 provides a legal basis for mandatory enrolment, mandating the compulsory registration of every Malawian citizen aged 16 and older. Furthermore, Section 41 of the act outlines penalties for non-compliance, which include fines and imprisonment. In addition to these legal provisions, its centrality in accessing both public and private services, such as banking, SIM card and voter registration, and social benefits, in effect makes its use mandatory *de facto* – it works as an enforcement mechanism for registration. The government is aware of the centrality of the biometric ID card. This is why it has allowed the use of expired cards until 2026, in the face of its failure to renew them (Keesing Platform 2023).

While digital-ID enrolment is compulsory, and the ID card is required to access services such as SIM card registration, voter registration, banking, education, and social welfare, this usage is not comprehensively regulated in the National Registration Act of 2010. This oversight poses the following challenges: the act lacks explicit legal provision that lists or limits the scope of services that may require the ID for access; no

independent oversight body is defined in the act to monitor misuse, exclusion risks, or abuse of digital-ID requirements; the law pre-dates the Data Protection Act, meaning privacy safeguards and individual rights are not embedded in the original ID law; and making the use of digital-ID mandatory without reasonable alternatives may infringe upon rights to health, education, political participation, and freedom from discrimination, as stipulated in Section 20 of the constitution.

However, the 'mandatory use' of digital-ID for accessing services, particularly if it becomes a gatekeeper for access to basic needs and/or essential services, raises legal and human rights concerns, especially in the absence of a robust data protection regime and clear oversight mechanisms.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

No. Decisions regarding the legitimacy, benefits, and human rights impact of Malawi's digital-ID system were not initially informed by a formal risk assessment when the National Registration Act of 2010 was enacted. There is no official record or policy document indicating that a formal privacy impact assessment or human rights impact assessment was conducted at the time of the law's development.

It may be that the process did not foresee the full range of digital-ID use cases later adopted, such as for SIM card registration, banking, voter rolls, and social protection. This strengthens the case for reviewing the law and limiting its use to the services stipulated within it.

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

Malawi's current legal and regulatory framework does not explicitly provide for a differentiated approach to governing the various uses of digital-ID based on their risk levels. The primary law governing the digital-ID system, the National Registration Act of 2010, largely focuses on the civil registration of citizens and the issuance of national identity cards. It fails to set out risk-based or sector-specific guidelines for how digital-ID should be used across different domains. Nonetheless, it is employed for other services such as elections, telecoms, banking, and social protection (Kainja 2024).

Similarly, while the Electronic Transactions and Cyber Security Act No. 33 of 2016 provides digital signatures and a general framework for online security, it lacks specific provisions that would enable a tiered or contextual governance approach, depending on the sensitivity of the use case. For instance, no distinction is made between using digital-ID for routine services such as student loan applications, and high-stakes uses such as biometric voter verification or SIM card registration. This uniform approach increases the risk of mission creep when digital-ID is applied in new contexts without clear legal oversight or accountability mechanisms.

Although the Data Protection Act has the potential to introduce more nuanced, risk-informed governance through tools such as data protection impact assessments (DPIAs) and purpose limitation, its implementation remains incomplete (Kasalika 2025). As a result, the regulatory environment does not yet support a differentiated, risk-based use of digital-ID.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

Malawi's legal framework on digital-ID does not explicitly envision governance that is proportional to the likelihood and severity of risks associated with its use. The foundational law, the National Registration Act of 2010, primarily focuses on establishing the NRIS and mandating universal registration for citizens aged 16 and older. It outlines general objectives such as improving service delivery, enhancing national security, and reducing fraud, but lacks risk-based or proportional governance mechanisms.

Proportional governance should mandate that the law distinguish between low-risk and high-risk uses of digital-ID. However, Malawi's current framework regards the digital-ID system as a one-size-fits-all solution, lacking customised safeguards, oversight, or access controls according to the possible severity of harms, such as privacy violations, exclusion or misuse of surveillance.

Although not yet fully implemented, the Data Protection Act has the potential to introduce proportionality through requirements such as data minimisation, purpose limitation, and DPIAs. These tools aim to ensure that data collection and processing practices align with the risk level of a specific use case.

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

Malawi lacks clearly defined legal mechanisms to prohibit or restrict the use of digital-ID in cases that pose a demonstrably high risk to individuals' rights. The National Registration Act of 2010 focuses on registration processes and the establishment of the NRIS. However, it does not contain specific provisions for risk-based restrictions on using identity data.

The lack of such mechanisms has raised concerns, particularly as the digital-ID system has grown into politically sensitive and high-risk areas such as biometric voter registration (Chitsulo 2024; Maulidi 2024). These expanded applications heighten the risk of exclusion, surveillance, or political manipulation, especially in a context characterised by limited oversight and an underdeveloped data protection infrastructure.

However, there is no clear guidance or precedent yet for restricting high-risk uses of digital-ID. Furthermore, the act has not yet institutionalised mandatory DPIAs or any formal prohibition framework for risky use cases. In practice, this legal gap means that even when harm is foreseeable or occurring, the current system lacks enforceable checks that can compel authorities or private actors to halt or modify high-risk uses of digital-ID.

6. Conclusion

Malawi's digital-ID system represents a significant evolution from its colonial-era and post-independence ID mechanisms, transitioning from fragmented and exclusionary forms of ID to a centralised, biometric infrastructure aimed at improving governance and access to services. However, despite its rapid rollout and wide coverage, the system continues to reflect structural inequalities and historical legacies of marginalisation, particularly for ethnic minorities, naturalised citizens, and those without formal documentation. While it has become a critical foundation for digital governance, the ID system is unevenly accessible and has been deployed without sufficient legal, procedural, and technological protections. Its integration into essential sectors, such as voter registration, banking, and telecommunications, without clear legal safeguards has compounded the risks of exclusion and deepened existing socioeconomic divides.

Critically, the legal framework underpinning Malawi's digital-ID system is incomplete, lacking enforceable safeguards regarding purpose limitation, data minimisation, access control, and redress. The system has expanded into high-risk domains without adequate risk assessments or proportional oversight, exposing individuals to privacy violations, surveillance, and political manipulation. The absence of differentiated governance mechanisms or effective enforcement of the Data Protection Act underscores a systemic failure to align the digital-ID with international rights-based standards. In its current form, the digital-ID risks becoming a tool of control and exclusion rather than empowerment and inclusion. To restore trust and legitimacy, urgent reforms are needed to introduce meaningful oversight, institutional accountability, and legal clarity, ensuring the system operates in the service of all Malawians, not just the state or powerful actors.

7. Bibliography

Baker, C. (1975) 'Tax Collection in Malawi: An Administrative History, 1891–1972', *The International Journal of African Historical Studies*, 8.1: 40–62

Bhatt, P.; Moulton, S. and Sutterlin, E. (2021) ***Identified but Unheard: Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities***, National Democratic Institute (accessed 8 February 2025)

Burt, C. (2019) ***Malawi Bank Integrates Biometric National ID System for KYC Checks***, BiometricUpdate.com, 13 June (accessed 5 May 2025)

Citizenship Rights in Africa Initiative (2017) ***Malawi: 9.19 Million Registered for National IDs, Cards Distribution Underway*** (accessed 28 May 2025)

Chitete, S. (2024) '**12.3 Million Register for ID Cards**', *Nation Online*, 23 August (accessed 28 August 2025)

Chitsulo, L. (2024) '**National ID Chaos Still Threatens Voter Registration**', *Nation Online*, 15 September (accessed 13 April 2025)

DataReportal (2025) ***Digital 2025: Malawi*** (accessed 9 February 2024)

DPA (n.d.) ***About DPA***, Data Protection Authority (accessed 13 April 2025)

Gwaindepi, A. (2023) 'Taxation in Africa since Colonial Times', in E. Frankema, E. Hillbom, U. Kufakurinani and F. Meier zu Selhausen (eds), *The History of African Development: An Online Textbook for a New Generation of African Students and Teachers*, African Economic History Network

Hersey, F. (2022) ***Malawi's Biometric ID Approaches Total Coverage, Huge Cost Savings***, BiometricUpdate.com, 9 December (accessed 28 May 2025)

Hungwe, K. N. (2000) 'Chapter Two: Breaking the Silence: Fax Transmissions and the Movement for Democracy in Malawi', *Counterpoints*, 59: 51–69

ID4Africa (2022) ***ID4Africa LiveCast Supplement: Malawi ID Roadmap***, 7 December (accessed 5 May 2025)

Issue Lab (2012) ***The Malawi National Registration Act: Policy Brief***, Candid (accessed 9 February 2025)

Kainja, J. (2024) ***Malawi Dragging its Feet on Filling Legal Gaps to Prevent Human Rights Violations***, Association for Progressive Communications, 15 August (accessed 12 March 2025)

Kainja, J. (2019) ***Are Malawians Sleep-Walking Into a Surveillance State?***, Collaboration on International ICT Policy for East and Southern Africa blog, 12 August (accessed 11 March 2025)

Kasalika, J. (2025) '**Gaps in Malawi's Digital Laws Raise Concerns – MACRA**', *Nation Online*, 2 March (accessed 12 March 2025)

Keesing Platform (2023) ***Malawi Extends Validity of Expired National ID Cards: Government Says Expired Cards Valid Until January 2026*** , 2 August (accessed February 2025)

Kubwalo, K. (2012) ***In Malawi, The Launch of Universal Birth Registration Guarantees Protection for Children***, ReliefWeb, 1 April (accessed 9 February 2025)

Laxton (2017) ***Malawi's First Digital Citizens' Registry and National ID Card*** (accessed 6 May 2025)

Lovering, T. J. (2002) '**Authority and Identity: Malawi Soldiers in Britain's Colonial Army, 1891–1964**', PhD Thesis, University of Stirling (accessed 10 March 2025)

Macdonald, A. (2025) ***Malawi Nears Full-Scale Digital ID Rollout to Streamline Access to Services***, BiometricUpdate.com, 27 May (accessed 28 May 2025)

Malik, T. (2020) **Malawi's Journey Towards Transformation: Lessons from its National ID Project**, Center for Global Development (accessed 9 February 2025)

Malimba, P. (2024) '**Malawi Electoral Commission, Parties at Odds Over IDs**', *Times News*, 3 October (accessed 11 March 2025)

Maulidi, C. (2024) '**National ID Cards Raise Suspicion**', *Times News*, 12 December (accessed 13 April 2025)

Michael-Phiri, M. (2017) ***National ID Programme in Malawi Raises Questions, Fears***, Anadolu Agency, 11 June (accessed 13 April 2025)

Monahan, M. (2019) '**An Unequal Partnership: Nyasaland and the Central African Federation, 1953–1963**', Bachelor's Thesis, Lund University (accessed 9 February 2025)

Okia, O. (2023) 'Migration and Labour in Sub-Saharan Africa During the Colonial Period', in M.J. Borges and M.Y. Hsu (eds), *The Cambridge History of Global Migrations*, Cambridge University Press

The Malawi Gazette (2024) 'Data Protection Act No. 3 of 2024', Government Press

The Malawi Gazette (2016) 'The Electronic Transactions and Cyber Security Act. No. 33 of 2016', Government Press

The Malawi Gazette (2010) 'National Registration Act. No. 13 of 2010', Government Press

UNDP (2022) ***Malawi's Foundational Legal Identity System Sets the Stage for a More Efficient and Responsible Digital Future***, United Nations Development Programme, 20 May (accessed 9 February 2025)

UNDP (2018) ***Moving Towards a Harmonised National Identity System in Malawi***, United Nations Development Programme, 29 October (accessed 9 February 2025)

Digital-ID in Namibia: Country report

Nashilongo Gervasius

 DOI: 10.19088/IDS.2025.062

1. Introduction

This report provides an overview of Namibia's biometric identification (ID) system. It centres on the national ID system that has evolved from paper-based documentation dating from pre-1990 to increasingly biometric inclusive documentation that incorporates fingerprint and facial recognition technologies. Namibia is seen as an early adopter of digital-ID within the Southern African Development Community (SADC) economic block, implementing biometric ID cards that allow for inter-country travel. The introduction of the of biometric ID, and its gradual rollout within the refugee community, specifically, is recognised as necessary to upscale service provision for essential services such as providing access to social grants, while also facilitating cross-border movement, and is among the many digital activities needed to transform Namibia into a knowledge-based economy.

This research assesses the current state of the biometric ID system and existing legislative framework, while also comparing operational implementation against established rule of law, rights-based, and risk-based tests. This report evaluates the strengths and vulnerabilities in the system's design and governance; it examines the system's effectiveness, and balances security considerations with citizens' rights to privacy, inclusion, and non-discrimination. The analysis is carried out through five interconnected sections: examining the historical landscape of identification in Namibia; applying rule of law tests to assess legal foundations; employing rights-based tests to evaluate human rights implications; utilising risk-based tests to identify and assess governance of potential harms; and concluding with findings and recommendations for improvement.

2. History of ID in Namibia

2.1 Colonial ID systems

The practice of government identification of citizens has existed in Namibia since the colonial governments and continued in a modified form post-independence.

The South African colonial administration introduced a formal system of ID documentation, which included travel and residence documentation, for Europeans and British subjects, while a pass system and labour registration requirements were implemented for indigenous Namibians. These systems regulated movement between districts and documented employment status, particularly for labour migration to South African mining operations (Parsons 2019). These early identification practices established procedural precedents that would influence post-independence approaches to ID documentation.

2.2 Post-liberation ID systems (pre-digital)

Following the attainment of Namibia's independence in 1990, birth certificates became foundational ID documents (Nashama 2024). With increasing urbanisation over the years, digitisation has also increased (Wesgro 2021). The country has a confirmed population of 3 million citizens (Namibia Statistics Agency n.d.), and an annual population growth rate of approximately 3.2 per cent. Registration for identification takes place within the country's 14 political regions and has served as the primary form of ID for multiple purposes, including school enrolment as well as access to health services, which have since become universal.

Generally, birth certificates and foundational IDs became the official documentation of citizenship and personal information. While birth registration expanded significantly, challenges persisted in reaching remote communities and minority groups. Namibia has built an efficient and accessible home-grown identity management system, and achieved near-universal birth and death registration coverage (88 per cent and 94 per cent, respectively) (Elghandour 2023).

2.3 Evolution of the digital-ID landscape in Namibia

Identification under the German colonial administration (1884)

Namibia's journey towards a comprehensive digital-ID system has progressed through several key evolutionary stages. Research shows that civil registration existed during the German colonial regime from 1884 to 1915, and that the Civil Registrar for Births, Marriages, and Deaths for South West Africa was in place under the apartheid South African government until Namibia's independence in 1990 (Family Search n.d.).

During Namibia's colonial period, ID documents, primarily 'native passports' or *Paßmarken*, were used to control the local population, and were a tool of the German and later South African administrations. These documents, used during the era of German South West Africa (1884–1915), and South West Africa (SWA) under South African rule (1915–1990), were intended to identify and classify people, particularly Black Namibians, denying them full rights of citizenship (Hubbard 2021).

Identification under British colonial power

Registration for Whites, Coloureds and Indians, for South Africans and South West Africans, exists online from 1955 to 1966.[17] However, during the period of South African control, apartheid policies restricted the rights and freedoms of Black Namibians.

While Black Africans born during the South African rule and before 1990 were also registered as South African nationals and given ID documentation, despite being considered as South African citizens, Black Namibians did not have full rights of citizenship, including voting rights and land ownership rights (Legal Assistance Centre 2024).

ID under the South African colonial region

Under colonial occupation, Namibia's inhabitants were identified against their will first as German (from 1885), then British (from 1918), and finally South African (from 1949), but they lacked the full rights of citizenship of any country during that period. Apartheid policies denied Black Namibians many of the fundamental rights of citizenship (Hubbard 2021).

ID in post-independence identification

The Namibian constitution outlines a detailed system for citizenship by birth, descent, marriage, registration, and naturalisation, with an emphasis on gender-neutral provisions.

17 See, for example, this **online catalogue search.**

Upon independence in 1990, the Namibian government began the transitioning of national registration. This process was not without flaws, given that it was manually based and registration processes were not easily accessible.

The SWA ID cards remained in use post-independence. World Bank (2016) describes this scenario as follows: 'A complicating factor is the continued use of Southwest African (SWA) identity cards and the legacy register these represent.'

The Ministry of Home Affairs and Immigration (MHAI) became the custodian responsible for the technical and organisational infrastructure used to define, design, and administer the identity management system in Namibia. The ministry is mandated to manage and administer the National Population Register, facilitate lawful migration, and receive and protect refugees and asylum seekers.

The biometrics currently required to issue an ID card are a photograph, fingerprints of all ten fingers, and any other biometrics that may be set out in future by regulation.

This is due to the Department of Civil Registration using an integrated web-based system, the National Population Registration System (NPRS), with 4.7 million records digitalised (November 2015). The MHAI had completed the digitalisation of all existing records by 31 May 2016 (UNICEF 2023). Since 2011, the NPRS has linked children's records with those of their parent in the system.

1996 legislation

Before 2024, Namibian citizens applied for their ID cards as set out in Identification Act, 1996, No. 21 of 1996. To ensure that as many people as possible obtained their national IDs, the MHAI has been registering eligible pupils for IDs at secondary schools on an annual basis.

ID documents are generally used as a means to facilitate access to education, state welfare benefits, and financial services, as well as providing a basis for exercising rights (such as the right to vote), and providing access to a host of other public and private transactions (UNECA 2020).

Significant technological advancement occurred from 1996 with the digitisation of the identification system through integration of an automated fingerprint identification system. This upgrade computerised the application processing workflow, enabled biometric data capture, and established centralised record storage (*ibid.*). The digitisation marked Namibia's first substantial step towards a biometric ID infrastructure.

Digitalisation of ID

Efforts have been in place since 2017 for Namibia to roll out an Integrated Border Management System. Implemented in various phases, this system includes scans of travellers' faces, while digital fingerprints are checked against various international watch lists such as lists of wanted criminals, missing persons, and lost or stolen travel documents. Data collected at the border is held in a central database hosted by the MHAI.

This system was designed to replace he SWA ID cards that contained inaccuracies in terms of the surname, name(s), and date of birth of card holders, thereby requiring an amendment to be effected before the issuance of a Namibian National ID card. This required special processes to fast-track ID applications to ensure that all applicants had their case resolved.

Biometrics in the ID card

For persons whose births were registered in Namibia, the ID number on the ID card will be either the unique identifier assigned at the time of birth registration, or another unique number linked via a confidential system to the birth identifier.

2024 legislation

Around 2021, the Namibian government launched new-look ID cards (*The Namibia Economist* 2021) that could enable citizens to travel to neighbouring countries without a passport. This began with testing out at the border crossing between Namibia and Botswana. The implementation of the new IDs has been presented as an advantage of e-governance and is expected to spread to other SADC borders.

The MHAI further introduced a new e-passport with an electronic microchip containing biometric information that is used to authenticate the identity of the passport holder. This was in compliance with International Civil Aviation Organization requirements.

First biometric digital-ID (2025)

While Namibian citizens still have a variety of functional IDs to access different services, many have increasingly being replaced by the new foundational digital-IDs issued by the NPRS.

As of 2024, Namibia began the rollout of the digital-ID system, focusing on issuing digital-IDs to refugees, in particular, in June 2024. The issuing of biometric IDs is primarily meant to facilitate access to vital services for thousands of forcibly displaced persons living within the country's territorial borders.

According to the analysis of Hubbard:

> Although such systems at international borders are not unusual, some analysts have expressed concern about possible compromises to the confidentiality of the data in the Namibian system due to the cross-linking across different systems, as well as concerns about the possible ramifications of government dependence on private operators for system function and maintenance. (Hubbard 2024)

While the MHAI is the lead ministry in the provision of Namibian ID documents, other government agencies are also involved. Generally, the collection of the following biometrics are key for identification in Namibia: photograph, fingerprints, palm prints, departure dates from Namibia, birth details, marital status, and details of their death, where relevant.

One such agency is the Electoral Commission of Namibia, which collects biometrics under the mandate of voter registration under Electoral Act 5 of 2014. In Section 30, this act requires potential voters to provide a digital image and digital fingerprints. The voter registration card displays a barcode with encrypted registration details, including the voter's name, surname, and address, along with information on which elections the voter qualifies for (with local and regional elections requiring proof of residency in the relevant constituency or local authority).

Another form of functional ID is issued by the Roads Authority of the Ministry of Works and Transport. The agency issues driving licences after receiving a digital image and digital fingerprints of the driver. The driving licence also contains a barcode on the reverse side with information about the driver, which is linked to a biometric system that ensures that the licence is collected by the person to whom it is issued.

Related to the issuance of national IDs, biometric verification is then used in connection with accessing social grants (cash entitlements for those aged 60 and over, as well as orphans and vulnerable people). This is done through fingerprint identification using the recipient's Namibian ID, or in the case of benefits (cash entitlements) provided to veterans of the liberation struggle and their dependants, by means of a separate registration card that includes a photograph, fingerprint, and registration number.

To obtain employment In Namibia it is sometimes necessary to obtain a Certificate of Conduct from the Namibian Police, who provide background information on past criminal convictions. This process requires presenting one's digital-ID to the police. Certificates of Conduct are required for many purposes in Namibia, including tender bids, as well as obtaining

visas for international travel. This process requires application procedures that involve taking fingerprint biometrics for comparison against the police database in order to verify their identity. The fingerprints collected for this purpose are saved and stored by the Namibian Police, despite the lack of any underlying law governing the process.

Another example concerns requirements introduced in 2023 under Namibia's Communications Act, 2009 for mobile phone SIM card registration. The act requires telecoms service providers to collect and retain personal information about their customers.

Digital-ID timelines

As of 2023, Namibia announced the introduction of a digital-ID system. The first digital-IDs were issued to refugees in June 2024. Since then, biometric digital-ID has begun to be issued to facilitate access to vital services for thousands of forcibly displaced persons living within the country's territorial borders. Older IDs had a representation of a fingerprint and a bar code on the back, but since 2023 the biometric digital-ID has contained a chip, a QR code and a machine-readable zone.

In 2021, a local United Nations Development Programme (UNDP) digitalisation project, the Accelerator Lab, began work to support the most underserved communities, focusing on addressing the lack of legal ID documentation among residents in Groot Aub, a community outside of Windhoek. In its report, UNDP confirmed that that without recognised ID, many individuals were left on the margins of society, unable to access essential services or fully engage in socioeconomic opportunities.

UNDP reports that a number of other pilot projects have been launched since 2024 to test these digital-ID tools and fine-tune them for Namibia's distinct contexts (Maritz 2024). These pilots use various methods for documenting legal identities, aiming to identify the most efficient and accessible practices for wider implementation.

In 2019–22, the Directorate of National Population Register, Identification and Production began the implementation of an e-birth notification system (including locations where e-birth identification could take place), assessment of network connectivity, installation of equipment such as computers, with the assistance of funding from the United Nations Children's Fund, and training of staff members of the MHAI, Ministry of Health and Social Services, and the Namibian Police.

The MHAI highlights that the aim of the e-birth notification system is to notify the e-National Population Registration System (eNPRS) electronically when a vital event such as birth has occurred at a hospital, health centre,

or clinic to secure the birth details of the child and to ensure verification of the mother's identity against the NPRS. By 2019, the e-birth notification system had been successfully implemented at 22 sites country-wide.

In line with the electronic notification of births, the goal was that all deaths should also be notified electronically. An e-death notification system was successfully implemented at 26 sites country-wide.

However, to support these efforts, a number of policy decisions were necessary to establish a legal, institutional, and technical basis for a digitally integrated identity management system for Namibia.

Digitalisation statistics in 2025

Data on connectivity in Namibia varies; however, this research relies on publicly available data from DataReportal (2024) and Statista (2025). The essential headlines for digital adoption and use in Namibia in early 2024 are:

- There were 1.63 million internet users in Namibia at the start of 2024, when internet penetration stood at 62.2 per cent.
- 2.91 million cellular mobile connections were active in Namibia in early 2024, with this figure equivalent to 110.8 per cent of the total population.
- 4G network coverage in Namibia is estimated to amount to 89.37 per cent in 2025.
- Internet penetration in Namibia is estimated to be about 77.78 per cent in 2025.

Challenges with implementation of digital-IDs

World Bank (2016) has raised concerns about the human, financial, and technological resourcing of Namibia's digital-ID programme, stating that it is important that sufficient resources are available for the design, development, and deployment of the system. The report's authors called for a detailed cost-benefit analysis of the investment needed to put in place the necessary infrastructure (connectivity, hardware, security, and software) and human resources (training and appropriate technical skills), and to promote user acceptance and uptake.

Biometrics related to IDs have been collected for various purposes in Namibia, mostly without legally authorised protection.

The Civil Registration and Identification Act, Act 13 of 2024 (Republic of Namibia n.d.a), was gazetted in December 2024 while awaiting operationalisation. Section 3 of this report will assess the adequacy of this legal framework for digital-ID using the Centre for Internet and Society's rule of law tests. Although the act contains essential elements of data

protection, the lack of a dedicated data protection law creates a number of human rights concerns, which will be addressed in Section 4 below.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Yes. Digital-ID in Namibia is backed by the Civil Registration and Identification Act, 2024, which was passed in December 2025, but is not yet fully operationalised – the government still needs to finalise work on pending efforts to put in place a personal data protection law. Previously, Namibia relied on an outdated national statute that made the registration of births, marriages, and deaths obligatory. The Civil Registration and Identification Act, 2024 requires that all citizens and permanent residents aged 16 years and over apply for Namibian ID documents.

Despite these many efforts, there is a clear lack of oversight mechanisms that leaves room for legal ambiguity, and the potential for overreach in data management and delegation of authority. As the legislation is very new and implementation in its early stages, at the time of writing (mid-2025) it is too early to assess whether implementation will meet the ambition of the legislative framework or if it will have to be tested in the courts.

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Yes. Overall, the act provides for six key objectives:

1. To provide for compilation and maintenance of a Civil Register;
2. To provide for the appointment of Registrar-General and Registrars;
3. To determine the age of certain persons recorded in the Civil Register in accordance with this Act;
4. To provide for name changes and other alterations to the Civil Register;
5. To provide for the issue of ID documents to certain persons listed in the Civil Register;
6. To provide for an Appeals Tribunal and incidental matters.

(Republic of Namibia n.d.a)

While it is yet to live up to its name, that of Civil Register, the act mentions e-services such as e-death notices, biometrics, and other

electronically provided notifications and databases. However, it does not provide much detail about the digital-IDs.

Part 3, Section 5 of the act deals with setting up, compiling, and maintaining a Civil Register for Namibia that would consist of details from the Birth Register, adopted from the Child Care and Protection Act, the Marriage Register, Death Register, and Identity Register. Section 27 of the act stipulates that the register should perform its duty in coordination with the Registrar-General, who must assign a unique identifying number to every person whose birth is registered in Namibia, and in the case of any other person, at the time of the creation of a personal profile of that person in the Civil Register. The act, however, does not clearly define the roles of other key actors that rely on the digital-ID system, including the Electoral Commission of Namibia (for voter registration), the Namibia Revenue Agency (for tax payment efforts), and telecoms companies (for mandatory SIM card registration), as well as financial institutions, and private sector entities such as banks and telecoms providers.

While in Section 74 the act positions appeals to the Registrar-General in terms of aggrievement by a decision of the registrars and how to submit appeals related to decisions of registration such as name changes, refusals to register, and withdrawal of documents, the Civil Registration and Identification Act, 2024 lacks a comprehensive redress framework for individuals affected by data misuse, leaving data owners without clear legal channels to challenge privacy violations. As Namibia's Data Protection Bill remains in draft format, it is not clear if civil registration data would be its key component.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

No. The Civil Registration and Identification Act, 2024 does not clearly and comprehensively specify the actors involved in the digital-ID ecosystem or the full range of purposes that flow from its legitimate aim. However, Section 58 of the act addresses verification and authentication of identity, mentioning that on written request the Registrar-General 'may verify or authenticate the information in an ID document presented by a data subject to any other person, or to any public or private entity'.

In this regard, the act offers limited detail on which entities, either public or private, it will guarantee verification. Section 68 of the act deals with issues

of disclosure of information from the Civil Register or related files to organs of the state, and Section 63 to private entities. While also dealing with issues of access to one's own information in the Civil Register (Section 59), and access to information by law enforcement or intelligence authorities (Section 66), the act does not go into further detail on the processes by which entities can access the register (such as the Electoral Commission, for voters' registration verification, or the Namibia Revenue Agency, for tax identity purposes), nor does it provide a clear framework on their involvement. This in itself raises concerns about data sharing, integration, accountability, and oversight.

While the purposes of the registration and attainment of documentation are clearly indicated in the Identification Act, Act 21 of 1996, both this old act and the Civil Registration and Identification Act, 2024 fail to articulate how this aim translates into specific, legitimate purposes across various sectors. Without detailed provisions connecting each use of digital-ID data to a legitimate aim – such as delivering public services, reducing fraud, or ensuring electoral integrity – the legal framework does not establish substantial purpose limitations. Thus, the law provides only a general foundation for the digital-ID system, and lacks the clarity and precision necessary to ensure the system is used lawfully and proportionately.

Additionally, other ministries, departments, and agencies that have some access to various ID systems are the:

- Ministry of Health and Social Services
- Ministry of Gender Equality and Child Welfare
- Namibia Statistics Agency
- Ministry of Justice
- Office of the Prime Minister
- Ministry of Education
- Ministry of Labour, Industrial Relations and Employment Creation
- Government Institutions Pension Fund.

Support for the attainment of national documents has been offered by:

- The United Nations Children's Fund
- UNDP
- The United Nations Economic Commission for Africa.

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

There is no dedicated and easily accessible avenue within the digital-ID framework to lodge a complaint, request an investigation, or obtain timely resolution. It is not clear if this is because of the lack of a data protection law preceding the new Civil Registration and Identification Act, 2024.

While the current law establishes a Registrar-General as well as an Appeals Tribunal as part of oversight bodies mandated with disputing and addressing matters related to registration, the act does not make clear the importance of monitoring the digital-ID system, investigating grievances, or imposing penalties on those who breach data protection principles. In the absence of a data protection law in the country, this creates an overall accountability vacuum for individuals and institutions that use or manage digital-ID data, and leaves individuals vulnerable to harm, without sufficient legal protections.

Overall, the legal framework governing digital-ID in Namibia under the Civil Registration and Identification Act, 2024 does not provide clear or comprehensive redress mechanisms for individuals whose rights may be violated through the use or misuse of the digital-ID system. Even with the established responsibilities of the Registrar-General and the Appeals Tribunal, the act lacks explicit procedures for individuals to challenge decisions, correct errors, or seek remedies when their data is mishandled or misused by government agencies or third parties.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

In the absence of operationalisation of the Civil Registration and Identification Act, 2024 and development of related regulations, the country has not set up clear accountability systems for governing bodies or for users of the digital-ID. Regulations on how other related actors access and engage with data related to the digital-ID are limited and underdeveloped. Consequently, there is no accountability framework that clearly defines the responsibilities of all actors involved, nor have mechanisms been created for monitoring compliance, investigating misconduct, or enforcing penalties.

While multiple private and public agencies have integrated digital-IDs into their operations, this has been happening without clear legal frameworks governing such integration. Overall, this contributes to

the risk of misuse, overreach, and unauthorised access to personal information without consequence. Namibia is yet to pass a data protection act, which would establish clear responsibilities for data controllers and processors, and provide a legal basis for holding actors accountable for breaches or abuse of personal information.

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

Namibia does not have well-defined legislative mechanisms to address mission creep cases when using digital-ID. This is because of the lack of operationalisation of the Civil Registration and Identification Act, 2024 and lacklustre implementation of related regulations. In addition to the absence of a data protection law, there are no detailed provisions that limit the use of ID to its original purpose, nor are there clear safeguards to prevent expansion into unintended or unauthorised areas of use.

The act puts forward an Appeals Tribunal, reporting to the minister of home affairs, who is accountable to Parliament. However, the role of parliamentary oversight is not clearly indicated in this instance, nor is judicial oversight in broader terms, and how they come into being. While parliament has a parliamentary committee on information and communications technology and innovation, as well as another on constitutionalism and legislative matters, it is not clear if these are important players in detecting, assessing, or even preventing mission creep.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

The aim of the Namibia Identification Act, Act 21 of 1996 (Republic of Namibia n.d.d), is to provide for the compilation and maintenance of the National Population Register in respect of the population of Namibia, for the issuance of ID documents to persons whose names are included in the register; and for matters connected therewith. The subsequent Civil Registration and Identification Act, 2024 aims to provide for the compilation and maintenance of a Civil Register, as well as to provide for the appointment of a Registrar-General and Registrars, among others. However, the latter implementation is yet to take place due to, among other reasons, the lack of data protection mechanisms as the country has no related laws in place. As such, privacy concerns in the context of accessibility of such data by other players, remain unanswered and are undermining legitimate use.

When designed well, digital-ID systems can support effective service delivery, as well as transparent state functions. However, this can only be realised given a clear legal provision governing its extended use, especially in sensitive areas such as elections and financial institutions.

Without strong safeguards, redress mechanisms, or oversight, the risks of exclusion, voter manipulation, privacy breaches, and abuse of power are heightened. The absence of clear boundaries about who can access and use digital-ID data further intensifies these concerns.

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

With the recently passed Civil Registration and Identification Act, 2024 in place, the country still lacks broader data governance frameworks, and a related mechanism for data regulations remains underdeveloped. The Data Protection Bill has remained in draft format since 2014 and creates a regulatory gap that exposes citizens to potential data misuse.

The use of digital-IDs for refugees and for travel between other countries such as Botswana further amplifies the challenges of the use of the digital-ID system beyond its original mandate. There is a need for strong legal

safeguards, oversight, and redress mechanisms in order to prevent abuse, protect individual rights, and ensure the digital-ID system serves the public good rather than becoming a tool for surveillance or exclusion.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

In its current form, the Civil Registration and Identification Act, 2024 falls short of clearly articulating strong data protection principles or imposing strict limitations on who can access, use, or share digital-ID data generated through both public and private use. Additionally, no specific legal provisions define or regulate the creation of a digital trail or digital footprints when digital-ID is utilised across various services such as banking, telecoms, voting, and social welfare.

This challenge is compounded by the lack of an overarching data protection mechanism generally in the country. Without a data protection law, there is no requirement for consent, no independent oversight of data-sharing practices, and no legal obligation for state or private entities to notify individuals about how their data is used or stored. This means that once a person's digital-ID is used for a government transaction or a commercial service, limited safeguards prevent access to or repurposing of that information without their knowledge.

Public and private entities extensively use Namibia's digital-ID system for identity verification. However, the lack of clear regulations and enforceable standards regarding data collection, storage, and sharing has resulted in significant legal and institutional deficiencies. This highlights the urgent need for a comprehensive data protection framework to ensure privacy, transparency, and accountability in the use of digital-ID data.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Namibia lacks sufficient mechanisms to ensure that the adoption of digital-ID does not result in exclusion or restricted access to entitlements or essential services. Concerns have been raised about the potential for exclusion, particularly among marginalised populations of elderly people, young people, and indigenous communities.

Anecdotally, 50,000 elderly people could not access their social grants due to systems challenges with accessing the system their thumbprints. This situation highlights a number of fundamental issues: expanding the ID's use beyond its original purpose of enabling universal and compulsory registration could create systemic exclusion, especially in the absence of adequate infrastructure and renewal mechanisms.

Rural populations, individuals living in poverty, persons with disabilities, and those without supporting documentation often face challenges during the registration process (Bhatt *et al*. 2021). Service providers and institutions frequently deny access to services due to the absence of a national ID. The lack of fallback options and accountability frameworks exacerbates the risk of systemic exclusion. This situation deepens existing social and economic inequalities, particularly for those among the unbanked section of society.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

Although the national ID system aims to enhance identification and service delivery, its mandatory use – especially in contexts such as voting, accessing public services, and mobile phone registration – presents risks of exclusion for individuals who do not have a digital-ID or face challenges in obtaining one.

The Civil Registration and Identification Act, 2024 allows all Namibian citizens aged 16 and over to register and obtain a national ID card, while registration must take place immediately upon birth. The digital-ID system was introduced to conform with universal registration to address challenges to inclusion in public service delivery. Hence, the ID is a central reference point, linking individual identities across various platforms to streamline services and provide access to both public and private services, such as banking, SIM card registration, and social benefits, in effect making it mandatory.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

As in other countries where the use of digital-IDs has been uniformly adopted, Namibia has not established a clear framework clear regarding the legitimacy of their use; their benefits, and their impact on individual rights are not systematically informed by comprehensive risk assessments. Although the Civil Registration and Identification Act, 2024 provides a legal foundation for the Civil Register, it lacks clear provisions requiring or guiding risk assessments related to the expanded use of digital-IDs across sectors such as banking, telecoms, and elections.

Despite the Civil Registration and Identification Act, 2024 not having been operationalised and without the Data Protection Bill having been passed, the government implemented a digital-ID system without the Data Protection Bill being passed and related regulations being in place. As such, decisions regarding the repurposing of the digital-ID, such as making it mandatory for SIM card registration, voter registration, banking, social welfare benefits, and more, are often made without transparent, formal risk assessments that consider the implications for privacy, exclusion, or misuse. This lack of assessment has the potential to undermine public trust in the digital-ID system.

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

Namibia's current legal and regulatory framework does not explicitly provide for a differentiated approach to governing the various uses of digital-ID based on their risk levels. The Civil Registration and Identification Act, 2024 largely focuses on the civil registration of citizens and the issuance of national identity cards. It fails to set out risk-based or sector-specific guidelines for how digital-IDs should be used across different domains.

Similarly, while the Electronic Transactions Act 4 of 2019 (Republic of Namibia n.d.c) provides for digital signatures and offers a general framework for online security, it lacks specific provisions that would enable a tiered or contextual governance approach, depending

on the sensitivity of the use case. In its current approach, there is an increased risk of mission creep when digital-ID is applied in new contexts without clear legal oversight or accountability mechanisms.

The awaited Data Protection Bill has the potential to introduce more nuanced, risk-informed governance through tools such as data protection impact assessments and purpose limitation; however, the bill remains to be passed. As a result, the regulatory environment does not yet support a differentiated, risk-based use of digital-ID.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

The legal framework on digital-ID in Namibia has not explicitly set out a clear governance outlook that is proportional to the likelihood and severity of risks associated with its use. The foundational law, the Civil Registration and Identification Act, 2024 is still to be operationalised, and primarily focuses on establishing the Civil Register and mandating universal registration for citizens aged 14 and over. However, in its current form, it lacks risk-based or proportional governance mechanisms.

Ideally, proportional governance would require that the law distinguish between low-risk and high-risk uses of digital-ID. However, in the current framework the digital-ID system is presented as a one-size-fits-all solution, lacking customised safeguards, oversight, or access controls in relation to the possible severity of harms, such as privacy violations, exclusion, or misuse of surveillance.

Although not yet enacted, the Data Protection Bill has the potential to deal with issues of proportionality through requirements such as data minimisation, purpose limitation, and data protection impact assessments.

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

Namibia has not defined legal mechanisms to prohibit or restrict the use of digital-ID in cases that pose a demonstrably high risk to individuals' rights. The Civil Registration and Identification Act, 2024 only focuses on registration

processes and the establishment of the Civil Register. However, it does not contain specific provisions for risk-based restrictions on using identity data.

The lack of mechanisms to address risk poses clear challenges for digital-ID systems, given political sensitivity around high-risk areas such as biometric voter registration, which has already been used in the country. These applications of digital-ID heighten the risk of exclusion, surveillance, or political manipulation, especially in a context characterised by limited oversight and underdeveloped data protection infrastructure. As such, the lack of clear guidance or precedent for restricting high-risk uses of digital-ID remains a national framework risk.

6. Conclusion

With digital transformation rising across the continent, Namibia's focus on digital inclusion and legal ID governance serves as a model for other African nations facing similar challenges.

The introduction of a biometrically based digital-ID system in Namibia marked a significant shift in the country's civil registration and identity verification processes. As in the case of other previously colonised countries, ID systems in Namibia served as tools of control, from colonial-era tax records and labour passbooks to post-independence political surveillance. The new digital-ID aimed to reverse this legacy by providing secure, universal ID that enhances access to essential services, and meeting sustainable and national development imperatives. It has the potential to become a critical component of Namibia's administrative infrastructure, supporting sectors such as banking, telecoms, social services, and elections. However, despite these advancements, the system faces substantial legal, operational, and ethical challenges. These include bureaucratic inefficiencies in ID renewal, poorly implemented legal frameworks, and inadequate safeguards for data protection and user rights.

The risks are amplified by the system's expansion into politically sensitive areas, as in the case of refugees' use, where the implementation started, but also in its use in voter registration, where manipulation can easily be cited by opposing parties. The digital-ID's mandatory nature in accessing basic services, combined with the barriers marginalised groups face, raises concerns about exclusion and inequality. The lack of a risk-based, context-sensitive governance model has resulted in a one-size-fits-all approach that overlooks the varying implications of ID use across sectors. Furthermore, rights-based principles such as necessity, proportionality, and data minimisation are under-emphasised in the current framework. Moving forward, the success of the digital-ID will depend on fully operationalising the Data Protection Bill, which has been in draft format since 2014; this has the potential to strengthen oversight, and ensure inclusivity. For the system to fulfil its promise of empowering citizens and promoting development, it must be restructured to prioritise justice, accountability, human rights, and efficiency.

Therefore, Namibia should pass this law without further delay as it is increasingly becoming intersectional with the Civil Registration and Identification Act, 2024 (Republic of Namibia n.d.a) and also other service delivery provisions. It must ensure that necessary oversight mechanisms are in place, in addition to ensuring recourse for individuals.

7. Bibliography

BiometricUpdate.com (2024a) ***Namibia Begins Issuance of Much-Anticipated Biometric ID Cards to Refugees***, 24 June (accessed 17 October 2025)

BiometricUpdate.com (2024b) ***Namibia's New CRVS, National ID System Reflects Key Data Protection Aspects***, 9 September (accessed 17 October 2025)

BiometricUpdate.com (2024c) ***Namibia Pushes for Inclusive Digital Identity Systems Through Legal Identity Governance***, 1 November (accessed 17 October 2025)

DataReportal (2024) ***Digital 2024: Namibia*** (accessed 17 October 2025)

Elghandour, I. (2023) *Legal Identity for All: What Can Madagascar Learn from Namibia?* 10 October, World Bank

Hubbard, D. (2024) ***Namibia Navigates Biometric Data Privacy Pending Civil Registration Bill***, Association for Progressive Communications, 4 November (accessed 17 October 2025)

Hubbard, D. (2021) *Report on Citizenship Law: Namibia*, 14 January, European University Institute

International Development Research Centre (2019) 'Case Study 4: Namibia in Centre of Excellence for Civil Registration and Vital Statistics (CRVS) Systems', *Compendium of Good Practices in Linking Civil Registration and Vital Statistics (CRVS) and Identity Management Systems*

Legal Assistance Centre (2024) ***Namibian Citizenship Act 14 of 1990*** (accessed 17 October 2025)

Legal Assistance Centre (2022) *A Sex Offender Register for Namibia? Right Idea, Wrong Solution*, Pro Bono series

MacroTrends (n.d.) ***Namibia Life Expectancy 1950–2025*** (accessed 17 October 2025)

Maritz, Y. (2024) ***UNDP Namibia: Pioneering Digital Legal Identity Governance for Inclusive Development***, United Nations Development Programme, 30 April (accessed 17 October 2025)

Mayhew, S. (2018) 'Namibia Makes the Switch to Biometric Passports', *Biometrics*

Ministry of Home Affairs, Immigration, Safety and Security (n.d.) ***ID Registration*** (accessed 17 October 2025)

Namibia Statistics Agency (n.d.) ***2023 – Population and Housing Census*** (accessed 17 October 2025)

Nashama, S. (2024) '**Mass Civic Registration Program Prompts 17,182 Applications for National Documents**', *Windhoek Observer*, 14 March (accessed 17 October 2025)

Parliament of Namibia (2019) ***Ministry of Home Affairs, Vote 5, Budget Motivation, 2019/2020***, 25 April (accessed 17 October 2025)

Parsons, N. (2019) ***A Brief History of Botswana*** (accessed 17 October 2025)

Republic of Namibia (n.d.a) ***Civil Registration and Identification Act, 2024*** (accessed 17 October 2025)

Republic of Namibia (n.d.b) *Communications Act 8 of 2009, Section 73: Duty to Obtain Information Relating to Customers ID, Regulations 3 and 5*

Republic of Namibia (n.d.c) ***Electronic Transactions Act 4 of 2019*** (accessed 17 October 2025)

Republic of Namibia (n.d.d) ***Identification Act 21 of 1996*** (accessed 17 October 2025)

Statista (2025) ***Digital & Connectivity Indicators – Namibia*** (accessed 12 November 2025)

The Namibia Economist (2024) '**Population Surges to Over 3 million: Census Report**', 13 March (accessed 17 October 2025)

The Namibia Economist (2021) '**New Secure Identification Cards That Can Double As Travel Documents to Neighboring Countries**', 22 November (accessed 17 October 2025)

The Namibian (2023) '**Home Affairs Considers Introducing Digital IDs**', 21 August (accessed 17 October 2025)

The Namibian Sun (2024) '**91 Per Cent of Namibians Able to Read and Write – Ministry**', 10 September (accessed 12 November 2025)

UNECA (2020) ***Snapshot of Civil Registration and Vital Statistics Systems of Namibia***, Centre Of Excellence For CRVS Systems, United Nations Economic Commission for Africa (accessed 17 October 2025)

UNICEF (2023) ***Namibia***, Civil Registration Vital Statistics and Identity (CRVSID) Country Case Studies, United Nations Children's Fund (accessed 17 October 2025)

Wesgro (2021) ***Namibia*** (accessed 17 October 2025)

Windhoek Observer (2024) '**Namibia's Population Surpasses Three Million**', May (accessed 17 October 2025)

World Bank (2016) ***Namibia Identity Management System Analysis Report***, Washington, DC: World Bank (accessed 17 October 2025)

Digital-ID in Botswana: Country report

Lesedi Bewlay

 DOI: 10.19088/IDS.2025.063

1. Introduction

This report examines Botswana's biometric digital identification (digital-ID) system, centred on the 'Omang' national identity card, which has evolved from a paper-based ID introduced in 1988 to a biometric platform incorporating fingerprint and facial recognition technologies. The Omang card serves as a general ID document for accessing various services such as voting, registering land titles, opening bank accounts, and collecting social security benefits (Government of Botswana 2025a; Embassy of the Republic of Botswana, Washington, DC 2025). Specific initiatives within the digital-ID ecosystem have defined purposes. Mandatory SIM card registration (2009) aimed to enhance security, while e-passports (2010) were introduced to reduce forgery (Ndlovu 2024b). The significance of the Omang system extends beyond mere identification, serving as a gateway to essential services, facilitating cross-border movement, and underpinning government efforts to transform Botswana into a knowledge-based digital economy.

This research assesses the current state of Botswana's digital-ID system, its legislative framework, and operational implementation against established rule of law, rights-based, and risk-based tests. Through this evaluation, the report identifies strengths and vulnerabilities in the system's design and governance, examining how effectively it balances security considerations with citizens' rights to privacy, inclusion, and non-discrimination. The analysis proceeds through five interconnected sections: examining the historical ID landscape in Botswana, applying rule of law tests to assess legal foundations, employing rights-based tests to evaluate human rights implications, using risk-based tests to identify and assess governance of potential harms, and concluding with findings and recommendations for improvement.

2. History of ID in Botswana

2.1 Colonial ID systems

In pre-protectorate Botswana, identity was established through social structures rather than formal documentation, primarily determined by tribal affiliations and lineage. Cattle ownership functioned as both an economic asset and a significant marker of social standing (Jerven Bolt and Hillbom 2013). Identity verification occurred through oral traditions, with family relations and tribal membership serving as the principal means of establishing identity.

Britain proclaimed the Bechuanaland Protectorate – the colonial name for present-day Botswana – in March 1885, primarily to block Boer and German expansion from neighbouring Cape Colony (present-day South Africa). The administration governed through a policy of indirect rule, relying on the authority of Tswana chiefs (plural: *Batswana*, the Setswana-speaking majority ethnic groups) to enforce the new regulations. In 1891, the High Commissioner extended selected Cape Colony statutes to Bechuanaland, creating racially differentiated legal frameworks for 'Europeans' and 'natives', and introducing the first pass and labour-registration systems that would later shape post-independence ID practices (Booi 2006).

The protectorate administration introduced formal ID documentation systems. Travel and residence documentation was established for Europeans and British subjects, while pass systems and labour registration requirements were implemented for indigenous Batswana. These systems regulated movement between districts and documented employment status, particularly for labour migration to South African mining operations (Parsons 2019). These early identification practices established procedural precedents that would influence post-independence approaches to ID documentation.

2.2 Post-liberation ID systems (pre-digital)

Following independence in 1966, Botswana's government prioritised developing a formal civil registration system. Registration became compulsory nationwide, with services strategically decentralised to 12 districts and 24 sub-districts to improve accessibility. The Ministry of Home Affairs was designated as the government body responsible for overseeing civil registration processes (Poloko 2017).

Birth certificates emerged as Botswana's foundational ID credential during this period, providing official documentation of citizenship and

personal information. While birth registration expanded significantly, challenges persisted in reaching remote communities and minority groups, with registration rates reaching 83.2 per cent by 2015–16 (*ibid.*).

The introduction of the Omang national identity card in 1988 marked a watershed moment in Botswana's ID systems. This initiative established a single, compulsory ID credential for all citizens aged 16 and over. The Omang card, whose name derives from the Setswana phrase '*Ke Omang*?' meaning 'Who are you?', was initially a laminated, bar-coded paper card containing the holder's photograph, fingerprint, and biographical information (Security SA 1999). The National Registration Act of 1986 provided the legal framework, mandating registration and establishing penalties for non-compliance (Government of Botswana 1993a).

2.3 Evolution of Botswana's digital-ID system

Botswana's journey towards a digital-ID system has progressed through several evolutionary stages. The Omang card represented Botswana's early adoption of a standardised national ID framework, positioning the country as an early implementer within the Southern African Development Community of a compulsory national ID system (van Rooyen 1999; Ndlovu 2024b).

An advancement occurred in 1999 with the digitisation of the Omang system through the integration of an automated fingerprint identification system (AFIS), , part of broader technological improvements being implemented across the region during this period. This upgrade computerised the application processing workflow, enabled biometric data capture, and established centralised record storage (van Rooyen 1999).

The digital-ID ecosystem expanded with the implementation of mandatory SIM card registration in 2009 and e-passports in 2010, which incorporated additional biometric identifiers (Ndlovu 2024b). In 2017, the launch of a multi-biometric platform integrated facial recognition capabilities with the existing fingerprint ID system (Paradigm Initiative 2021).

The government formalised its digital strategy in 2020 with the SmartBots Digital Transformation Strategy, aiming to transform Botswana into a knowledge-based economy through efficient public service delivery (SmartBots 2021). In May 2023, Botswana engaged in cross-border collaboration with Namibia, contracting German identity technology company Veridos to build an interoperable platform that would allow citizens of both countries to use their national ID cards for automated checks at the Mamuno–Trans-Kalahari border crossing (McConvey 2023).

2.4 Current structure and implementation of the digital-ID system

Administrative framework and requirements

The current digital-ID system is administered primarily by the Department of Civil and National Registration under the Ministry of Nationality, Immigration and Gender Affairs (Government of Botswana 2025a). Technical support and infrastructure management are provided by the Department of Shared Digital Services within the Ministry of Communications, Knowledge and Technology, which oversees IT systems and security protocols (Government of Botswana 2025c).

Since 2011, first-time Omang applicants must present a certified birth certificate (now a compulsory 'breeder' document), copies of both parents' identity cards or passports, and two recent passport-style photographs (World Bank 2015; Embassy of the Republic of Botswana, Washington, DC 2025). This reliance on foundational documents demonstrates the connection between Botswana's civil registration system and its digital-ID infrastructure, which was further strengthened when the system was digitised in 1999 with the implementation of the AFIS.

Coverage and accessibility

According to the 2022 Population and Housing Census, 86.7 per cent of individuals aged 15 and over possess an Omang card, indicating substantial coverage (Statistics Botswana 2023). Approximately 13.3 per cent of the eligible population remain unregistered, representing roughly 200,000 people out of Botswana's 1.5 million eligible citizens (*ibid.*). Field studies indicate that most unregistered individuals are concentrated in sparsely populated western districts and include Basarwa (San) communities, where geographical isolation creates barriers to enrolment (Minority Rights Group 2018).

Those without Omang cards tend to be from several overlapping demographic groups: indigenous minorities such as the San people who face historical marginalisation; rural populations in remote areas with limited transportation infrastructure; persons with disabilities who encounter accessibility challenges; and economically disadvantaged individuals (World Bank 2019; Governance4ID 2025). Young people who have just reached the age of eligibility also represent a significant portion of the unregistered population.

Without an Omang card, citizens are excluded from exercising fundamental rights such as voting, accessing public services including health care

and social assistance, opening bank accounts, registering SIM cards, and securing formal employment (Ndlovu 2024b). This exclusion can perpetuate intergenerational cycles of marginalisation, as children whose parents lack ID documentation may face additional barriers to establishing their own legal identity (Ansar and Clark 2025).

Technical infrastructure and partnerships

The current technical implementation captures multiple biometric identifiers, including fingerprints and facial images, to enhance security and ensure unique ID (Paradigm Initiative 2021). These biometric components are also incorporated into Botswana's e-passports, extending biometric verification across different ID documents (Ndlovu 2024b).

Funding for Botswana's digital-ID system comes from various sources, including the European Union and International Development Research Centre (Expertise France 2022; IDRC 2025). Private sector suppliers include Face Technologies (South Africa), IDEMIA (France), and Veridos (Germany). Contract values have not been published, but press releases confirm their roles in the Omang card's production (van Rooyen 1999) and the 2017 multi-biometric upgrade (IDEMIA 2017), while Veridos supplies infrastructure for the cross-border ID system shared with Namibia (McConvey 2023).

Digital context and implementation factors

The implementation of Botswana's digital-ID system operates within the broader context of the country's digital landscape. Botswana's digital-ID system has been made possible by the rapid expansion of cellular and digital government services. According to DataReportal (2025), internet penetration reached 81.4 per cent in early 2025, with 2.07 million internet users. The country has 4.21 million active cellular mobile connections (active registered SIM cards), representing 166 per cent of the total population of 2.54 million, indicating widespread mobile (cell) phone usage, with many individuals maintaining multiple SIM cards (DataReportal 2025).

A disparity exists between urban and rural areas regarding connectivity. While urban centres have high-speed internet access, rural areas experience limited or non-existent connectivity (Masendu 2024). This disparity affects rural citizens' ability to access digital services. Additionally, internet access costs present an economic barrier to digital inclusion (Paradigm Initiative 2021).

Varying levels of digital literacy exist across demographic groups. Younger and urban populations generally demonstrate greater technological proficiency compared to older citizens and rural communities (Daily News 2024). Implementation considerations for

Botswana's digital-ID system include access across geographical locations, connectivity infrastructure, privacy frameworks, and interoperability with other government and private sector systems (African Declaration on Internet Rights and Freedoms 2024; Ndlovu 2024b).

However, a notable digital divide exists between urban and rural areas, with urban centres having high-speed internet access while rural areas experience limited connectivity (Masendu 2024). Digital literacy levels vary significantly across the population, with younger and urban demographics demonstrating greater comfort with technologies (Daily News 2024).

2.5 Drivers of digital-ID

A key public driver is SmartBots, the Government's 2020 Digital Transformation Strategy, aimed at modernising public services and expanding broadband nationwide (SmartBots 2021). Advocates claim digital-ID will cut fraud, ease cross-border travel, and spur e-commerce, though independent evaluations have yet to demonstrate measurable benefits (Governance4ID 2025).

Implementation carries significant risks including privacy concerns given the extensive personal data involved (*ibid.*), potential state surveillance (Paradigm Initiative 2021), exclusion of vulnerable groups lacking digital access (African Declaration on Internet Rights and Freedoms 2024), and biometric data security concerns. A breach could enable identity theft, fraudulent benefit claims, and long-term reputational harm to victims (Ndlovu 2024b; MacDonald 2024).

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Botswana's digital-ID system finds its legal foundation in the National Registration Act of 1986, which mandates registration for citizens aged 16 and over, and provides the framework for the Omang identity cards (Government of Botswana 1993a). This legislation specifies the collection of personal details including name, residence, sex, date of birth, and marital status. However, established in 1986 and amended in 1993, the act pre-dates contemporary digital-ID systems, raising questions about its adequacy in addressing modern technological complexities.

Botswana strengthened its legal framework when Parliament passed the Data Protection Act 2024 on 29 October 2024; the act entered into force on 14 January 2025, repealing the stalled 2018 version (TechHive Advisory 2024; Michalsons 2024). This introduced comprehensive regulation of personal data processing, establishing principles for lawful data handling, and designating the Information and Data Protection Commission (IDPC) as the supervisory authority (TechHive Advisory 2024).

The minister responsible for nationality, immigration, and gender affairs holds authority over the national registration system, including appointing registrars, prescribing implementation regulations, and authorising government access to the national register (Government of Botswana 1993a).

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

Botswana's National ICT Policy 'Maitlamo' (translated as 'commitment' in English) frames the public-interest aim of accelerating socioeconomic development by making government services faster, cheaper, and more transparent (Paradigm Initiative 2021). The multi-biometric platform upgrade aims to integrate identification operations across government ministries (*ibid.*), serving the legitimate aim of improving efficiency.

The SmartBots Digital Transformation Strategy (2020) outlines Botswana's plan to transition to a knowledge-based economy, focusing on digitising

the public sector and enhancing service delivery (SmartBots 2021). Digital-ID plays a crucial role in enabling e-government services under this strategy.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

In December 1993, the National Registration (Amendment) Act, 1993 inserted a Third Schedule that authorises four government bodies to draw on Omang data: the Botswana Police Service, the Department of Surveys and Lands, the Elections Office (today's Independent Electoral Commission), and the Department of National Transport and Communications (Government of Botswana 1993a). The Omang card functions as the primary means of ID for accessing government services, though specific services are not exhaustively detailed.

The role of private entities in using or insisting on digital-ID is now regulated by the Data Protection Act 2024, which applies to all 'data controllers' and 'data processors', public or private. Sections 2 and 22 classify fingerprints, facial images, and other biometric identifiers as 'special personal data', while Sections 17–19 restrict their collection, storage, and onward use to situations in which individuals have given their explicit consent, or the processing is authorised by written law and accompanied by strict purpose- and storage-limitation safeguards. Consequently, mobile network operators carrying out SIM card registration and banks deploying biometric authentication must satisfy the act's security and retention requirements and remain subject to oversight by the Information and Data Protection Commission (Sections 42–46) (Botswana Laws 2018).

Section 6 of the National Registration Act obliges every citizen to register within 30 days of turning 16 (or acquiring citizenship), including submission of fingerprints and a photograph, on pain of criminal sanction (Government of Botswana1993a). Individuals cannot opt out of the Omang system entirely. Section 6(1) of the National Registration Act requires every citizen to register within one month of turning 16 or acquiring citizenship, with Section 18(a) establishing that failure to register within the prescribed time constitutes an offense subject to penalties under Section 19 (*ibid.*).

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

Botswana's Data Protection Act 2024 requires data controllers to notify the IDPC within 72 hours of data breaches that put individuals' rights and freedoms at risk (DLA Piper 2025). Affected individuals must be promptly informed of such breaches.

The act grants individuals several rights regarding their personal data, including access, correction, deletion, and objection to processing under certain circumstances (Michalsons 2024). The IDPC handles data protection complaints, while the Botswana Communications Regulatory Authority addresses complaints against communications service providers (BOCRA 2025). The Office of the Ombudsman investigates complaints of improper administrative conduct within the public sector (Government of Botswana 2025b).

The Data Protection Act 2024 allows individuals to pursue judicial remedies for damages resulting from unlawful processing (Botswana Laws n.d.).

While these mechanisms offer avenues for redress, their effectiveness specifically for digital-ID-related issues requires ongoing evaluation.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

Accountability measures for Botswana's digital-ID system are embedded in the legal framework. The National Registration Act specifies the Registrar's responsibilities and establishes penalties for offenses such as providing false information during registration (Government of Botswana 1993a). The Data Protection Act 2024 enhances accountability, with stringent penalties for non-compliance with data-processing requirements and breach notification obligations (TechHive Advisory 2024).

The IDPC serves as the primary regulatory body responsible for ensuring compliance with data protection regulations (Michalsons 2024). The commission can conduct investigations, issue sanctions, and advocate for data subjects' rights (MISA 2025). However, questions remain about the commission's operational independence and resource adequacy (Ndlovu 2024b).

The courts have shown willingness to intervene in digital-ID matters. In *ND v Attorney-General* (2019), the High Court ordered the Registrar

of National Registration to correct the applicant's Omang gender marker, citing constitutional rights to dignity and privacy (ESCR-Net 2019), demonstrating judicial oversight of administrative decisions.

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

The National Registration Act defines the primary purpose of the Omang system as providing official ID for citizens, but does not comprehensively address all current and potential uses in the digital ecosystem (Government of Botswana 1993a). The prevention of mission creep is primarily addressed through principles in the Data Protection Act 2024, particularly purpose limitation and data minimisation (TechHive Advisory 2024).

Purpose limitation still requires that personal data be collected for specific, explicit aims and not later repurposed incompatibly; and data minimisation demands that only the data strictly necessary for those aims be gathered. However, consent is not the operative legal basis for Omang.

Botswana's Data Protection Act 2024 therefore grounds Omang processing in 'compliance with a legal obligation' and 'performance of a task carried out in the public interest' rather than in 'freely given' consent. Authoritative commentary notes that in such circumstances consent is not required where processing is authorised by written law (DLA Piper 2025). In short, the mandatory nature of Omang, coupled with the denial of essential entitlements absent the card, renders meaningful consent largely theoretical.

Early signs of mission creep are evident. When Parliament created Omang in 1986 its sole purpose was to record citizenship and provide a domestic identity credential, but the card and its biometric database now power functions beyond that founding mandate. They serve as a cross-border travel document with Namibia (Fragomen 2023), as a compulsory know your customer key for SIM card registration, as the biometric token for e-passport enrolment (Ndlovu 2024b), and as polling station voter verification (Embassy of the Republic of Botswana, Brussels 2024). Most recently, the Gaborone City Council has linked a city-wide facial recognition CCTV network to the Omang database for real-time public security surveillance (Ndlovu 2024a). Each step repurposes data gathered for civil registration into successively wider activities, spanning international mobility, private sector service gating (requiring specific credentials to access services), and surveillance.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

Botswana's constitution guarantees the right to privacy (ILO 2025), requiring derogations to be justified as necessary and proportionate in a democratic society. The digital-ID system heavily relies on collecting biometric data, including fingerprints and facial recognition, as core ID components (Ndlovu 2024b). The Data Protection Act 2024 acknowledges such information's sensitivity by classifying biometric data used for unique ID as sensitive personal data (DLA Piper 2025).

A key proportionality question is whether extensive biometric data collection is truly the least-intrusive option, given that biometrics are (1) irrevocable if leaked, (2) prone to 'false rejects' that can lock legitimate users out of services, and (3) highly attractive to hackers because they enable identity theft at scale (Ndlovu 2024b; Privacy International 2023).

For Botswana's system to meet the data protection standards established by the Data Protection Act 2024, the government must demonstrate that current biometric data collection practices are strictly necessary for legitimate aims, that less intrusive alternatives have been considered, and that benefits outweigh inherent privacy risks. Independent oversight and public discourse play vital roles in ensuring privacy intrusions remain proportionate to legitimate state interests.

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

Data minimisation – collecting and retaining only necessary personal data for specific purposes – is another crucial rights-based consideration. Botswana's National Registration Act mandates collecting specific personal details, including name, residence, sex, date of birth, and marital status (Government of Botswana 1993a). The system also involves collecting biometric data such as fingerprints and facial images (Ndlovu 2024b). Additionally, mandatory SIM card registration requires personal data collection by mobile network operators.

The Data Protection Act 2024 explicitly incorporates storage limitation principles, requiring personal data retention only as necessary to fulfil collection purposes (TechHive Advisory 2024). While this principle is legally established, the act leaves retention schedules to future regulations, none of which have been issued to date. Oversight is vested in the IDPC, which may conduct on-site inspections, order audits, and impose fines of up to 1 million pula for excessive retention (TechHive Advisory, 2024; DLA Piper 2025).

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

For government entities, the National Registration Act permits authorised access to the national register by specific departments (listed in Section 15.2 as the Botswana Police Service, Department of Immigration and Citizenship, Department of Surveys and Lands and the Independent Electoral Commission) (Government of Botswana 1993a).

The Data Protection Act 2024 further governs personal data processing and disclosure by data controllers, including government agencies involved in the digital-ID system (TechHive Advisory 2024).

Private entities such as mobile network operators collect personal data for SIM card registration (Ndlovu 2024b). Specific rules governing their access and potential sharing with the national ID system require clarification. The multi-biometric platform upgrade aims to integrate identification operations across government ministries (Paradigm Initiative 2021), inherently involving database linking. While this integration may increase efficiency, it necessitates robust access control mechanisms.

The Data Protection Act 2024 mandates appropriate technical and organisational measures for personal data security (Michalsons 2024). However, specific details about measures preventing unauthorised sharing across databases are not provided. A draft National Interoperability Framework is under development, with European Union technical support, but it has not yet been gazetted, so no binding cross-agency data-sharing standard is currently in force.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Reports indicate a digital divide in Botswana, characterised by unequal access to digital skills and affordable internet connectivity (Paradigm Initiative 2021). The availability of alternative identification methods for those lacking digital access is not explicitly detailed. Botswana law makes Omang the default proof of identity: the National Registration Act obliges citizens to present their Omang card for voting, land allocation, social assistance applications, and most civil service interactions, and there is no statutory duty on agencies to accept alternative documents (Government of Botswana 1993a).

Although specific documented cases of individuals being denied benefits due to digital-ID failures in Botswana were not identified, experiences from other African nations that have implemented similar systems highlight exclusion risks for undocumented individuals and marginalised communities (Mutung'u 2025).

Botswana's digital divide presents a potential exclusion risk if digital-ID becomes the primary means of accessing essential services. Ensuring accessible alternatives and addressing underlying digital literacy and connectivity issues is crucial to mitigating exclusion risks, particularly for vulnerable populations.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

The National Registration Act mandates that all citizens aged 16 and over must register for a national identity card (Government of Botswana 1993a). The Omang card is legally required for every citizen of Botswana over 16, underscoring the mandatory nature of enrolment (Embassy of the Republic of Botswana, Washington, DC 2025). The act does not provide a blanket 'opt-out.' Section 6.3 excuses a person only when 'prevented by sickness, absence from Botswana or other sufficient cause approved by the Registrar', and the exemption lapses once that cause ends; anyone who wilfully refuses to enrol commits an offence punishable by a fine or imprisonment (Government of Botswana 1993a).

The justification for mandatory enrolment likely centres on establishing a functional national ID system for verifying citizenship, facilitating government service access, and enhancing security. However, as digital-

ID reliance expands to encompass more services, careful evaluation of potential impacts becomes crucial, ensuring those facing genuine enrolment or usage barriers are not unduly disadvantaged.

While initial mandatory registration for basic ID might be justified, making digital-ID compulsory for accessing a wide range of services necessitates thorough assessment of whether alternative identification and service access means are adequately provided for those facing digital exclusion or other legitimate challenges.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

Botswana's approach to risk assessment in its digital-ID system has evolved with the implementation of the Data Protection Act 2024. This legislation, effective from 14 January 2025, establishes core principles for data processing including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability (TechHive Advisory 2024; MISA 2025).

Formal risk assessment mechanisms were limited prior to the DPA 2024, which now mandates data protection impact assessments (DPIAs) for processing activities likely to cause high risk to individuals' rights and freedoms (IT Law Co 2024). The IDPC serves as the designated oversight authority (Botswana Laws n.d.).

Several categories of risk have been identified in relation to Botswana's Omang system.

Privacy considerations: The centralised storage of biometric data presents significant security challenges due to the permanent nature of biometric identifiers (Ndlovu 2024b). Documentation of incidents involving electronic device confiscation and CCTV footage requests has raised surveillance concerns (Ndlovu 2024a). The Data Protection Act 2024 contains exemptions for state processing related to national security that could potentially undermine privacy protections (Data Law Africa n.d.). The integration of Omang data with SIM card registration systems creates additional data-processing linkages that increase privacy risks (Ndlovu 2024b).

Access barriers: Research indicates the transition towards electronic ID systems may present additional barriers for those with limited digital access or literacy. World Bank (2015) documents challenges in Omang enrolment for persons in remote areas, those with disabilities, and individuals lacking prerequisite documentation.

Administrative gaps: Cases involving transgender individuals encountering difficulties with ID documentation have been documented. Despite court rulings establishing rights to gender marker changes on Omang cards (ESCR-Net 2019), the absence of standardised administrative procedures has necessitated judicial intervention (Fortuin 2023).

While the Data Protection Act 2024 represents a significant advancement in establishing formal risk assessment mechanisms, effectiveness depends on implementation factors, particularly the institutional capacity, resources, and independence of the IDPC (Ndlovu 2024b).

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

The Data Protection Act 2024 has implemented a risk-based regulatory framework that applies varying levels of oversight to different data-processing activities based on risk classification.

While the act does not explicitly categorise uses as 'harmful' or 'not harmful' per se, it establishes clear prohibitions and stricter requirements for higher-risk activities. Processing sensitive personal data (including racial origin, political opinions, health, biometrics used for unique ID, genetics, etc.) is generally prohibited unless specific, narrow conditions are met, such as explicit consent, necessity for employment law, vital interests, legal claims, substantial public interest authorised by law, or specific health/research purposes with safeguards (MISA 2025).

A key risk-based element is the statutory requirement for DPIAs before initiating high-risk processing activities (IT Law Co 2024). This explicitly links regulatory scrutiny to the assessed level of risk. The act is grounded in principles such as purpose limitation and data minimisation, requiring data collection and processing to be necessary for specified, legitimate purposes (TechHive Advisory 2024).

The effectiveness of this differentiated approach depends significantly on the IDPC's capacity to develop consistent interpretations of 'high-risk' conduct thorough DPIA reviews, and enforce conditions for sensitive data processing. A significant challenge is the broad exemption for state processing related to national security or public interest (Data Law Africa n.d.), which could potentially allow high-risk state activities to bypass standard risk assessment requirements, creating an inconsistency in the risk-based framework.

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

Proportionality analysis examines whether measures infringing on rights are necessary, suitable, and represent the least intrusive means to achieve

legitimate objectives. Analysis of Botswana's digital-ID system requires consideration of both potential harms and stated justifications.

The potential harms associated with the Omang system range in severity. Compromised biometric data poses particularly serious harm due to its immutable nature (Ndlovu 2024b). Discrimination leading to exclusion from essential services also has highly negative impacts, as documented in cases where inconsistencies between gender identity and official documentation have resulted in difficulties accessing services (Fortuin 2023).

The Data Protection Act 2024 incorporates principles addressing proportionality, including data minimisation, purpose limitation, and storage limitation (TechHive Advisory 2024). It mandates 'appropriate technical and organisational security measures' tailored to the risks involved (Data Law Africa n.d.). The requirement for DPIAs for high-risk processing is another measure intended to ensure proportionality by forcing an assessment of necessity and impact before deployment.

However, questions remain about whether collecting biometric data from the entire citizenry is truly proportionate to stated goals such as preventing duplicates or fighting crime (Ndlovu 2024b). While the Data Protection Act 2024 introduces 'data protection by design and by default' requirements (DataGuidance 2025), research indicates limited implementation of alternative technical approaches such as tokenisation or decentralised identity architectures (SAIIA 2023).

The justifications for the Omang system include preventing identity fraud, enhancing national security, enabling efficient access to government services, promoting financial inclusion, and potentially boosting tax revenue (Ndlovu 2024b). However, a transparent assessment demonstrating that benefits outweigh risks to fundamental rights appears to be lacking, hindering public debate regarding the system's true proportionality.

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

The Data Protection Act 2024 establishes formal mechanisms to address risks associated with digital-ID systems through both preventive and remedial measures.

The legislation restricts high-risk processing activities through specific prohibitions. Processing of sensitive personal data is prohibited outside

narrowly defined conditions (MISA 2025). Transborder data transfers are restricted based on adequacy determinations or specific safeguards (TechHive Advisory 2024). The IDPC possesses corrective powers, including the ability to impose limitations or bans on processing, and to order data erasure (DLA Piper 2025).

A significant preventive measure is the mandate for 'Data protection by design and by default' (DataGuidance 2025). This legally requires data controllers, including government entities managing Omang, to embed data protection principles such as data minimisation and security measures into systems from the design phase.

For addressing materialised risks, the Data Protection Act 2024 establishes clear breach response protocols. Data controllers must notify the IDPC of a personal data breach within 72 hours unless the breach is unlikely to risk individuals' rights (MISA 2025). If the breach poses a high risk, affected data subjects must also be notified without undue delay. Data controllers must maintain internal records of all breaches (DLA Piper 2025).

Regarding redress, data subjects have the right to lodge complaints with the IDPC and seek compensation through the courts for damages resulting from unlawful processing (Botswana Laws n.d.). An Appeals Tribunal provides a mechanism for appealing IDPC decisions (Botswana Laws 2024).

However, the framework faces challenges in addressing irreversible harms, particularly compromised unique biometric data. While compensation is available, it may be insufficient to remedy lifelong risks associated with stolen biometric identifiers (Ndlovu 2024b). The Data Protection Act 2024 does not offer specific mitigation strategies tailored to this unique type of harm beyond preventive measures and standard post-breach responses.

The adequacy of all response mechanisms ultimately relies on robust, independent oversight and enforcement by the IDPC and the judicial system. Institutional capacity and independence are critical factors determining the real-world effectiveness of the legal framework's risk response capabilities.

6. Conclusion

This research set out to assess Botswana's digital-ID system against established rule of law, rights-based, and risk-based tests, examining how effectively it balances security considerations with citizens' rights. Our analysis reveals a system in transition, with significant legislative progress but persistent implementation challenges that require attention to ensure equitable service to all citizens.

Botswana's journey from manual identification to using biometric digital-IDs represents a pioneering effort within the Southern African Development Community. The Omang system has evolved from a simple paper-based credential in 1988 to a sophisticated biometric platform, incorporating facial recognition alongside fingerprint identification, reflecting Botswana's commitment to modernising public administration and aligning with global technological trends.

Our rule of law assessment finds that while the National Registration Act of 1986 provides the foundational legal mandate for the Omang system, it pre-dates modern digital-ID complexities. The Data Protection Act 2024 significantly strengthens the legal framework by establishing comprehensive data protection principles and creating an oversight authority. However, broad security exemptions and the lack of explicit restrictions on private sector ID requirements are concerning. The High Court's intervention in cases such as *ND v Attorney-General* demonstrates judicial willingness to safeguard individual rights, but reliance on case-by-case judicial intervention rather than systematic administrative processes places undue burdens on marginalised individuals.

Rights-based analysis reveals several challenges. The proportionality of extensive biometric data collection is questionable, especially given the permanent nature of biometric identifiers. While data minimisation principles now exist in law, practical implementation through specific retention schedules has yet to materialise. Access control mechanisms lack clarity, particularly regarding cross-agency data sharing. The mandatory nature of the Omang card, combined with its centrality to accessing essential services, poses risks of exclusion for those facing barriers to enrolment.

Our risk-based assessment finds that the Data Protection Act 2024 introduces formal tools, most notably the obligation to run DPIAs for any high-risk processing, but these mechanisms alone are not sufficient to guarantee effective risk governance. The act's safeguards remain largely on paper: enforcement has already been postponed three times because

the IDPC still lacks the readiness needed to review DPIAs or police breaches (Cybersmart Botswana 2024). Although the 2024 act mandates that the commission operate with complete independence, analysts note that this independence is still being operationalised and the regulator's institutional framework is only now taking shape (Mulindwa 2025).

While overall internet penetration has reached 81.4 per cent, significant disparities exist between urban and rural areas in terms of connectivity, affordability, and digital literacy, risking exacerbating existing inequalities as service access becomes increasingly tied to digital-ID. Based on these findings, we recommend focusing on several priority areas to strengthen Botswana's digital-ID governance:

1. **Enhanced independent oversight:** Ensure the IDPC has sufficient resources, expertise, and independence to effectively monitor compliance across all sectors.
2. **Narrowed security exemptions:** Amend the broad exemptions for state processing to include enhanced oversight mechanisms, ensuring proportionality principles still apply.
3. **Accessible administrative procedures:** Develop standardised procedures for addressing common ID-related challenges, particularly gender marker changes, reducing reliance on judicial interventions.
4. **Comprehensive proportionality assessments:** Conduct and publish assessments that transparently weigh the benefits of biometric collection against fundamental rights impacts.
5. **Digital literacy initiatives:** Implement programmes to improve digital literacy among vulnerable populations, coordinated with the rollout of enhanced digital-ID services.
6. **Retention schedule development:** Prioritise the creation of data retention schedules as mandated by the Data Protection Act 2024's storage limitation principle.
7. **Finalisation of the National Interoperability Framework:** Complete and implement the draft framework, with robust privacy safeguards to govern cross-agency data sharing.

Future research should explore implementation challenges the IDPC faces, document the experiences of marginalised communities interacting with the digital-ID system, and evaluate alternative approaches to biometric ID.

By addressing these recommendations, Botswana can build on its legislative progress to create a digital-ID system that balances security imperatives with fundamental rights protection, supporting inclusive

digital transformation while ensuring no citizen is left behind. The country has an opportunity to establish a model for rights-respecting digital-ID governance in the region, requiring sustained commitment to both technical excellence and human rights principles.

7. Bibliography

African Declaration on Internet Rights and Freedoms (2024) '***SADC's Rocky Path: The Challenges of Biometric and Digital Identity Systems***', *Digital Rights Southern Africa* 3, April (accessed 18 October 2025)

Ansar, S. and Clark, J. (2025) ***The Importance of ID Access in Three Charts: Insights from Sub-Saharan Africa***, Digital Transformation blog, World Bank, 9 September (accessed 18 October 2025)

BOCRA (2025) ***Electronic Evidence***, Botswana Communications Regulatory Authority (accessed 18 October 2025)

BOCRA (2022) ***Annual Report 2022***, Botswana Communications Regulatory Authority (accessed 18 October 2025)

Bolt, J. and Hillbom, E. (2013) ***Social Structures, Standards of Living, and Income Distribution in Colonial Bechuanaland Protectorate***, Morton Jerven (accessed 18 October 2025)

Booi, L. (2006) ***Botswana's Legal System and Legal Research***, NYU Law Global (accessed 18 October 2025)

Botswana Laws (n.d.) ***Chapter 42:17 – Data Protection*** (accessed 18 October 2025)

Botswana Laws (2024) ***Act 18 of 2024 – Data Protection Act*** (accessed 12 November 2025)

Botswana Laws (2018) ***Data Protection Act, No. 32 of 2018*** (accessed 18 October 2025)

Cybersmart Botswana (2024) ***Enforcement of the Data Protection Act Has Been Postponed Once Again***, LinkedIn post (accessed 18 October 2025)

Daily News (2024) ***Digital Divide Between Urban and Rural Areas Proof of Inequality*** (accessed 12 November 2025)

DataGuidance (2025) ***Botswana: Salient Features of the Botswana Data Protection Act***, 28 March (accessed 18 October 2025)

Data Law Africa (n.d.) ***Botswana*** (accessed 18 October 2025)

DataReportal (2025) ***Digital 2025: Botswana*** (accessed 18 October 2025)

Delegation of the European Union to Botswana and SADC (2025) ***European Union and Botswana Partner on Digital Transformation***, 5 May (accessed 18 October 2025)

DLA Piper (2025) ***Data Protection Laws in Botswana*** (accessed 18 October 2025)

Embassy of the Republic of Botswana, Brussels (2024) ***Notice of Date for the External Voting for the 2024 General Elections*** (accessed 12 November 2025)

Embassy of the Republic of Botswana, Washington, DC (2025) ***National Identity Card (Omang)*** (accessed 18 October 2025)

ESCR-Net (2019) ***ND v Attorney-General of Botswana and Others – Case Summary*** (accessed 18 October 2025)

EU Digital Transformation Project (2023) *EU Support to Digital Transformation in Botswana*, Project Factsheet, European Union

European Commission Directorate-General for International Partnerships (n.d.) ***Botswana*** (accessed 18 October 2025)

Expertise France (2022) ***EU Support to Digital Transformation in Botswana*** (accessed 18 October 2025)

Fortuin, B. (2023) ***Legal Gender Recognition: An Unexplained Delay by the Botswana Government High Court in 2017 Ruled on the Issue***, Southern Africa Litigation Centre , 19 June (accessed 18 October 2025)

Fragomen (2023) ***Botswana/Namibia: Use of National Identity Cards for Cross-Border Travel***, 22 February (accessed 18 October 2025)

Governance4ID (2025) ***Why Good Governance of Digital ID Matters*** (accessed 18 October 2025)

Government of Botswana (2025a) ***National Identity Card Application*** (accessed 18 October 2025)

Government of Botswana (2025b) ***Provision of Redress Against Administrative Decisions of Public Functionaries*** (accessed 18 October 2025)

Government of Botswana (2025c) ***Shared Digital Services*** (accessed 18 October 2025)

Government of Botswana (1993a) ***Botswana National Registration Act 1986 Consolidated 1993***, Citizenship Rights in Africa Initiative (accessed 18 October 2025)

Government of Botswana (1993b) ***National Registration (Amendment) Act, 1993, No. 17 of 1993*** (accessed 18 October 2025)

IDEMIA (2017) ***Government of Botswana Selects Morpho South Africa to Provide a Single Multi-Biometric Platform for All the Identification Requirements of Various Government Departments***, 2 February (accessed 18 October 2025)

IDRC (2025) ***Management of Research and Innovation Funds by Botswana***, International Development Research Centre (accessed 18 October 2025)

ILO (2025) ***Constitution of Botswana 1966***, International Labour Organization (accessed 18 October 2025)

IT Law Co (2024) ***Data Protection Act 18 of 2024 – Botswana*** (accessed 18 October 2025)

MacDonald, A. (2024) ***Report Points Out Personal Data Protection Lapses in Botswana***, BiometricUpdate.com, 8 July (accessed 18 October 2025)

Masendu, N. (2024) '**Botswana's Digital Divide: Unveiling Disparities in Internet Access**', *Mmegi Online*, 26 April (accessed 18 October 2025)

McConvey, J.R. (2023) ***Botswana and Namibia Select Veridos Technology for Cross-Border Digital ID***, BiometricUpdate.com, 24 May (accessed 18 October 2025)

Michalsons (2024) ***Botswana's Data Protection Act Comes into Effect*** (accessed 18 October 2025)

Minority Rights Group (2018) ***Securing Recognition of Minorities and Marginalised People and Their Rights in Botswana*** (accessed 18 October 2025)

MISA (2025) ***New Botswana Data Protection Act Progressive Step to a More Secure Digital Environment***, Media Institute of Southern Africa, 17 January (accessed 18 October 2025)

Mulindwa, C. (2025) ***Understanding Botswana's 2018 and 2024 Data Protection Acts***, Centre for Intellectual Property and Information Technology Law, 26 March (accessed 18 October 2025)

Ndlovu, T. (2024a) ***Botswana Showcases E-Government's Privacy Pitfalls***, Association for Progressive Communications, 28 February (accessed 18 October 2025)

Ndlovu, T. (2024b) ***Essential Reforms Needed to Elevate Biometric Data Protection: Botswana's Biometric Data Security Challenges and Urgent Calls for Legal Reforms***, Association for Progressive Communications, 5 July (accessed 18 October 2025)

Nkwe, N. (2012) '**E-Government: Challenges and Opportunities in Botswana**', *International Journal of Humanities and Social Science*, 2.17 (accessed 18 October 2025)

Mutung'u, G. (2025) ***Digital ID: From Governance by Technology to Governance of Technologies***, OpenGlobalRights, 6 February (accessed 18 October 2025)

Paradigm Initiative (2021) ***Londa – Digital Rights and Inclusion in Botswana*** , 17 May (accessed 18 October 2025)

Parsons, N. (2019) ***A Brief History of Botswana*** (accessed 18 October 2025)

Poloko, J.D. (2017) '**Botswana Strategy for the Development of Statistics (BSDS), Civil Registration and Vital Statistics (CRVS): 2016 Progress Report**', presentation, 17 March, Fairgrounds Holdings, Ministry of Nationality, Immigration & Gender Affairs (accessed 18 October 2025)

Privacy International (2023) *A Primer on the Risks of Biometrics*

SAIIA (2023) ***Digital Identification and Biometrics in East Africa: Opportunities and Concerns***, Policy Brief, South African Institute of International Affairs (accessed 18 October 2025)

SmartBots (2021) *Expression of Interest for the Design, Supply, Installation, Commissioning, Operation and Support of Internet and Backhaul Connectivity to Facilities in 61 Villages*

Statistics Botswana (2023) ***Population and Housing Census 2022: Key Demographic and Socio-Economic Indicators*** (accessed 18 October 2025)

TechHive Advisory (2024) ***Understanding Botswana's New Data Protection Act: Key Updates and Changes*** (accessed 18 October 2025)

van Rooyen, G. (1999) '**Botswana ID Cards Take On a New Face**', *Smart Security Solutions*, April (accessed 18 October 2025)

World Bank (2019) *ID4D Practitioner's Guide: Version 1.0,* Washington, DC: World Bank Group

World Bank (2015) ***ID4D Country Diagnostic: Botswana***, Washington, DC: World Bank Group (accessed 18 October 2025)

Digital-ID in Côte d'Ivoire: Country report

Grace Mutung'u

 DOI: 10.19088/IDS.2025.064

1. Introduction

Côte d'Ivoire is among West Africa's largest economies. While the country is well known as a global cocoa and cashew nut producer, on the digital front it also has a vibrant start-up industry, with notable ventures in financial technology and e-commerce (StartupBlink 2025). The administration considers digital identification (digital-ID) the foundation of an inclusive digital economy.

Côte d'Ivoire has a complex history of identification of persons that dates back to the colonial era. The country has historically hosted migrants, including foreign labourers and refugees. In the 1990s, however, politicisation of identity became a basis for exclusion and marginalisation. In the past decade, the country has been digitalising its national ID system to enhance governance, financial inclusion, and service delivery. Digital-ID is now linked to many services and is mandatory for access to health care, banking, passports, and voting in elections. Some of the reasons for public service digitalisation include to reduce fraud; for example, by identifying 'ghost workers' and fraudulent beneficiaries of social welfare (Sid'Ahmed and Morisset 2017).

Studies on the digital-ID system show there are many barriers to access, particularly for low-income earners. There is reason to believe that these patterns of (dis)advantage are being reproduced by digital-ID systems that exclude people from accessing government services, banking, food entitlements, and other human rights. While the *Carte nationale d'identité* (National Identity Card, CNI) project promises economic and governance benefits, its success hinges on addressing infrastructure gaps, ensuring inclusivity, and safeguarding privacy.

This paper analyses the current state of digital-ID using the Centre for Internet and Society (CIS) framework (CIS 2021). It assesses the legitimacy of use and governance of digital-ID in Côte d'Ivoire through three checks: rule of law, rights-based, and risk-based tests. The paper begins with a brief history of ID in Côte d'Ivoire, followed by a general overview of its digital-ID system. The discussion then delves into analysis of the law and policies around digital-ID in Côte d'Ivoire using the three tests.

2. History of ID in Côte d'Ivoire

2.1 Colonial foundations (1893–1960)

The history of written ID in Côte d'Ivoire dates back to the colonial era when the French introduced various documentation systems for their colonies in West Africa (CRAI n.d.). Although the French approached their colonies in West Africa as a union (Cooper 2014), the systems were segregated along lines of ethnicity, race, and nationality. Under an administrative scheme known as the *indigénat*, the French created a layered system that differentiated between French citizens and African subjects (Mann 2009). The *indigénat* registration system that was introduced in the French West Africa region from 1904, registered people in the colonies in a hierarchy according to their proximity to French citizenship. Settlers who had come from France were registered as French nationals with full citizenship rights in French West Africa, while those from other territories were considered nationals without citizenship. Africans were considered subjects, with only a few Africans who passed tests on assimilation to French civilisation being considered nationals without citizenship.

Another system introduced by the French from 1908 was the *Livret d'identité* or passbook. Passbooks were issued to African colonial subjects and were mandatory for travel, employment, and taxation purposes. While passes were initially issued to Ivorian males, the French mitigated shortages of labourers by extending this system to African males who came to work on colonial estates from other territories such as Upper Volta (present-day Burkina Faso).

The colonial concepts of identity, nationality, and belonging influence current constructs in relation to identification of persons. Banégas and Cutulo (2023) demonstrate how political and bureaucratic attitudes have denied ID documentation to people in the rural (Voltaic) villages as they are not considered to be indigenous Ivorians.

2.2 Post-independence period (1960–90s)

Post-independence, Côte d'Ivoire adopted a national registration system known as the CNI in 1962. This was a paper identity card where individuals were manually registered. Although uptake of the card was hindered by state incapacity, particularly in rural areas, the card still serves as the official proof of identity for citizens (World Bank 2016).

In the 1990s, identification was highly politicised in national debates over *Ivoirité* (Ivorian identity). Côte d'Ivoire had experienced a

surge in migration particularly from Burkina Faso, Mali, and later southern Nigeria during the civil war in that country. *Ivoirité* sought to exclude migrants from obtaining nationality, which fuelled ethnic conflict in the 1990s–2000s (US Department of State 2018).

2.3 Digital-ID

Côte d'Ivoire has 12.8 million internet users, who make up about 45 per cent of the population (DataReportal 2025). The country had an estimated 46.4 million active mobile cellular connections, and 7.55 million social media users in early 2025 (*ibid.*). The high number of active mobile (cell) phone connections could be explained by people having more than one SIM card. This is common practice in African countries, where people buy multiple SIM cards in pursuit of offers from various mobile network operators (GSMA 2014).

In the past decade or so, Côte d'Ivoire has been digitalising its registration system. The CNI has transitioned to biometric digital-ID with fingerprints and facial images. The legal basis for the biometric CNI is the 2017 Digital Code (Côte d'Ivoire 2017b), and the 2019 digital-ID law (Loi No. 2019-566 du 26 juin 2019 instituant une carte d'identité nationale biométrique, Côte d'Ivoire 2019a). A form of foundational ID, such as a birth certificate, proof of residency, and family book (*Livret de famille*) is required for CNI registration (ONECI n.d). During registration, biometrics collected include fingerprints, facial photograph, and iris scans (Banégas and Cutolo 2024).

The current digital-ID programme was launched in 2023. It is under the oversight of the Ministry of Interior and Security and implemented by the National Office of Civil Status and Identification (Office National de l'Etat Civil et de l'Identification, ONECI) with the support of the Ministry of Digital Transformation. Besides these public agencies, private businesses also play important roles in the digital-ID project. Notable foreign private companies include Idemia, which provided the biometric technology, Semlex, the current project operator, and Orange Côte d'Ivoire, a mobile network operator, which has partnered with the government for mobile registration. The project has also received support from the international development community. The World Bank has provided funding to the tune of US$100 million and the European Union (EU) has provided technical assistance (World Bank 2024; European Commission n.d.).

By 2024, about 8 million citizens (30 per cent of the population) had been registered (MacDonald 2024). The challenges to digital-ID registration include limited registration centres in rural areas, and barriers to accessibility for elderly and disabled persons (ADRH 2021).

However, the biggest barrier is statelessness, where strict citizenship requirements exclude migrants and other minorities from registration.

2.4 Drivers of digital-ID adoption

There are internal as well as external drivers of digital-ID adoption. Internal drivers include local policies on digital transformation for development such as the national digital transformation plan (Stratégie nationale de développement du numérique en Côte d'Ivoire SNNCI 2021–2025, Côte d'Ivoire 2022), and the E-Government Strengthening Support Project (Projet d'Appui au Renforcement de l'Administration Electronique, PARAE), which aims to modernise government services through digitalisation (ADB 2023). The national vision, Côte d'Ivoire Solidaire, which was launched by President Alassane Ouattara in 2018, identified digitisation as a lever for economic growth and social transformation. The plan envisions digital-ID as a means of reducing electoral fraud and streamlining welfare programmes such as social cash transfers (Diakalidia 2019).

External drivers include private sector and international development partners' goals on financial inclusion and migration management. Private sector entities such as mobile money networks view digital-ID as a lever for credit services and financial inclusion (Meagher 2017). The government has also engaged various private foreign companies to roll out different aspects of the system under public–private partnerships. For example, in 2021 the government agency in charge of digital-ID partnered with Belgian firm Semlex to build the digital-ID database (Semlex 2022). Prior to that, another Belgian company, Zetes, had been issuing functional biometric cards such as for national health insurance, and biometric passports (Identity Week 2015). Zetes won a seven-year contract to produce biometric cards in 2015 (Mayhew 2015).

Other external influences for digital-ID include global programmes such as the World Bank's Identification for Development (ID4D) Initiative which aims to solve the global gap in identification of persons by supporting governments to increase digital-ID coverage (World Bank 2016). Inspired by the Sustainable Development Goals, ID4D promotes digital-ID as a means to count every person on the planet (Desai *et al*. 2018). The EU's Joint Valletta Action Plan is another influence. The plan aims to manage the migration of Africans to Europe by increasing knowledge about potential migrants through biometric ID (European Union 2015). For example, a system known as the Migration Information and Data Analysis System (MIDAS), which is managed by the International Organization for Migration collects travellers' biometric data in several West African countries including Côte d'Ivoire. The data is used to manage migration,

study migration patterns, and also screen out individuals suspected of irregular migration (IOM 2019). Iwuoha (2025) posits that the system externalises European border control by profiling travellers while they are still in African countries. Notably, the MIDAS infrastructure is based on national biometric ID programmes, since data collected is related to government-issued documents such as CNIs and biometric passports.

Regional integration in the Economic Community of West African States (ECOWAS) is another driver of digital-ID adoption. The community launched the ECOWAS National Biometric Identity Card (ENBIC) in 2014 to facilitate trade and free movement of people within the region (MacDonald 2024). Côte d'Ivoire has access to ENBIC and the West Africa Unique Identification for Regional Integration and Inclusion (WURI) programme (World Bank 2024b). Among ENBIC's stated goals is to make it easier to establish people's identity and therefore process applications for regular migration, residence, and establishment of ECOWAS citizens within the bloc (MacDonald 2024). ENBIC, which is coordinated by the member states' immigration authorities, would therefore help to conclusively identify citizens and curb problems such as human trafficking, irregular migration, and border insecurity (*ibid.*).

2.5 Risks

There are technical as well as political risks with the CNI. According to CIPESA (2022), the digital-ID system in Côte d'Ivoire was developed with limited public participation, thereby failing to factor in important human rights issues such as the risk of exclusion and discrimination. In addition, although Côte d'Ivoire has a data protection law – Law No. 2013-450 dated June 19, 2013 on the Protection of Personal Data (Côte d'Ivoire 2013b) – CIPESA posits that CNI did not incorporate privacy by design. As such, privacy considerations, including data protection, transparency and accountability, and public awareness were not built into the system but added afterwards. Even so, they have not been fully incorporated into the system. The group calls for greater participatory design that responds to the needs of vulnerable communities, such as those in rural and underserved areas, and data privacy. This would ensure that people can access services on one hand, and also that their access to those services does not unnecessarily expose their data.

Such risks are exacerbated by the history of Côte d'Ivoire's politicisation of identity and ethnic conflict. This puts marginalised groups at risk of being excluded from the CNI and connected services. With a history of political tensions such as those witnessed in the 2020 elections, there is also concern that the system could be used to profile and target political opponents and groups. The biometric digital-ID is linked to public services

such as elections and health insurance; it is also required for private services such as SIM card registration and banking (MacDonald 2021).

Côte d'Ivoire's digital-ID system reflects both the legacy of colonial control and the potential for equitable modernisation. While the CNI project promises economic and governance benefits, its success hinges on addressing infrastructure gaps, ensuring inclusivity, and safeguarding privacy (ADRH 2021; Access Now 2024). Without resolving systemic issues, Côte d'Ivoire's biometric digital-ID risks becoming another tool of exclusion in a nation still healing from identity-based conflicts.

3. Rule of law tests

3.1 Legislative mandate

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Côte d'Ivoire's digital-ID project is based on a national digital transformation plan (Côte d'Ivoire 2022) and backed by the Law on Digital Identification (Law No. 2019-566) (Côte d'Ivoire 2019a), an executive decree based on Decree No. 2019-458 (Côte d'Ivoire 2019b), as well as the data protection law, Law No. 2013-450 on the Protection of Personal Data. The digital-ID law also incorporates the National Register of Persons (Registre National des Personnes Physiques, RNPP) that was developed under a 2018 decree (Decret No. 2018-454 du 09 Mai 2018 relatif au registre national des personnes physiques, Côte d'Ivoire 2018). The Digital Code (Orientation of the Information Society Law No. 2017-803, Côte d'Ivoire 2017b) aspires to modernise the country through digitalisation of government services and identifies digital-ID as among the pillars of digital transformation.

The digital-ID law has five articles that establish the legal basis for the biometric digital-ID, and give the scope of the subjects of the law and the validity period of the biometric ID. Article 2 describes the ID as a secure, multi-application electronic smart card that can be used for several unspecified purposes (Côte d'Ivoire 2019b).

The digital-ID law mandates the Council of Ministers to create a framework for operationalisation of the biometric ID. Article 5 lists the mandate as including: development of the technical specifications of the law, as well as procedural issues such as application for and renewal of the biometric ID, and the transition from the paper to the biometric ID (*ibid.*). The subsequent executive directives provide technical and administrative details for the operation of the digital-ID system.

The law was duly approved by the parliament then assented to by the president in 2019. An associated executive order, Decree No. 2019-458, established ONECI to serve as a dedicated agency for implementing biometric registration of all citizens and residents of Côte d'Ivoire.

While the primary digital-ID law mandates the executive to issue decrees, the delegated authority is excessively broad. For example, it allows executive discretion on important issues such as technical standards for biometrics, data collection procedures, and data-sharing protocols required under the data protection law (Côte d'Ivoire 2013b). It also appears to ratify previous

executive actions on the digital-ID project. For example, the executive launched the RNPP in 2018 to unify civil status data and create a single database of natural persons in the country using digital-ID (ADRH 2021). The unification was supported by a cabinet decision to restructure identity resources and agencies, which had not been captured in the digital-ID law. The implementing agency, ONECI, initiated a public–private partnership with Semlex to collect digital-ID data and build the database (MacDonald 2021).

Another key law governing digital-ID is the law on the protection of personal data (Côte d'Ivoire 2013b). This law provides safeguards for the protection of personal data, which is integral to digital-ID systems. For example, it requires prior authorisation for processing of biometric data by the Regulatory Authority for Telecommunications in Côte d'Ivoire (Autorité de Régulation des Télécommunications de Côte d'Ivoire, ARTCI).

3.2 Legitimate aim

Does the law have a 'legitimate aim'? Are all purposes flowing from the legitimate aim identified in the relevant law?

The Côte d'Ivoire constitution requires that where a law impacts fundamental rights, such as privacy, fundamental principles of that law should be defined (Côte d'Ivoire 2016: Art. 70).

The digital-ID law explicitly states its objectives as creating a national population register for improved governance and service delivery; providing biometric ID to combat fraud and identity theft; and streamlining administrative processes such as elections, social services, and taxation (Côte d'Ivoire 2017).

These objectives align with the aims identified in policy documents. For example, the Digital Code (Côte d'Ivoire 2017b) mentions economic development as being among the objectives for digitalisation. PARAE (AfDB 2023) lists fraud prevention as a rationale for digitalising public services. However, these policies and rationale are not incorporated into the digital-ID law, leaving it to the discretion of the executive to rationalise new use cases for digital-ID.

3.3 Defined actors and purposes

Does the law governing digital-ID clearly define all the actors permitted to access or use the ID data? Does the law define the nature of data that can be collected? Do individuals have the right to access, confirm, and correct their data, and to opt out?

The digital-ID law does not specifically address data sharing. However, the decree establishing a national population register implies but does not clearly specify data-sharing roles for actors such as government ministries and public agencies, as well as private entities, since these actors are required to facilitate access to services (Côte d'Ivoire 2018). The executive decree on digital-ID also designates ONECI as the entity primarily responsible for implementing the national ID system (Côte d'Ivoire 2019b).

Executive discretion resulted in changing the digital-ID project into a public–private partnership when ONECI contracted Semlex to implement the digital-ID (Semlex 2023). As a public–private partnership, the company did not receive money from the government for the project. However, it charged 5,000 CFA francs (US$8.60) per card (Hersey 2019). Ecofin Agency (2019) estimated that the project would cost 460 billion CFA francs (US$790 million) over a ten-year period. Other notable private sector actors include GenKey (Jarrahi 2021) and CIVIPOL (Privacy International 2020).

Notably, these are foreign companies (GenKey is from the Netherlands, and CIVIPOL from France) with the capacity to transfer personal data outside of Côte d'Ivoire, yet the data-sharing and transfer agreements have not been published. While some of Semlex's operations, such as document production, are done in-country (Semlex 2023), it is not clear if all the data is stored within Côte d'Ivoire.

Some of the explicitly stated mandates for the digital-ID system are: issuance of civil status documents such as birth certificates and national IDs; access to public and private services such as banking and health care; electoral processes such as voter registration; and national security functions such as law enforcement and border control (Côte d'Ivoire 2017).

The data protection law prescribes that personal data must be collected, recorded, processed, stored, transmitted, and interconnected in a fair and lawful manner. The law also requires data to be processed for specified purposes, and under the principles of data minimisation, accuracy, storage limitation, and confidentiality. This law is overseen by ARTCI, which consists of a seven-member council appointed by the Council of Ministers for a non-renewable six-year term. These members have security of tenure, and are required to report annually on enforcement of the data protection law to both the president and National Assembly. While these provisions establish ARTCI's independence, the authority's enforcement of the law has mainly focused on private entities and not public agencies.

Neither the data protection law (Côte d'Ivoire 2013b) nor the digital-ID law (Côte d'Ivoire 2019a), explicitly proscribe or limit secondary uses of collected data; for example, for commercial uses or political surveillance.

The lack of explicit purpose limitations in the law allows the government to repurpose ID data for unrelated aims (e.g. political surveillance, social scoring[18]), magnifying privacy risks by using data for purposes beyond what was originally intended. Given that the country has a history of surveillance of human rights defenders and dissidents (AEDH *et al*. 2021), purpose limitation for digital-ID data is paramount for protection of human rights.

The digital-ID law envisages data sharing with public and private entities. Private entities are required to sign data access agreements. However, the lack of a reporting mechanism has resulted in an opaque process and lack of accountability. Decree No. 2019-458 (Côte d'Ivoire 2019b) requires government entities to justify data requests to ONECI, but there are no strict proportionality assessments or public logs of access requests. The digital-ID law does not require public reporting by ONECI on the system. Although the data protection law requires reporting to ARTCI on data breaches and misuse, the authority lacks independence to provide proper oversight of ONECI.

There is no statutory requirement for third-party audits of government agencies' use of the digital-ID system, leaving accountability to internal reviews. Given that many private and public actors are involved in the project, there is need for transparency reports and independent oversight to retain public (and private) trust in the system (Access Now 2024).

3.4 Redress mechanisms

Does the law provide for adequate redress mechanisms against actors who use digital-ID and govern its use?

Three main avenues for redress exist under the digital-ID law, data protection law, and the constitution. None of these frameworks provide for notifying citizens when their data is accessed and used for various functions. Citizens have no way of knowing if or how their data is used, whether it is securely stored, or with whom it is shared and for what purpose.

The data protection law grants individuals the right to access, correct, or delete their personal data held by ONECI or other entities (Côte d'Ivoire 2013b). In terms of due process, the digital-ID law provides for administrative appeals on denial of ID cards. The procedure for appeal is set out in Decree No. 2019-458 (Côte d'Ivoire 2019b). While the law makes provisions for appeal, in practice, many low-income earners and rural populations are unable to pursue appeals because of the costs involved. As reported by ADRH (2021), costs such as transport to public

18 Social scoring is defined under the **EU AI Act** as 'classifying people based on behaviour, socio-economic status or personal characteristics'.

offices and missing out on a day's work deter people from administrative appeals. The UN Refugee Agency (UNHCR) which has been coordinating initiatives to register stateless people also notes that the country has a high number of stateless persons who are low-income earners (UNHCR 2024: 535). To resolve statelessness, the state must undertake deliberate efforts to reach people who face barriers to registration.

Additionally, the data protection law, empowers data subjects to file grievances with the data protection authority, ARTCI (Côte d'Ivoire 2013b). However, there are practical barriers to filing such complaints. ARTCI is under-resourced and therefore lacks sufficient technical capacity to handle complaints effectively. The authority also lacks proper funding to raise public awareness, particularly in rural areas (Bogui and Atochua 2016).

Overall, the digital-ID system appears to prioritise state control over individual and group rights (ADRH 2021). For example, the digital-ID law (Côte d'Ivoire 2019a) does not sufficiently incorporate human rights but instead mandates the creation of a system to collect biometric data. Similarly, the PARAE project elaborates on the infrastructure, software, financing, and management of the project, but is almost silent on protection of individual and group rights. World Bank (2020) points out that the digital-ID project has a weak redress mechanism.

3.5 Accountability

Are there adequate systems for accountability of governing bodies, users of digital-ID, and other actors?

The data protection law makes provision to impose fines of up to 100 million CFA francs, as well as criminal penalties for unauthorised data processing and breaches (Côte d'Ivoire 2013a). The digital-ID law creates crimes related to integrity of the ID system but does not require accountability for service delivery.

There are many issues arising out of mandatory digital-ID from a service delivery perspective. These include inability to enrol, lack of documents, and technical failure (Banégas and Cutulo 2023; ADRH 2021). However, there was no evidence of reported cases of or regulatory action on digital-ID-related violations. Given the high number of cases of citizens excluded from digital-ID, and thereby excluded from accessing banking and government services, and social protection entitlements, it might be expected that there would have been a long queue of people seeking redress. However, it may be that barriers to registration overlap with barriers for redress.

ADRH (2021) research demonstrates the various costs associated with the digital-ID system that exclude low-income earners. These range from the actual cost of the digital-ID itself, which was prohibitively high for most low-income earners and rural dwellers (Banégas and Cutulo 2023; Adjami 2016: 86). In addition, people have to travel to administrative centres to apply for the ID, at times missing 1–2 days' work (ADRH 2021). If these administrative costs were too high for most individuals, it can be inferred that such people could not afford the time and resources to engage with redress mechanisms or litigation.

3.6 Mission creep

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of digital-ID?

The digital-ID law as well as the national digital transformation plan (Côte d'Ivoire 2022) specify broad intended functions of the system to include governance and service delivery; the provision of biometric ID to combat fraud and identity theft; and the streamlining of administrative processes such as elections, social services, and taxation (Côte d'Ivoire 2019). Development finance and technical support from partners such as the EU states that another objective of digital-ID is migration control (European Union 2015; Privacy International 2020). However, this is not captured in Côte d'Ivoire's digital-ID law.

In pursuance of the executive mandate, the government has expanded the digital-ID's use cases to functions such as voting and administration of social services without publicly available assessments of the privacy or equity implications of this expansion (MacDonald 2021). Pilot programmes – for example, biometric voter registration (Idowu 2021) – were implemented without transparent ex ante evaluations of risks such as authentication failures or data misuse.

There has also been progressive application of biometrics for other identification processes such as applying for immigration papers and visas (Identity Week 2017). However, the digital-ID law does not provide an oversight mechanism for dealing with mission creep arising from digital-ID uses. There have also not been any reported cases of administrative or judicial causes regarding mission creep.

4. Rights-based tests

4.1 Necessity and proportionality

Are privacy violations arising from the use of digital-ID necessary and proportionate to achieving a legitimate aim?

The digital-ID law makes it mandatory for all citizens to enrol biometrically, using fingerprints and a facial photograph (Côte d'Ivoire 2019a). The rationale for mandatory biometric enrolment is to reduce fraud (*ibid.*; Diakalidia 2019). An example of such fraud is ghost workers on the government payroll (AfDB 2023). The World Bank estimates that the rollout of a digital personnel and wage management system resulted in weeding out 2,300 records of ghost workers in Côte d'Ivoire (Sid'Ahmed and Morisset 2017).

World Bank (2018) promotes centralised biometric systems as a way of combating fraud in government-to-person transfers, reducing administrative costs, and increasing tax collections. Biometrics are also rationalised as a means of giving governments better control over large systems such as pensions and welfare. Considering the intrusiveness of biometrics, the government has not proved that less invasive methods (e.g. non-biometric IDs with enhanced security features) would fail to achieve the same goals.

4.2 Data minimisation

Are there clear limitations on what data may be collected, how it may be processed, and how long it is retained during the use of digital-ID?

The data protection law establishes clear limitations on data collection, processing, and retention that are applicable to the digital-ID system (Côte d'Ivoire 2013b: Art. 14). Nevertheless, the system collects multiple biometric identifiers and links them to a wide range of services such as health care and banking (World Bank 2016). This exceeds the data minimisation principle, as simpler identifiers could suffice for these purposes.

The data minimisation principle is also abrogated when other laws intersect with the digital-ID law. For example, Decree No. 2017-193 (Côte d'Ivoire 2017a) requires telecoms operators to identify their subscribers through collection and storage of ID data. This data includes a facial photo, date and place of birth, profession, email and physical address, plus a copy of the biometric national identity card, biometric national driving licence or biometric passport. Considering that the decree was enacted prior to the digital-ID law, it could have been expected that the data collected under the later

decree would be minimised, given the broad range of data collected under the digital-ID system. Without data minimisation, a lot of data is collected under the public system as well as the private systems of telecoms operators.

4.3 Access control

Are protections in place to limit access to the digital trail of personally identifiable information created through the use of digital-ID by both state and private actors?

Both the digital-ID law and the data protection law require access controls. The data protection law requires that personal data only be collected for specified, legitimate purposes (Côte d'Ivoire 2013b: Art. 16). The law also requires that data controllers implement technical and organisational measures to protect such data (Art. 34). It imposes fines of up to 100 million CFA francs for unauthorised access or breaches (Art. 22).

However, the data protection law provides broad exemptions for public interest processing such as for digital-ID (Art. 13). There are no principles or procedures for determining what constitutes public interest. In addition, enforcement of the law is weak, particularly where government agencies are concerned (ADRH 2021).

The digital-ID law implies role-based access for different actors such as law enforcement, public agency service providers, and private actors. Decree No. 2019-458 (Côte d'Ivoire 2019b) further outlines protocols for government and private actors. However, there are no reporting mechanisms under the digital-ID law through which the protocols can be scrutinised by the public or parliament.

4.4 Exclusions

Are there adequate mechanisms to ensure that the adoption of digital-ID does not lead to exclusion or restriction of access to entitlements or services?

Côte d'Ivoire has a complex history of politics of nationality where people from particular groups have systematically faced barriers in accessing foundational ID documentation (Cooper 2014). These include colonial and post-colonial era migrants, rural and border populations (Banégas and Cutulo 2023). Digital-ID is based on ID documents such as a birth certificate, proof of residency, and family book (livret de famille), yet the digital-ID law does not specify principles for inclusion (ADRH 2021). Examples of such principles could be waiving the cost of ID for low-income populations, taking ID registration services to underserved people, and allowing access to key services such as emergency health care even without ID.

In addition, the law envisages mandatory ID solely through biometric digital-ID. This excludes people from access to services where there is technology failure, or due to lack of fingers and fingerprints since there are no non-biometric fallbacks. The law does not provide a redress mechanism where a person is unable to access services due to authentication failure.

4.5 Mandatory use

In cases where enrolment and use of digital-ID are made mandatory, are there any valid legal grounds for doing so?

The digital-ID law explicitly states that enrolment is mandatory for all citizens of 16 years and over. In practice, citizens have had to enrol in order to access services such as voter registration and identification, banking, and obtaining a driving licence. The government has also advanced digital-ID use cases (MacDonald 2021). A report by ADRH (2021) also attributes enrolment to the linkage of digital-ID to national health insurance. Beginning in 2014, the government has rolled out a universal health coverage programme whereby citizens and residents can access health-care services. For citizens to be registered for services, they need to first have a national identity card number.

There has also been progressive application of biometrics for other identification processes such as obtaining immigration papers, and visas (Identity Week 2017). Another example of progressive and mandatory application of digital-ID is the issuance of national identity numbers to newborn children. The national identity number serves as a unique personal identifier that is later linked to the children's biometric profiles.

5. Risk-based tests

5.1 Risk assessment

Are decisions regarding the legitimacy of uses, benefits of using digital-ID, and their impact on individual rights informed by risk assessment?

The digital-ID law does not require a risk assessment. While Decree No. 2019-458 (Côte d'Ivoire 2019b) outlines technical and organisational measures such as data-sharing codes, there is no requirement to systematically assess risks in digital-ID data processing.

Another risk arising from digital-ID is privacy harms arising from a centralised database of biometric data. The database is prone to breaches or surveillance (ADRH 2021). The data protection law calls for prior notification to the data protection authority, ARTCI, before implementing data-processing projects such as the digital-ID (Côte d'Ivoire 2013b: Art. 5). However, the law does not mandate risk assessments, even for such high risk projects.

Other risks include exclusion and discrimination. Given the country's historical complexities with citizenship documentation, linking digital-ID to citizenship documents risks excluding undocumented populations (ADRH 2021). There are no risk mitigation measures such as alternatives to biometrics, creating a risk of identification failure due to biometric failure. Biometric failure refers to when a biometric reader fails to identify a person. In national digital-ID systems, a person who has not been biometrically identified is not authorised to receive services.

5.2 Differentiated approach to risks

Do the digital-ID law and regulations envisage a differentiated approach to governing uses of digital-ID, based on the risks it entails?

Current laws and decrees do not adopt a differentiated approach to governing digital-ID usage based on varying risk levels, nor do they include mechanisms to restrict or prohibit high-risk applications.

For example, the digital-ID law does not specify mechanisms for redress for inaccurate data collection, authentication errors, mission creep, or indiscriminate data sharing. However, the Cybercrime Law (Law No. 2013-451) outlaws identity theft or fraud by individuals (Côte d'Ivoire 2013a: Art. 34).

5.3 Proportionality

Does the digital-ID law envisage governance that is proportional to the likelihood and severity of the possible risks of its use?

The digital-ID laws and related policies rationalise mandatory ID for access to services to reducing fraud, increasing efficiency, streamlining access to social protection and government services, increasing security, and growing the economy (World Bank 2018; CIVIPOL n.d.). However, mandatory ID bars people without primary documents required for digital-ID enrolment from receiving services, as well as rural and underserved populations who do not always have access to digital technologies (ADRH 2021).

The digital-ID laws and policies do not assess or mitigate these risks. They do not consider alternative measures for achieving the same goals that would also reduce barriers to accessing services. Examples of alternatives include non-biometric smart cards, devolution of social services to smaller areas where recipients are known to service providers, and non-digital identification methods in rural and underserved areas.

Another aspect that raises proportionality concerns is centralisation of digital-ID data. Some of the risks arising from such centralisation include surveillance, political manipulation, and control of vulnerable populations and political dissidents. World Bank (2016)'s technical analysis promotes digital-ID as a means of modernising citizenship documentation systems. The analysis settles on centralised biometric digital-ID, but does not analyse the viability of alternative models such as federated ID, which avoids central storage.

5.4 Response to risks

In cases of demonstrably high risk from uses of digital-ID, are there mechanisms in place to prohibit or restrict its use? Do the laws and regulations envisage a differentiated approach to governing uses of digital-ID, based on the likelihood and severity of risk?

Besides the digital-ID and data protection laws, the Cybercrime Law creates offences related to information and communication technologies. However, the framework does not specifically focus on the governance of digital-ID systems or the risks they may entail.

The government has responded to some risks – for example, the risk of exclusion – through mass registration campaigns and use of agents to enrol people into the digital-ID system (MacDonald 2021). These responses are in collaboration with partners such as UNHCR and mobile network operator Orange.

On the issue of the cost of the ID, which is a barrier to low-income earners, the state has not conceded to waiving the fee of 5,000 CFA francs for low-income earners. However, it extended validity of older digital-ID cards to June 2020 to facilitate participation in elections (Hersey 2019). The risk mitigation actions taken by the state and partners are not legal requirements, but depend on the government's goodwill.

6. Conclusion

This report set out to evaluate the implementation of biometric digital-ID in Côte d'Ivoire by using the CIS framework of tests, incorporating rule of law, rights-based, and risk-based tests. On applying the tests, this report finds that while Côte d'Ivoire's digital-ID project is supported by legitimately enacted laws, digital-ID uses are disproportionate, and the digital-ID project lacks independent oversight. This is because the law excessively delegates power to the executive and does not have sufficient mechanisms to prevent risks arising from the use of digital systems. The project also lacks sufficient redress mechanisms to resolve rights violations.

The Côte d'Ivoire digital-ID project presents an opportunity to resolve past challenges with citizenship documentation by creating a system that is inclusive of all persons with long-standing citizenship claims, rural populations, and low-income earners. To achieve this objective, the system should exclude barriers such as documentation requirements and strengthen redress mechanisms.

The design of digital-ID as a centralised system collating data from civic and private systems is rationalised as a way of removing fraud and corruption, increasing efficiency, streamlining access to social protection and government services, increasing security, and growing the economy. However, a centralised system presents significant risks to rights in terms of privacy and access to services. To mitigate these risks and protect rights, legislation should include non-biometric fallbacks for identification of persons, particularly for essential services. There must also be guaranteed access to services, and prioritisation of access to services over identification of persons. No person should lack access to health care, education, social welfare, pensions, and similar socioeconomic rights because they lack a digital-ID.

7. Bibliography

Access Now (2024) ***A human rights-centered approach to digital public infrastructure*** (accessed 23 October 2025)

Adjami, M. (2016) ***Statelessness and Nationality in Côte d'Ivoire – A Study for UNHCR***, United Nations Refugee Agency (accessed 18 October 2025)

ADRH (2021) ***The Inclusiveness or Exclusiveness of National IDs in West Africa***, Africa Digital Rights' Hub (accessed 18 October 2025)

AEDH; ritimo; Tournons La Page; Duval, V. and Pourchier, M. (2021) ***Sécurité numérique en Côte d'Ivoire,*** ritimo, 15 December (accessed 18 October 2025)

AfDB (2023) ***Côte d'Ivoire – E-Government Strengthening Support Project (PARAE)***, Project Appraisal Report, African Development Bank (accessed 18 October 2025)

Banégas, R. and Cutulo, A. (2023) ***ID Wars in Côte d'Ivoire: A Political Ethnography of Identification and Citizenship***, Oxford: Oxford University Press (accessed 18 October 2025)

Benamara, A. (2019) ***Axon Wireless Launches 'Tap & Go' SIM Registration in Ivory Coast***, TechAfrica News, 30 October (accessed 18 October 2025)

Bogui, J.M. and Atochua, J.F. (2016) '**La régulation des usages des TIC en Côte d'Ivoire entre identification et craintes de profilage des populations**', *tic&société* 10.1 (accessed 18 October 2025)

CIPESA (2022) ***Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa***, Collaboration on International ICT Policy for East and Southern Africa (accessed 18 October 2025)

CIS (2020) ***Governing ID: Principles for Evaluation***, Centre for Internet and Society (accessed 18 October 2025)

CIVIPOL (n.d.) ***Appui à la mise en œuvre de la strategie nationale de l'état civil et de l'identification de Côte d'Ivoire*** (accessed 18 October 2025)

Cooper, F. (2014) *Citizenship between Empire and Nation: Remaking France and French Africa, 1945–1960*, Princeton NJ: Princeton University Press

Côte d'Ivoire (2022) ***Stratégie nationale de développement du numérique en Côte d'Ivoire SNNCI 2021–2025***, Ministère de l'Économie Numérique, des Télécommunications et de l'Innovation (accessed 18 October 2025)

Côte d'Ivoire (2019a) ***Loi No. 2019-566 du 26 juin 2019 instituant une carte d'identité nationale biométrique***, Citizenship Rights in Africa Initiative (accessed 18 October 2025)

Côte d'Ivoire (2019b) ***Decret No. 2019-458 portant création, organisation et fonctionnement de l'Office national de l'État civil et de l'Identification*** JuriAfrica (accessed 18 October 2025)

Côte d'Ivoire (2018) ***Decret No. 2018-454 du 09 Mai 2018 relatif au registre national des personnes physiques*** (accessed 18 October 2025)

Côte d'Ivoire (2017a) ***Decree No. 2017-193 on the identification of subscribers of telecommunications/ ICT services open to the public and users of cybercafés*** (accessed 18 October 2025)

Côte d'Ivoire (2017b) *Digital Code/Orientation of the Information Society Law No. 2017-803*

Côte d'Ivoire (2016) ***Côte d'Ivoire 2016***, [Constitution] (accessed 18 October 2025)

Côte d'Ivoire (2013a) ***Act No. 2013-451 Dated 19 June 2013 on the Fight Against Cybercrime*** (accessed 18 October 2025)

Côte d'Ivoire (2013b) ***Law No. 2013-450 Dated June 19, 2013 on the Protection of Personal Data*** (accessed 18 October 2025)

CRAI (n.d.) ***Côte d'Ivoire***, Citizenship Rights in Africa Initiative (accessed 18 October 2025)

DataReportal (2025) ***Digital 2025: Côte d'Ivoire*** (accessed 18 October 2025)

Desai, V.T.; Witt. M.; Chandra, K. and Marskell, J. (2017) ***Counting the Uncounted: 1.1 Billion People without IDs***, World Bank blog, 6 June (accessed 18 October 2025)

Diakalidia, K. (2019) ***De la Maitrise de l'identité juridique en Afrique a la résolution des problèmes de l'identification à travers le Registre National des Personnes Physiques: Cas de la Côte d'Ivoire***, ID4Africa Conference, Johannesburg (accessed 18 October 2025)

Dosso, Z. (2019) ***Côte d'Ivoire Commissions Belgian SEMLEX for the Development and Implementation of its National Natural Persons Registry***, Ecofin Agency, 11 April (accessed 18 October 2025)

European Commission (n.d.) ***Côte d'Ivoire – International Partnerships***, Directorate-General for International Partnerships (accessed 19 April 2025)

European Union (2015) ***Joint Valletta Action Plan*** (accessed 18 October 2025)

GSMA (2024) ***Understanding 7 Billion: Counting Connections and People***, 15 April (accessed 18 October 2025)

Hersey, F. (2019) ***Digital ID in Africa this Week: Biometric ID for Guinea, Continued ID Controversy for Côte d'Ivoire***, BiometricUpdate.com, 4 July (accessed 18 October 2025)

Identity Week (2017) ***Ivory Coast Introduces Biometric Residence Cards***, 15 August (accessed 18 October 2025)

Identity Week (2015) ***Côte d'Ivoire Taps Zetes for Health Cards***, 24 February (accessed 18 October 2025)

Idowu, H. (2021) '***Biometric Technologies and the Prospect of Sustainable Democracy in Africa***', *Journal of African Elections*, 20.1: 23–43, DOI: 10.20940/JAE/2021/v20i1a2 (accessed 18 October 2025)

IOM (2019) ***Migration Governance Indicators – Republic of Côte d'Ivoire***, International Organization for Migration (accessed 18 October 2025)

Iwuoha, V.C. (2025) '***European Biometric Borders and (Im)Mobilities in West Africa: Reflections on Migrant Strategies for Border Circumvention and Subversion***', *Politics & Policy*, 53.1 (accessed 18 October 2025)

Jarrahi, J. (2021) ***GenKey Delivers National Biometric ID to Ivory Coast***, BiometricUpdate.com, 5 January (accessed 18 October 2025)

MacDonald, A. (2024) ***ECOWAS Agrees to Accelerate Implementation of ENBIC Regional ID Card for Stronger Integration***, BiometricUpdate.com, 1 October (accessed 18 October 2025)

MacDonald, A. (2021) ***Côte d'Ivoire, Ghana Share Digital ID Success Stories in ID4Africa livecast***, BiometricUpdate.com, 1 November (accessed 18 October 2025)

Mann, G. (2009) '**What Was the *Indigénat*? The "Empire of Law" in French West Africa**', *Journal of African History*, 50.3: 331–53 (accessed 18 October 2025)

Mayhew, S. (2015) ***SNEDAI Partners with Zetes for Biometric ID Card Registration and Production***, BiometricUpdate.com, 27 February (accessed 18 October 2025)

Meagher, P. (2017) ***Regulatory Framework for Digital Financial Services in Côte d'Ivoire: a Diagnostic Study***, Washington, DC: CGAP (accessed 18 October 2025)

ONECI (n.d.) ***Documents a Fournir Concernant la Carte Nationale D'Identite (CNI)*** Office National de l'Etat Civil et de l'Identification (accessed 18 October 2025)

Présidence de la République de Côte d'Ivoire (n.d) ***Une Côte d'Ivoire Solidaire:*** (accessed 18 October 2025)

Privacy International (2020) ***Here's How a Well-Connected Security Company is Quietly Building Mass Biometric Databases in West Africa with EU Aid Funds***, 10 November (accessed 18 October 2025)

Semlex (2023) ***International Enrollment***, 11 April (accessed 18 October 2025)

Sid'Ahmed, T.O. and Morisset, J. (2017) ***In Côte d'Ivoire, Every Story Counts: New Computerized Personnel and Wage Management System has Improved Employee Satisfaction and Effectiveness in the Civil Service***, World Bank blog, 26 April (accessed 18 October 2025)

StartupBlink (2025) ***The Startup Ecosystem of Ivory Coast*** (accessed 18 October 2025)

UNHCR Côte d'Ivoire (2024) ***Report on Statelessness 2023***, United Nations Refugee Agency

US Department of State (2018) ***Country Report on Human Rights Practices 2017 – Cote d'Ivoire*** (accessed 18 October 2025)

World Bank (2024a) ***Côte d'Ivoire Third Investment for Growth DPF and PBG (P180234)***, Program Information Document, Washington, DC: World Bank (accessed 18 October 2025)

World Bank (2024b) ***West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program*** (accessed 18 October 2025)

World Bank (2022) ***Côte d'Ivoire – Country Partnership Framework for the Period FY23–FY27*** (accessed 18 October 2025)

World Bank (2018) ***Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints***, Washington, DC: World Bank (accessed 18 October 2025)

World Bank (2016) ***ID4D Country Diagnostic: Côte d'Ivoire***, Washington, DC: World Bank (accessed 18 October 2025)

institute of development studies

Delivering world-class research, learning and teaching that transforms the knowledge, action and leadership needed for more equitable and sustainable development globally.

Institute of Development Studies
Library Road
Brighton, BN1 9RE
United Kingdom
+44 (0)1273 606261
ids.ac.uk

Charity Registration Number 306371
Charitable Company Number 877338