Global Report

Biometrics and Digital Identity: Trend Analysis and Comparative Assessment

Greater Internet Freedom

Centre for Intellectual Property and Information Technology Law (CIPIT)
Strathmore University

September 2023

Acknowledgments

This report is published under the USAID Greater Internet Freedom (GIF) project implemented by Internews and the GIF Consortium.

Lead Researcher

We would like to express our gratitude to the Centre for Intellectual Property and Information Technology Law (CIPIT) for acknowledging Florence Ogonjo, Joshua Kitili, Lilian Olivia Orero, Doreen Aoko Abiero, Josephine Kaaniru, and Dan Allan Kipkoech who conducted this research and authored this report in close consultation with Internews.

Research Oversight

Olga Kyryliuk, Berhan Taye, Technical Advisors on Internet Governance and Digital Rights, (GIF) Internews

Sigi Waigumo Mwanzia, Digital Rights Advisor, (GIF) Internews

Brittany Piovesan, Chief of Party, (GIF) Internews

Jessica Moncrieff, Program Officer, (GIF) Internews

Wakesho Kililo, Technical Coordinator (Africa), (GIF) Internews

Mavzuna Abdurakhmanova, Central Asia Regional Coordinator for Digital Rights, (GIF) Internews

Diana Bichanga, Program Associate, (GIF) Internews

Research Contributors

Africa Region

Africa Regional Report - Victor Kapiyo, Independent Researcher

Angola, the Central African Republic and the Democratic Republic of Congo - Dr. Dércio Tsandzana, Independent Researcher

Mozambique - Media Institute of Southern Africa (MISA Mozambique)

Tanzania - Digital Agenda for Tanzania Initiative and Advocate Josephina Nshunju, Independent Researcher

Uganda - African Centre for Media Excellence (ACME) and Paul Kimumwe, Independent Researcher

Zimbabwe - Media Institute of Southern Africa (MISA Zimbabwe) and Kuda Hove, Independent Researcher

Balkans Region

Balkan Investigative Reporting Network and Predrag Tasevski, Expert

Central Asia Region

Dana Utegen, Independent Researcher

Latin America and the Caribbean Region

Derechos Digitales, and Carlos Guerrero and Paloma Lara Castro, Independent Researchers

South and Southeast Asia Region

Engage Media and Shruti Trikanad, Independent Researcher

We are also grateful to all the GIF partners, consultants, communities, and individuals who generously shared their time, experiences, and perspectives with us, and contributed to the research process.

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of the CIPIT and do not necessarily reflect the views of USAID, the United States Government, or Internews.

Published September 2023

Table of Contents

Executive Summary

The "*Biometrics and Digital Identity: Trend Analysis and Comparative Assessment*" global report is produced by the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, under the Greater Internet Freedom (GIF) project implemented by Internews and the GIF Consortium. It is informed by a trend analysis and comparative assessment performed by the CIPIT based on the reports produced by the GIF Consortium.

The GIF Consortium conducted multi-region research in **27 GIF countries** seeking to identify and compare the state of biometrics and digital identity threats, usage, and impact in Africa, the Balkans, Central Asia, Latin America and the Caribbean, and South and Southeast Asia. This research was guided by three core considerations, including:

1. *Documenting biometrics and digital ID adoption drives by national and international actors*
2. *Generating knowledge about biometrics and digital ID systems*
3. *Enhancing GIF Partners' capacity to influence the discourse around digital identity through research-informed input into this critical global discourse.*

Key Findings

The key findings are summarized in detail below and explored extensively in the report.

Table 1: Summary of Key Findings

Trend/Assessment	Key Findings
On BDI and Pertinent Sectors	Rapid growth is expected in the biometric technology market, with implications for digital rights and Internet freedoms in the GIF regions. The public (government) sector and BFSI sectors are leading the general uptake and use of BDI solutions in the GIF regions.
On Technology and the BDI Fields	Tech has facilitated a steady, ongoing, transition away from paper-based to digitized ID systems across all five GIF regions. The collection of biometrics by state and private entities is an entrenched practice, relying on the deployment of biometric

	technologies. The most commonly deployed biometric tech include fingerprint scanners/readers, facial recognition cameras, and iris scanners, to capture fingerprint, facial and iris biometric.
On Legal Frameworks and BDI Fields	States are obliged to develop and implement a robust and proportionate legal framework for BDI systems consisting of policies, laws, regulations, codes of practice etc All 27 GIF countries have either amended existing civil registration and vital statistics (CRVS) laws, population registration laws, or identification laws, or enacted new laws to accommodate the introduction of a digitized ID system 18 out of the 27 GIF countries have enacted a stand-alone law on the protection of personal data that apply to BDI systems. The remaining countries rely on sectoral laws, which are inadequate to comprehensively protect individuals' data.
Concerns in BDI Fields	**Privacy, Security and Ethical Concerns:** Observed misuse of personal and biometric data giving rise to mission creep concerns; Observed tech-vendor and supplier dominance in at least three out of the five GIF regions, giving rise to fears of vendor lock-in, potential biases in tech, impaired data sovereignty, and weakened data security **Accountability and Transparency Concerns:** Observed gaps in accountability and transparency mechanisms for the regulation of BDI systems, technologies and procedures **Accuracy and Reliability Concerns:** Observed risk of data **inaccuracy** reflected across different thematic areas, namely regulation, limitation of use, security, and integrity.
Workforce Considerations	Creation of **digital transformation specialists roles**, driven by technology and digitization efforts.

Stakeholder Engagements and BDI	On the **stakeholder diversity and inclusion front:** public participation arises mainly as opposition to government decisions regarding BDI systems. There has been no observable change in the siloed stakeholder engagements revolving exclusively around governments, international development partners, and the private sector, to the exclusion of all other stakeholders.
	Source: GIF Reports.

The findings in this global report serve as a call to action for relevant stakeholders, including government, developers, vendors, policymakers, the international community, civil society actors, and ID users, highlighting the urgent need to address:

- Existing gaps and inconsistencies in laws and regulations governing the collection of biometric data for digital ID to restore public trust and confidence
- Ethical concerns that create room for discrimination, exclusion, and marginalization
- Use of data in digital ID and biometrics systems for unlawful surveillance and targeting
- Core concerns including privacy, security, ethics, accountability, transparency, accuracy and reliability throughout the BDI lifecycle
- Lack of a human rights approach in adopting and utilizing biometric and digital ID technologies and systems.

Key Recommendations

Recommendations Guided by Key Findings

GIF Governments are urged to:

Develop and implement a robust and proportionate legal framework for BDI systems consisting of policies, laws, regulations, codes of practice etc. The nine GIF countries

(out of 27 researched) without comprehensive, stand-alone data protection laws should immediately adopt frameworks to protect personal data

The International Community operating in GIF regions is urged to:

Ensure that technical and financial support for BDI programs granted/loaned to governments incorporates a public awareness budget line. This should sensitize BDI users on both the risks and benefits of BDI technologies and encourage participatory and inclusive multi-stakeholder engagement across the ID lifecycle.

GIF civil society organizations (CSOs) are urged to:

Leverage a range of soft (e.g., press releases) and hard (e.g., public interest litigation) tactics to introduce rights-respecting reforms into BDI systems across all five researched regions, including leveraging the capacities of the GIF Consortium to engage in advocacy and policy efforts.

Promote digital rights and Internet freedom in the BDI ecosystem, through policy engagements, advocacy and awareness campaigns, research, collaborations and partnerships.

Glossary of Terms

Biometric data	Physical or behavioral attributes of a person, such as fingerprints, irises, facial image, signature[1].
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
Digital Identity	A set of attributes and/or credentials collected and stored electronically that uniquely identifies a person.
Foundational ID	A multipurpose ID meant to provide identification for the general population, often forming the basis for various public and private sector transactions.[2]
Functional ID	ID designed for a specific purpose (e.g., voter IDs, health records, tax ID numbers, social protection, ration cards, or driving permits) and usually covering a subset of the population. However, in many cases, these are accepted as proof of identity for broader purposes beyond their original scope, especially when robust foundational ID systems are not present.[3]

[1] World Bank Guide. < https://id4d.worldbank.org/guide/biometric-data>
[2] 'The Emerging Era of Digital Identities: Challenges and Opportunities for the G20.' (ADB Institute, 2022) <https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf>
[3] ibid

Personal data	Any information relating to an identified or identifiable individual.[4]
Centralized system	Centralized identity systems are where digital identity credentials are held in a single place, and each identity is used for a single purpose. In this model, the identity provider is responsible for authentication. An example of a centralized model is a digital driving license issued by a national or regional government. [5]
Decentralized system	Decentralized identity is a model in which certain identities are replaced by other self-owned identities, such as usernames. This means that digital identity credentials are generally created and managed directly by the owner of the credentials. They are also usually stored in a decentralized manner, such as on a mobile device. Due to the fact, decentralized identities are independently created, traditional means of logging in, such as passwords, are replaced with cryptographic keys. Decentralized identities can be either blockchain or non-blockchain based. Decentralized identity can also include distributed identity.[6]
Single Factor Authentication	Use of one feature to verify a person's identity. This may include passwords, fingerprints, PINs, facial, voice, iris, and vein recognition. Single-factor authentication is widely used in various industries,

[4] World Bank https://www.worldbank.org/en/about/legal/privacy-notice
[5] 'Digital Identity: Next Frontier of Cyber Security' (Juniper Research, 2023) <https://www.juniperresearch.com/researchstore/fintech-payments/digital-identity-research-report>
[6] ibid

	including government, consumer electronics, banking and finance, and healthcare.
Multi-Factor Authentication	Uses more than one feature often three to verify a person's identity. Multi-factor authentication ensures the confidentiality of personal information by providing a high level of security. Multi-factor authentication methods may combine a code, a token or pin number, and biometrics for example fingerprint. Something you know, something you have, and something you are.

List of Abbreviations

AI	Artificial Intelligence
BDI	Biometric Digital Identity
GIF	Greater Internet Freedom
LAC	Latin America and the Caribbean
ML	Machine Learning
SDG	Sustainable Development Goal
SSE Asia	South and Southeast Asia
UDHR	Universal Declaration on Human Rights
ICCPR	International Covenant on Civil and Political Rights

Introduction

The Sustainable Development Goals (SDG), Target 16.9 calls on UN Member States to prioritize legal identity for all including free birth registration. Generally, this indicator promotes peaceful and inclusive societies for sustainable development, access to justice, and effective, accountable, and inclusive institutions at all levels.[7] Legal identity plays a crucial role in advancing global development as it enables access to a wide range of services, including voting, financial services, land ownership, business registration, and school enrollment, among others. Further, legal identity and associated systems play a pivotal role in shaping and safeguarding digital rights and Internet freedoms. The establishment of a robust legal identity framework not only fosters but also empowers the free exercise, enjoyment, and promotion of these rights on online and digital platforms.

The existence of digital identity is inherently intertwined with the continuous evolution of digital technology. Proof of identity in physical and digital environments plays a vital role in determining access to opportunities and the establishment of trust with one another. [8] Identity shapes our social contracts as it exists in relation to the economic, political, cultural, and social structures we live in.[9] The social contract of identity derives from the legal relationship between a citizen and the citizen's state, usually involving obligations of support and protection.[10] Notably, government biometric digital identity (BDI) systems are increasingly viewed as a form of "digital public infrastructure"[11] that facilitates the social contract between the state and individuals.

The Universal Declaration on Human Rights (UDHR) provides for the inherent right of every individual to dignity and human rights (Preamble). Articles 6 and 7 of the UDHR envisage that "everyone has the right to recognition everywhere as a person before the law" and to "equal

---

[7] Indicators and a Monitoring Framework.<https://indicators.report/targets/16-9/>
[8] Identity in a Digital World A New Chapter in the Social Contract (World Economic Forum, 2018) https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
[9] *Ibid.*
[10] Barbara von Rütte, 'Citizenship and Nationality' The Human Right to Citizenship(Vol 21,Brill | Nijhoff 2022) https://brill.com/display/book/9789004517523/BP000002.xml
[11] UNECA (2023). Implementing digital ID systems in Africa: ECA's Stakeholders Dialogue explores pathways for leveraging Digital ID Systems and disruptive technologies.

protection of the law."[12] This right is given legal force in Article 16 of the International Covenant on Civil and Political Rights (ICCPR) which guarantees the right to "recognition everywhere as a person before the law", while Article 24(2) recognises the right to registration at birth.[13] The right to nationality, as an element of identity, is recognized in these international instruments, such as Article 24 of the ICCPR, and numerous national constitutions.[14]

The adoption and implementation of digital identity systems, relying on biometrics and biometric technologies, to establish a digitized form of identification at national levels has become a growing trend in all five regions covered in this report, including Africa, the Balkans, Central Asia, Latin America, and South and Southeast Asia. This is prompted by technological advancements that have led to the digitization of activities and services, such as e-government, e-identification or digital identification, e-commerce, digital banking, amongst others. Across many countries, the goal of biometrics and digital identity (BDI) systems will differ depending on local context and needs, but most are geared at establishing secure, reliable, efficient and inclusive ways to identify and verify individuals in the digital age.[15]

The utilization of digital technology for collecting, processing, and storing individuals' personal data, is touted as beneficial for bolstering the integrity of ID systems. In many cases, tools such as biometrics, smart cards, or public-key infrastructure are used to safeguard credentials. Compared to paper-based systems, digital ID strengthens security and can be linked to more diverse services at the public and private levels. Where citizens' experience of governance has been characterized by graft and abuse, automation of the citizen–state interface can help rebuild trust. By leveraging the digital footprints of a connected population, digital ID opens new routes to inclusion for people who lack formal documentation.

[12] Universal Declaration of Human Rights https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[13] International Covenant on Civil and Political Rights https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
[14] IOM Institution Strategy on Legal Identity (IOM) https://publications.iom.int/system/files/pdf/Legal-Identity-Strategy_0.pdf
[15] Identification for Development. (World Bank) https://thedocs.worldbank.org/en/doc/325451527084344478-0190022018/original/ID4DProgramFlyerV52018.pdf

Table 2: Global ID Facts

Snap Shot: Identity Statistics and Under-Identified Populations

- *Nearly "**850 million people globally lack official identity**":* this leads to restricted access to services and the absence of protections associated with having an official identity.[16]
- *The term "**under-identified**" encompasses a large number of people, including poor, rural, indigenous, female, refugee, immigrant, or marginalized populations and refers to:*
    - "people who have been enrolled in a government ID system at some point in their lives, but whose identity credentials may not empower them to exercise their rights, receive government services, or participate fully in the modern economy."[17]

Sources: World Bank. USAID.

Like all systems that leverage digital advancements and technologies, BDI systems inevitably face challenges and risks, primarily arising from the susceptibility of technologies to manipulation, the type of infrastructure deployed to store and process this data, and the nature of the information collected to make these systems a reality. Concerns about the privacy and security of collected data, which often includes a combination of personal or biometric information, lead to a loss of public trust as apprehensions arise regarding the potential misuse of data for unauthorized purposes.

Additionally, many ID-related risks, including state-facilitated mass surveillance, data breaches, and identity theft, are heightened by existing and emerging digital ID technologies, which are making it easier to find information on individuals from a consolidated source for various illegal purposes, such as unauthorized 'tracking and tracing' activities, ID-related extortion, amongst others. A few examples of these technologies include biometric identification, mobile-based identity solutions, blockchain-based identity solutions, digital ID wallets, artificial intelligence (AI) and machine learning (ML) in identity verification, amongst others.[18]

Generally, the lack of comprehensive legislative and governance structures exacerbates the issues of surveillance, data protection concerns and cybersecurity. Critically, legal frameworks and governance structures, such as oversight and redressal mechanisms, play a

[16] Identity in a Digital Age : Infrastructure for Inclusive Development (USAID, 2022) https://www.usaid.gov/sites/default/files/2022-05/IDENTITY_IN_A_DIGITAL_AGE.pdf
[17] Ibid 8
[18] Ibid 2

critical role in the design, implementation, and operation of digital ID systems. Legal frameworks delineate what is and what is not permissible, particularly regarding the processing and sharing of personal data and biometric information, outline ID users' consent, control and rights, define the scope of identity verification and authentication, establish oversight bodies or regulatory authorities, amongst others. The intersection and tension between legal frameworks and digital ID systems is exemplified by the ongoing debate over 'function creep,' which refers to the apprehension regarding the expansion and utilization of BDI programs beyond their initial intended purposes and scope.

This global report offers a global outlook on BDI adoption and use in five researched GIF regions, highlighting variations and similarities in deployment, threats, and impact. It examines BDI ecosystem trends, market share, global concerns, and regulatory mechanisms. Stakeholder engagement and investments crucially determine BDI system success or failure, with regional analysis presented. The report delves into historical motivations for BDI adoption, differences and similarities in impact, and identifies gaps, opportunities, and recommendations for the BDI landscape worldwide.

Report Structure

The "*Biometrics and Digital Identity: Trend Analysis and Comparative Assessment*" global report is split into two parts and is organized as follows:

a. **Trend Analysis:** this explores the BDI landscape focusing on understanding the global market share and sectoral utilizations of BDI; the impact of technology on the growth and adoption of BDI; BDI legal and regulatory frameworks; the impact of BDI on the employment sector focusing on jobs, skills, and tasks; and the evolution of stakeholder engagements in BDI deployment.

b. **Geographic Assessment:** this provides a comparative BDI analysis from a geographical perspective. Perspectives presented in this section outline similarities and differences in the five GIF regions exploring BDI definitions, purposes and types; adoption rates; risks in BDI systems; utilizations and use cases of BDI; and stakeholder participation and engagement.

By analyzing the BDI landscape in the five researched GIF regions, this global report equips a wide variety of stakeholders with the requisite knowledge and insights necessary to navigate this domain, including governments, policymakers, BDI developers, private entities, CSOs, and BDI users. A report of this nature is crucial for understanding how BDI intersects with the ever-evolving digital space, digital rights and Internet freedoms, and associated usage, threats and impact considerations.

Methodology

The trends analysis and comparative geographical impact assessment methodology are based on a predefined set of parameters that take into account the current BDI ecosystem both globally and in the identified regional areas. The analysis is largely guided by information and statistics gathered from the GIF regional reports, and supplemented with a review of selected literature.

The GIF regions under evaluation in this report:

Table 3: GIF BDI Research Regions

BDI Research – Five Focus Regions

- **Africa:** Angola, Central African Republic (CAR), Democratic Republic of Congo (DRC), Mozambique, Tanzania, Uganda, and Zimbabwe.
- **Balkans:** Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, and Serbia.
- **Central Asia:** Kazakhstan, Kyrgyzstan, and Tajikistan.
- **Latin America and the Caribbean:** Bolivia, Brazil, Colombia, and Ecuador,
- **South and Southeast Asia:** Bangladesh, Cambodia, Indonesia, Maldives, Nepal, Philippines, and Sri Lanka.

Source: GIF.

In ***Part I*** of the global report, a comprehensive trend analysis is conducted to examine the BDI landscape. The parameters explored include:

- **Trend 1**: an examination of key sectors influencing the growth and expansion of biometrics and digital ID. The information and statistics utilized for this examination is derived from secondary data, including industry analyses, articles, media reports, and market research reports.

- **Trend 2:** an examination of advancements in biometrics, biometric technologies, and digital ID.
- **Trend 3:** a legal and regulatory framework analysis, focusing on legal challenges and court rulings.
- **Trend 4:** thematic BDI concerns, focusing on privacy, security, ethics, transparency, accountability, accuracy, and reliability in the researched GIF regions.
- **Trend 5:** changes brought by BDI in the employment sector relating to jobs, skills, and tasks. This trend is informed by information and statistics derived from the literature review, rather than content located in the GIF reports.
- **Trend 6:** stakeholder participation and engagement in the adoption, implementation, and use of BDI, including shifting collaborations and partnership levels, public awareness and engagement, shifts in the stakeholders engaged in policy and development, and the steps taken to increase stakeholder diversity and inclusion.

In ***Part II*** of the global report, the impact points explored in all five researched GIF regions include:

- **Impact 1:** comparative analysis of GIF research reports to assess similarities and differences in the definitions of BDI, the purpose of BDI systems, the types of data collected, and use cases. The analysis also focuses on how the regional historical factors have influenced the type of BDI system adopted.
- **Impact 2:** comparative analysis of GIF research reports to assess cross-cutting risks in the use of BDI and recommended solutions.

Trend Analysis

Trend 1: BDI and Pertinent Sectors

The global digital identity solutions market size is "valued at an estimated USD 27,508.5 million, and this is expected to advance at a compound annual growth rate (CAGR) of 17.2% from 2023 to 2030."[19] Conversely, the global biometric technology market size was "valued at USD 34.27 billion in 2022 and is expected to expand at a compound annual growth rate (CAGR) of 20.4% from 2023 to 2030."[20] By 2031, it is estimated that the biometrics market will be 'worth USD 136.18 billion.'[21] These indicative figures indicate that the BDI market will expand significantly over the coming years, with more rapid growth expected in the biometric technology market, especially for authentication purposes.[22]

For digital rights and Internet freedom advocates, this projected market growth is a call to action to ensure that documented concerns and considerations in the GIF reports are (i) addressed by relevant actors, including states, private entities such as BDI infrastructure providers, and the international community, and (ii) mitigated to avoid entrenching documented concerns. Specifically, issues of privacy and surveillance, government and corporate control, exclusion and discrimination, biometric data misuse, and stifled anonymous expression, amongst others, must be integrated into sectoral expansion considerations.

Key Factors Influencing BDI Ecosystem

There are multiple factors driving BDI sectoral expansion or downswing. These include, but are not limited to:[23]

---

[19] Grand View Research (2023). Digital Identity Solutions Market Size, Share & Trends Analysis Report By Component, By Solution, By Identity Type, By Biometric, By Solution Type, By Authentication, By Deployment, By Vertical, And Segment Forecasts, 2023 - 2030.

[20] Grand View Research (2023). Biometric Technology Market Size, Share & Trends Analysis Report By Component, By Offering, By Authentication Type, By Application, By End-use, By Region, And Segment Forecasts, 2023 - 2030.

[21] Transparency Market Research (2022). Biometrics Market Size worth $136.18 Billion by 2031 | CAGR: 13.3%: Notes TMR Study.

[22] Biometrics Institute (2023). Digital Identity and Biometric Authentication paper.

[23] Other factors include security level concerns, amongst others.

At the government level: expanding BDI uptake is propelled by a growing emphasis on the transformation of national economies relying on digital technologies. Governments worldwide are mandating digital IDs relying on biometrics for access to public and/or private services. Further, legal and regulatory frameworks imposing stricter compliance standards on both state and private entities continue to drive BDI uptake across the regions, e.g., through the adoption/amendment/review of civil registration, population registration or identification laws, laws promoting the protection of personal data, amongst others.

Illustratively, digital transformation efforts by governments, including at the legal and regulatory level, have fueled the growth of the ***identity as a service (IDaaS) market*** which is 'projected to grow from an estimated USD 5.6 billion to reach USD 16.8 billion by 2027 [with a] CAGR of 24.7% from 2022.'[24]

At the consumer level: the BDI market is heavily consumer-centric, and sectoral expansion or downswing is influenced by consumers. Notably, uptake is fuelled by consumer demands for interoperable identity solutions that can be utilized across different use cases in the digital ecosystem.[25]

At the access and cross-industry level: expanding BDI uptake is presented as capable of enabling cross-industry, service and application access. Notably, the growth of 'reusable identity', i.e., "a single digital identity that can be used to access multiple services and applications" is quickly developing into a key trend that is critical for digital identification. It is estimated that the reusable identity global market size will "expand from USD 32.8 billion in 2022 to USD 266.5 billion by 2027."[26]

At the technological level: expanding BDI uptake is fuelled by technological advancements that are presented as safe, reliable, and secure. Notably, the promise of security and safety is embodied by the increasing uptake of digital identity-based authentication methods such as multi-factor authentication (MFA) over traditional password-based systems.

---

[24] ResearchAndMarkets (2022). IDaaS Market by Component (Provisioning, Single Sign-On, Advanced authentication, Audit, Compliance, and Governance, Directory service, and Password management), Organization Size, Deployment Type, Vertical and Region - Global Forecast to 2027.

[25] Liminal (2022. The Market Opportunity for Reusable Identity and How to Get There.

[26]

At the financial level: expanding BDI uptake is presented as cost-effective to both state and private entities, especially as BDI technologies become more accessible and mature.

Regional Observations

Sectoral Examination

Across the five researched regions, the demand for biometrics and digital ID solutions is heavily concentrated in the public (government) and the banking, financial services, and insurance (BFSI) sectors. However, as Figure 1 below illustrates, digital ID impacts a wider range of sectors and services that are not explored in this report due to the GIF scope. Notably, these BDI services are facilitated by solutions provided by ***private sector identity and biometrics technology vendors***, which largely includes integrated infrastructure system management platforms or associated hardware, technical capacity and assistance, or services to support governments and BFSI organizations to integrate biometric technologies and digital ID solutions into their existing infrastructure.[27]

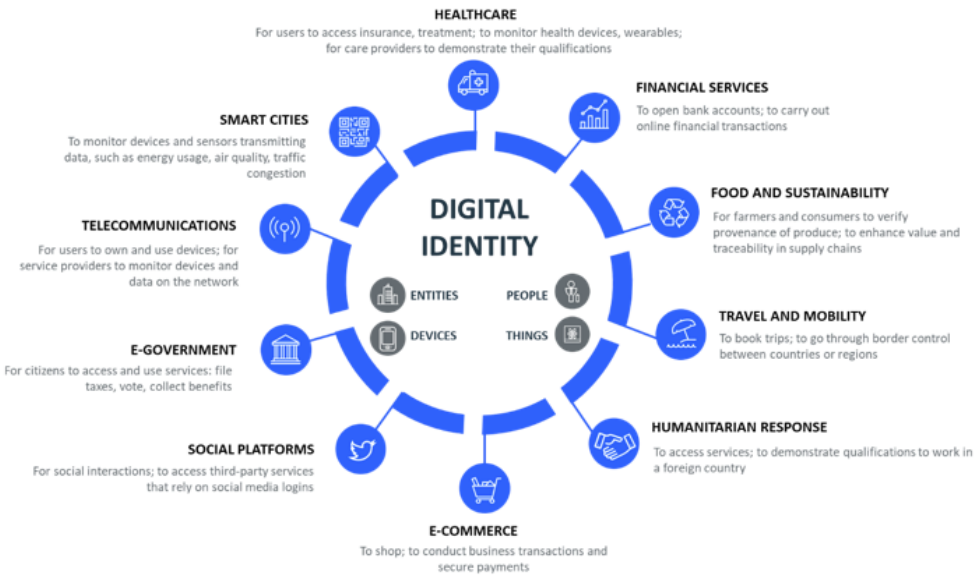

Figure 1: World Economic Forum.

Following the COVID-19 pandemic where BDI solutions were advanced as critical for online learning, there has been a ***general downswing*** in the publicly-reported uptake of BDI in the

[27] Grand View Research (2023). Digital Identity Solutions Market Size, Share & Trends Analysis Report By Component, By Solution, By Identity Type, By Biometric, By Solution Type, By Authentication, By Deployment, By Vertical, And Segment Forecasts, 2023 - 2030.

education sector. However, some countries in the Africa region, such as the DRC, are ramping up digital ID uptake for student digital IDs, following a partnership between Sycamore and TECH5.[28] Based on a review of GIF reports and an exploratory literature review, there is an ***increased uptake*** of biometrics and digital ID solutions observed in the following sectors (*this is not exhaustive and is not applicable across all GIF regions*):

Table 4: Expanding BDI Sectors

BDI Sectoral Expansion

- **BFSI Sector:** Private sector entities are deploying BDI solutions for e-Know Your Client (e-KYC) purposes, online banking, digital payment systems, and identity verification for financial transactions.[29]
- **Government Applications/Services:** Governments worldwide have increasingly invested in biometric identification systems to issue national identification cards, e-passports, driving licenses, and other forms of legal identity documentation to streamline administrative processes.[30] Further, many governments have integrated biometric technologies for electoral management purposes, including voter registration, and population censuses.[31]
- **E-Commerce Sector:** Entities are deploying BDI solutions for secure 'purchase and sale transactions of goods or services conducted over computer networks.'[32]
- **Border Control, Travel, and Aviation Services:** Biometric technologies have been integrated into border control, airport, and travel processes, enabling faster and more secure passenger identification, check-ins, and boarding.[33]
- **Mobile Services:** The use of biometric authentication on digital devices, such as smartphones and tablets, continues to increase in an unprecedented manner. Fingerprint sensors, facial recognition, and iris scanning technologies have become a ubiquitous feature of user authentication, including in the mobile commerce sector.[34]

---

[28] Biometric Update (2023). Tech5 provides contactless biometrics, issuance platform for student digital IDs in DRC | Biometric Update

[29] Biometric Update (2016). Technavio identifies top 4 trends affecting biometrics in BFSI through 2020 | Biometric Update. Also: SmartTech Asia 2023.

[30] Notably, the ID4Africa Conference hosted by the World Bank in Nairobi, Kenya underscored this global uptake, guided by the theme that 'digital identity is public infrastructure.' See: ID4Africa 2023.

[31] PSD Group (2020). How Digital Identity & Biometric Technology Are Transforming Emerging Economies; Frost & Sullivan (2021). Global Digital Identity Solutions Growth Opportunities.

[32] UNCTAD (2023). Measuring the Value of E-Commerce; Medium (2018). Digital identity, enters a new era of e-commerce; Mario Masaya (2022). E-Commerce, Digital Identity, and Inclusive Digital Economy in Southeast Asia.

[33] IFSEC Insider (2021). Growth in biometrics-driven digital identity to automate airport security and improve passenger experience; Chris Burt (2020). Biometric airport checks, border security and digital ID for travel increasing around the world.

[34] Grand View Research (2023). Biometric Technology Market Size, Share & Trends Analysis Report By Component, By Offering, By Authentication Type, By Application, By End-use, By Region, And Segment Forecasts, 2023 - 2030; Marcin Frąckiewicz (2023). The Future of Biometric Authentication: Trends and Predictions; GSMA (2021). Access to Mobile Services and Proof of Identity 2021.

- **Healthcare Sector:** The healthcare sector continues to aggressively implement biometrics and digital identity solutions to ensure accurate patient identification, secure access to medical records, and prevent medical identity theft.[35]
- **Law Enforcement, Military & Defense Sectors:** The expansion of law enforcement services and surveillance solutions is driving the uptake of biometric solutions to satisfy security requirements and needs.[36]

Additional Sources: Biometric Update (BFSI). Biometric Update (Government). World Economic Forum. Transparency Market Research. Liminal. Juniper.

The sectors identified in Table 4 are key drivers in the **growing demand for *multi-factor authentication (MFA)***, with heightened uptake being witnessed in the BFSI sector, particularly for mobile banking purposes.[37] The National Institute of Science and Technology (NIST) defines MFA as "*an authentication system that requires more than one distinct authentication factor for successful authentication.*"[38] MFA relies on three authentication factors, namely 'something you know' such as your date of birth or a password, 'something you have', such as a smartphone, and 'something you are', such as your iris or fingerprint.[39]

MFA is predicted to record the fastest growth in the authentication methods/type market, with an estimated valuation of "USD 26.7 billion by 2027 with a CAGR of 15.6%."[40] This is partly attributed to the fact that MFA offers the sectors identified above with layered solutions to cybersecurity and data protection issues, such as cyber-attacks, data breaches, identity theft, fraud, amongst others, faced by governments and entities in the BFSI sector.[41]

Conversely, market research reports detail a **preferred adoption (rather than *downswing)*** of 'more robust, and secure biometric authentication measures and methods' over traditional or

[35] Grand View Research (2023). Digital Health Market Size, Share & Trends Analysis Report By Technology (Healthcare Analytics, mHealth, Tele-healthcare, Digital Health Systems), By Component (Software, Hardware, Services), By Region, And Segment Forecasts, 2023 - 2030; Vantage Market Research (2022). Digital Health Market - Global Industry Assessment & Forecast.
[36] HID Global. Solutions - Biometrics for Law Enforcement; Meticulous Market Research (2022). Biometric Systems Market by Offering, Biometrics Type (Fingerprint Recognition, Voice Recognition), Contact Type, Authentication Type, Platform, Application, End User (Government, Military & Law Enforcement, and Others)– Global Forecast to 2029.
[37] MarketsandMarkets (2022). Multi-Factor Authentication Market Size, Share, Trends, Revenue Forecast & Opportunities.
[38] National Institute of Science and Technology (2017). Digital Identity Guidelines.
[39] IDMe (2021). What is Multi-Factor Authentication?
[40] MarketsandMarkets (2022). Multi-Factor Authentication Market Size, Share, Trends, Revenue Forecast & Opportunities.
[41] Meticulous Market Research (2022). Biometric Systems Market by Offering, Biometrics Type (Fingerprint Recognition, Voice Recognition), Contact Type, Authentication Type, Platform, Application, End User (Government, Military & Law Enforcement, and Others)– Global Forecast to 2029; Alessandro Mascellino (2022). Biometrics trends for 2023: multimodal and MFA to grow alongside privacy regulations.

conventional authentication measures, such as password systems and key cards.[42] Despite this, passwords are still very rampant across the five regions, and are generally used for various applications, such as securing email accounts and facilitating online purchases.

This report notes a **general shift in the types of biometrics** being collected and used in ID systems for identification, authentication or verification purposes. Across many GIF countries, those that are yet to transition or integrate digital ID into their national ID systems and countries that are aggressively relying on digital transformation for economic growth typically collect ***physiological rather than behavioral biometrics***, such as fingerprint, iris, or face biometric modalities.

The following transitions are critical for this trend:

a. Shifting reliance on fingerprint recognition as the dominant biometric modality towards ***multi-modal biometrics***: i.e., the use of two or more biometric modalities combining fingerprint, facial, iris recognition, amongst others. Illustratively, reports indicate that global multimodal biometrics in the healthcare market is expected to rise from "USD 14.68 billion in 2022...to reach USD 42.96 billion by 2028 growing at a CAGR of 15.8%."[43]

b. Transition towards ***contactless biometric systems leveraging palm vein, iris, face, or fingerprint biometrics for authentication***:[44] following the COVID-19 pandemic, countries in five researched regions aggressively pushed for more contactless, hygienic, non-face-to-face interactions. IDEMIA, a leading provider of contactless biometrics, states that its contactless biometric devices integrate "algorithms [that are] powered by ***Artificial Intelligence***"[45] evidencing an integration of emerging technologies into the BDI market. It is estimated that contactless biometrics will provide a "USD 59.5 billion market opportunity by 2030 [with a] 14.6% CAGR."[46]

---

[42] Grand View Research (2023). Biometric Technology Market Size, Share & Trends Analysis Report By Component, By Offering, By Authentication Type, By Application, By End-use, By Region, And Segment Forecasts, 2023 - 2030;
[43] WeMarket Research (2023). Global Multimodal Biometrics In Healthcare Market.
[44] Fujitsu. Palm Secure.
[45] IDEMIA (2021). Contactless biometrics in action.
[46] Prescient & Strategic Intelligence (2022). Contactless Biometrics Market.

c. Transition towards the collection of immutable biometrics, such as ***Deoxyribonucleic Acid (DNA) data in civilian identification systems***: Companies such as Veridos, through VeriDNA, are expected to aggressively push for the collection and processing of DNA data for identification purposes in national registries. Notably, collection of DNA for identification purposes was held unconstitutional in some jurisdictions (e.g., Kenya).[47]

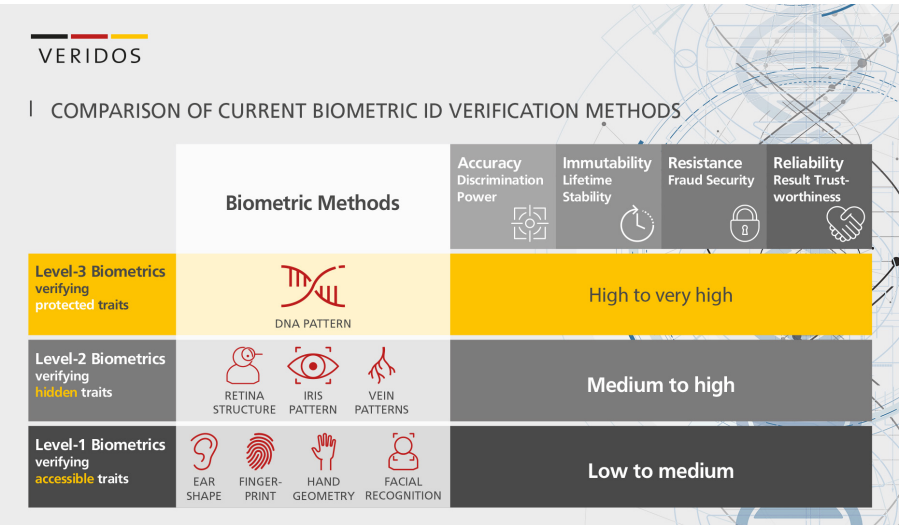

Figure 2: Veridos

Key Findings

- Rapid growth is expected in the biometric technology market, with implications for digital rights and Internet freedoms in the GIF regions.
- The public (government) sector and BFSI sectors are leading the general uptake and use of BDI solutions in the GIF regions.
- Private sector entities, such as vendors, infrastructure providers etc., have heavily invested in the BDI ecosystem, and are increasingly expanding their geographical reach in the GIF regions.
- Increased adoption across the board is attributed to digitization and technological advancements and the overall commercial benefit.
- Consumer demand for easy accessibility through digital solutions greatly influences the growth and adoption of BDI.

[47] *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR.

Trend 2: 'Technology' and the BDI Fields

Technology (tech) changes in the BDI field not only impact the manner in which individuals are identified and authenticated for varied purposes, but also influence the BDI sectors (*see Trend 1 above*) that are expanding or on the downswing.

Regional Observations

Tech Influencing the Transition from Paper-Based to Digitized ID Systems

According to GIF regional BDI reports, the most prominent transformation that tech has brought to the BDI fields is the ***steady transition away from paper-based to digitized ID systems***.[48] This tech transition is influenced by various factors, such as market demand for digitized ID services, applications and systems for efficient service delivery; e-government and digital transformation; international drives for digital ID (*World Bank, ID4D*); consumer demands for interoperable systems; innovation and research by vendors; stringent legal/regulatory frameworks and compliance environments; and human rights concerns, such as the exclusion and marginalization of vulnerable populations, amongst others.

In terms of ranking, digitized ID systems have been fully adopted in all four researched LAC countries at the foundational and/or functional levels.[49] This is followed by the Balkans, SSE Asia and Central Asian regions. In the Balkans, with the exception of North Macedonia, the rapid digitalisation of ID systems continues to be witnessed. In Central Asia, with the exception of Tajikistan, biometric digital identification systems are being used to deliver public and private services.

In the SSE Asia region, six out of seven researched countries have deployed either some form of digitized identification system with biometric features or a fully functional biometric digital ID system. Finally, five out of the seven African countries covered by the research, with the exception of the CAR and the DRC, have implemented functioning digitized systems for identification, voter registration, financial inclusion, amongst other purposes.

---

[48] The World Bank (2019). Practitioner's Guide - Types of ID Systems.
[49] Yury Myshinskiy (2020). Latin America biometrics and digital ID landscape.

Notably, **digital ID is replacing traditional physical identification documents**, leading to the increasing roll-out of ID documents such as biometric ID cards, voter cards, e-passports, and e-driving licenses. This trend is being witnessed across all five researched GIF regions, but some countries such as the CAR, due to political or operating environments, are still a long way from a full-fledged transition.[50]

Expanding Adoption of Biometrics Technologies in Digital ID Systems

According to the GIF regional BID reports, the **collection of biometrics and the expanded adoption of biometric tech has had a profound impact on digital ID systems.**[51] As technology becomes more accessible and affordable, governments and private entities in the five researched regions continue to leverage biometrics and biometric technologies for functional and foundational ID purposes, and for an expanding array of applications.

Concerningly, **details about the broader biometric tech infrastructure are extremely limited,** besides the top-level product/solution information provided by biometric tech vendors on their websites.[52] Specifically, there is scarce information at the national level about the deployment of **biometric software applications, such as automated fingerprint identification systems (AFIS) or automated biometric identification systems (ABIS)** in all five researched regions. This is despite projections of growth, signaling "USD 68.00 billion by 2030, growing at a CAGR of 23.3% from 2021 to 2030," fuelled by the government and BFSI sectors.[53]

This limited information hampers efforts by digital rights and Internet freedom advocates to monitor the evolution and impact of biometric tech, including at the hardware and software levels, and examine them against international human rights requirements or rights-respecting commitments.

Table 5: Tech and BDI

[50] Juniper Research (2023). How Digital Documentation is Revolutionising Identity in 2023.
[51] Youzec Kurp (2023). The imperative for responsible use of biometrics.
[52] In the growing AFIS market, the key biometrics vendors include Thales, Idemia, HID Global, Precise Biometrics, Innovatrics, and Suprema, Dermalog, among others. See: Allied Market Research (2022).Automated Fingerprint Identification Systems (AFIS) Market Outlook - 2030
[53] Allied Market Research (2022).Automated Fingerprint Identification Systems (AFIS) Market Outlook - 2030; World Bank (2022). A Primer on Biometrics for ID Systems.

Biometrics and Biometrics Tech in the 5 Regions

- Generally, the collection and processing of multiple biometric modalities including fingerprints, face and iris characteristics in five researched GIF regions is a rampant, entrenched practice that shows no signs of abating. This lends to the conclusion that biometrics technologies, such as ***fingerprint scanners/readers, facial recognition cameras, and iris scanners***, are being deployed at scale to capture individuals' biometrics. In a few outlier GIF countries, there are proposals or legislative requirements to capture DNA and palm print data (Zimbabwe, Bangladesh, Kazakhstan).
- In some countries in the African, Central Asian, and SSE Asian regions, the adoption of biometric technologies is a ***gradual process.*** This is attributed to factors such as financial constraints, infrastructure limitations, and limited internal capacity at the technical expertise levels, amongst others.

Sources: GIF Reports.

Additionally, **biometric tech has altered the use of biometrics in government-issued ID documentation and private sector systems in the five regions**, expanding from simply identifying and verifying individuals' identity to authenticating identities to varying degrees. This serves as evidence that biometric technologies 'dramatically expand the capabilities' of national BDI programs.[54] Illustratively, across the five researched regions, governments are issuing biometric ID cards to serve as proof of legal identity. These cards, in some regions, also enable biometric authentication permitting individuals to access state and private systems or applications, such as e-portals using their biometrics, such as fingerprints or facial scans. At the private sector level, entities continue to integrate biometric authentication for secure access to BFSI services, healthcare, and e-commerce, amongst others.

Tech Influencing Uptake of Identity Management Systems (IDMS)

Tech advancements continue to influence the uptake and shape of IDMS by state and private sector entities. One of the key considerations driving tech changes in the IDMS field is the demand from state and private entities for ***interoperability;*** a number of GIF countries are permitting private sector entities to leverage the data in their ID databases, which requires a seamless integration between systems, applications, platforms and IT infrastructure.

[54] Alan Gelb and Anna Diofasi Metz (2018). Identification Revolution: Can Digital ID Be Harnessed for Development?

In addition to the deployment of biometric technologies (*explored above*) which greatly influences IDMS uptake, other tech advancements are being deployed in GIF regions including:[55]

Holistic Biometric Identity Management Solutions (BIDMS): Across the five researched regions, a number of vendors have deployed holistic BIDMS solutions for foundational national ID systems for varied purposes, including population registration, and voter registration, amongst others. Illustratively, in the SSE Asia region, the Phillipines deployed Gemalto's BIMS for voters' verification and registration processes in 2019.[56] The Laxton Group supported Mozambique (2018-2019) to deploy an end-to-end election solution, the Central Voter Management System, including "*biometric voter registration hardware and software; a central voter management system; registration and election day supplies; election officer training; supply-chain management, and in-country project management and technical support*."[57]

Open Source Digital ID Platforms: in the Asia and African regions, there is an increasing uptake of open source digital ID platforms for foundational and functional purposes. The **Modular Open Source Identity Platform (MOSIP):** is integrated into foundational IDMS and is gaining popularity due to its avoidance of 'vendor lock-in that arises from closed, proprietary technology' and its interoperability benefits.[58] Based on the GIF reports, MOSIP is gaining popularity in the GIF SSE Asia countries. The Philippines digital ID system, the Philippine Identification System (PhilSys), has already integrated MOSIP. In 2023, the Sri Lanka government received a USD 3.8 million grant under the Indo-Sri Lanka Joint Project for the Sri Lanka Unique Digital Identity Project, facilitating the integration of MOSIP into Sri Lanka's national ID systems.[59]

Mobile Biometrics: Taking advantage of the widespread adoption of mobile devices worldwide, ***IDM systems have adapted to support mobile authentication***. Specifically,

[55] Other tech advancements that are not explored in this report but are influencing changes in the BDI fields include cloud computing, Internet of Things (IoT) devices, amongst others.
[56] Chris Burt (2019). Gemalto launches biometric identity management solution for foundational national systems; Stephen Mayhew (2019). Philippines selects Gemalto biometric technology to verify voters in upcoming elections.
[57] Laxton (20). Mozambique's Highest-Ever Voter Turnout: Case Study.
[58] MOSIP. Resources.
[59] Chris Burt (2023). MOSIP ready for next phase after building up digital ID ecosystem; MOSIP (2021). The Philippine Statistics Authority (PSA) crosses critical milestones for the Philippine Identification System (PhilSys); MOSIP (2021). MOSIP enters partnership with Sri Lanka on digital ID system; William McCurdy (2023). Procurement begins for Sri Lanka's national digital ID.

mobile-based identity and biometrics solutions, including mobile biometrics and MFA, enable secure access to services on-the-go. Across the GIF region, mobile-based biometric solutions are supporting faster ID enrollment and verification, enabling greater inclusion and accessibility to services. Mobile biometrics uptake is **most prevalent in the LAC, African, Central Asian, and SSE Asia regions.** In the LAC region, countries such as Bolivia and Colombia have integrated mobile biometrics into their digital ID systems. In the SSE Asia region, the use of mobile biometrics is a growing trend in Nepal and the Philippines to extend identification services to remote and underserved areas where travel costs are a barrier to ID uptake. In Tanzania, the government leverages mobile network operators (MNOs) capacities to deploy mobile-based digital identity.

Significantly, tech advancements in the BDI fields are gradually challenging conventional narratives about what constitutes a 'safe and secure' identity management solution, bringing the **centralized versus decentralized/distributed IDMs** conversation to the fore. Centralized IDMs are extremely popular with governments in five researched regions. On the efficiency front, centralized IDMS are preferred as they enable governments to efficiently manage and process large volumes of identity data for vast populations using centralized repositories, such as central databases. On the service delivery front, centralized IDMS are touted as enabling users' seamless access to various services using a single identity, consequently reducing a duplication of efforts and providing a unified user experience. **Single sign-on (SSO) solutions (including those integrating biometrics) and passwordless authentication options** are presented as facilitating seamless user experiences, with SSOs "*[simplifying] the login experience by giving users access to multiple applications with a single login*."[60]

However, centralized IDMS pose significant privacy risks and are generally known to present a **single point of failure (SPOF)** because all identity data and authentication processes are concentrated in a central repository (database or system). This means that malicious actors can exploit a single vulnerability in the IDMS, such as poor security measures, infrastructure dependency or insider threats, to cripple or prevent access to a country's or entity's IDMS.

[60] Daniel Lu (2018). Fact of Fiction: SSO Creates a Single Point of Failure, so It's Less Secure.

Centralized ID databases, an SPOF in itself, are extremely attractive for data breaches and unauthorized access due to the sensitive ID data contained therein.

Due to these privacy, security and user control perils, entities are encouraging a transition away from centralized IDMS to **decentralized IDMS leveraging newer technologies, such as distributed ledger technology, including blockchain technology and other ledger systems such as Hashgraph.**[61] Blockchain technology, "*a decentralized, distributed ledger that stores the record of ownership of digital assets*,"[62] is encouraging uptake of decentralized IDMS by leveraging its architecture to distribute ID data across multiple network nodes. This is argued to be a more privacy-respecting and secure alternative for digital ID management that centralizes privacy and user control.[63]

This transition is being encouraged by international institutions, such as the Digital Identity Initiative (DII) of the World Economic Forum (WEF), and decentralized ID vendors, such as Hedera Hashgraph.[64] A report by Frost and Sullivan noted that the integration of blockchain tech with biometrics will result in the "establishment of a **single-token digital identity** for individuals."[65] Notably, while tokenisation is growing in other regions, the **five researched GIF regions are still heavily reliant on identifiers**, such as unique ID numbers.[66]

The other emerging tech alternative to centralized IDMS are **self-sovereign identity (SSI) systems.** SSI systems leverage decentralized identifiers and blockchain to enable individuals to control their identity information and share it securely with trusted parties.[67]

---

[61] Distributed ledger technology refers to "a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants. A 'blockchain' is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called "blocks" that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner." See: International Bank for Reconstruction and Development/ the World Bank (2017). Distributed Ledger Technology (DLT) and Blockchain; World Economic Forum (2023). Reimagining Digital ID 2023.pdf

[62] Sam Daley (2022). What Is Blockchain Technology? How Does It Work?

[63] Ayang Macdonald (2023). World Economic Forum panel pushes for blockchain-based decentralized digital ID.

[64] Brett McDowell (2023). How we create an international framework for privacy-preserving digital ID; Hedera. Decentralized Identity on Hedera.

[65] Frost & Sullivan (2021). Global Digital Identity Solutions Growth Opportunities.

[66] "Tokenization substitutes a sensitive identifier (e.g., a unique ID number or other PII) with a non-sensitive equivalent (i.e., a "token") that has no extrinsic or exploitable meaning or value. These tokens are used in place of identifiers or PII to represent the user in a database or during transactions such as authentication. The mapping from the original data to a token uses methods—e.g., randomization or a hashing algorithm—that render tokens infeasible to reverse without access to the tokenization system." See: The World Bank (2022). Practitioner's Guide - Tokenization.

[67] OKTA (2022). Self-Sovereign Identity (SSI): Autonomous Identity Management.

Key Findings:

- Tech has facilitated a **steady, ongoing, transition away from paper-based to digitized ID systems across all five GIF regions covered in the research.** The adoption of digital ID for the issuance of ID documentation, such as biometric ID cards and e-passports, is an emerging trend.
- The collection of biometrics by state and private entities is an entrenched practice, relying on the deployment of biometric technologies. The most commonly deployed biometric tech include fingerprint scanners/readers, facial recognition cameras, and iris scanners, to capture fingerprint, facial and iris biometric.
- Despite governments and the BFSI sector fuelling the growth of the biometric tech market in the five regions, there is scarce information about biometric tech infrastructure at the national level.
- Across the five researched regions, biometric tech is expanding the capabilities of national BDI programs, as evidenced by the increasing transition towards biometrics authentication from simply identification/verification.
- At a regional level, all researched regions evidence an adoption of biometric and digital ID technologies for varying purposes ranging from national identification, election management, voter registration, border control, law enforcement, and service delivery, amongst others. The LAC region has the highest uptake of tech for BDI programs, including identity access, management and control.

Trend 3: Legal Frameworks and BDI Fields

To ensure the promotion of the principle of the rule of law, states are obliged to develop and implement a ***robust, proportionate, legitimate, and necessary legal framework*** (i.e., policies, laws, regulations, codes of practice, etc.) for BDI systems. Notably, legal frameworks regulating BDI systems are critical for (i) striking a balance between the implementation of BDI systems and addressing their potential impact on individuals' and communities' human rights, (ii) boosting innovation and promoting privacy and security,[68] (iii) preventing the misuse of BDI systems by both state and private actors, and (iv) providing grievance and redressal mechanisms to BDI users in case of data breaches or violations of their rights, amongst others.[69]

This legal framework is integral for providing a ***legislative basis*** for the existence and operation of BDI systems, ensuring ***legal protection*** for the system and ***legal recourse*** for users, outlining the ***roles and responsibilities*** of relevant actors, ***delineating liability***, and creating appropriate governance mechanisms.[70] The World Bank succinctly categorizes the legal framework underpinning ID systems into two categories, namely:

1. *"Enablers — directly define and govern the ID system, including its design, management, operation, and relationships with stakeholders and other systems.*
2. *Safeguards — address potential risks surrounding the ID system, including those related to data privacy, security, and non-discrimination."*[71]

Integral to the BDI legal framework are **legally-mandated state bodies or entities** (i.e., ministries, authorities, regulatory bodies, etc.) **charged with fostering public trust and confidence in deployed digital ID systems and biometric solutions.**[72] In GIF countries,

[68] Christine Horton (2022). Why biometric regulation needs to be risk-based and proportionate to use-cases.
[69] Yesha Tshering Paul (2020). An Evaluation Framework for Digital ID.
[70] World Bank Group and Center for Global Development (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.
[71] The World Bank (2022). Practitioner's Guide - Legal Framework.
[72] Other responsibilities include: (i) setting industry standards and best practice guidelines for BDI implementation to ensure uniformity and interoperability, (ii) enforcing sectoral BDI laws on data protection, consumer protection, amongst others, (iii) promoting intra-agency, regional and international collaboration, (iv) promoting oversight and monitoring compliance of BDI systems, vendors, service providers, and government agencies with relevant regulations, including conducting audits and investigations, (v) mediating BDI disputes, (vi) developing BDI policies, (vii) engaging in public awareness and education campaigns to educate and sensitive citizens about BDI programs and systems, rights, and technologies.

government agencies or authorities are charged with the **issuance and validation of BDI documentation,** including biometric ID cards, e-licences, e-passports, amongst others, and ensuring their authenticity and accuracy. Illustratively, in Tanzania, the National Identification Authority (NIDA) is tasked with identifying and registering citizens and resident foreigners, and issuing national ID cards.

These entities are also **tasked with managing BDI databases,** such as electronic civil registration and vital statistics (CRVS) registers, population databases and national ID databases. For instance, in the Philippines, SSE Asia, the **PhilSys registry** is owned, maintained, and administered by the Philippine Statistical Authority (PSA).[73] The **PhilSys registry** is the database that contains all registered information of ID holders, all application form information, and any updates made by ID holders.[74] In Ecuador (LAC region), the foundational ID system consists of three centralized databases, including births and deaths, civil registration, and identification. These databases contain biometric data and are managed by the *Dirección General de Registro Civil, Identificación y Cedulación* (DIGERCIC, or the *General Directorate of Civil Registration, Identification, and Identification Card Issuance,* or Civil Registry).[75]

Table 6: Key Considerations for BDI Entities

Key Considerations
BDI legal frameworks place obligations on charged entities (government, private sector players, vendors, etc.) at the deployment, access, implementation or maintenance levels to pay specific attention to: ○ **Prioritizing BDI Goals and Purposes:** BDI systems must strictly adhere to the goals, purpose and vision outlined, unless compelling changes are required. Ideally, any changes to the BDI goals or purposes should be aligned with the public interest. ○ **Upholding Voluntary Participation:** Users should not be compelled to participate in BDI systems, and alternative forms of identity proof should be provided to avoid creating an unnecessary dependence on one identity credential. Further, alternatives for identity verification should be available to those who choose not to provide or use biometrics.

[73] Republic of the Philippines. Philippine Statistics Authority.
[74] *Ibid.*
[75] Dirección General de Registro Civil Identificación y Cedulación. Trámites y Servicios Institucionales. See: https://www.gob.ec/dgrcic.

- **Facilitating User Rights and Remedies:** The rights of BDI users should be respected, promoted, protected, and fulfilled at every stage of BDI deployment.
- **Safeguarding Privacy and Data Protection:** BDI systems must adhere to data protection laws and policies, ensuring that individuals' personal information is collected, stored, and processed in line with data protection principles (especially data minimisation and purpose limitation), informed consent, the rights of data subjects, and in compliance with privacy laws.
- **Promoting Security and Authentication Measures:** BDI systems must be accompanied by robust security and authentication mechanisms to safeguard the integrity of the personal and biometric data collected, and prevent unauthorized access or misuse.
- **Incorporating Transparency and Accountability:** BDI systems should be transparent about identity management processes and infrastructure, data practices, resource allocation, amongst others. Entities or stakeholders that fail to adhere to the legal framework must be held accountable relying on civil and/or criminal procedures.
- **Fostering Non-Discrimination and Inclusion:** BDI systems should be designed and used in a manner that prevents discrimination and promotes inclusion, avoiding biased practices or discriminatory technologies.
- **Promoting Interoperability and Standards:** Responsible entities should ensure that the BDI system is interoperable with other relevant systems and IT infrastructure, following recognized standards for data exchange and integration.
- **Addressing Law Enforcement and Surveillance Concerns:** Legal frameworks must establish clear guidelines for the use of BDI data (personal and biometrics) for law enforcement, monitoring, or surveillance activities to prevent abuse and protect individual rights.
- **Supporting Periodic Audits and Assessments:** Regular audits and assessments (including human rights impact assessments) of the BDI system's compliance with the legal framework should be conducted to identify vulnerabilities and areas for improvement.
- **Promoting Independent Oversight:** BDI systems should be independently monitored to ensure that all stakeholders are complying with the legal framework.

Sources: Principles on Identification. Open Government Partnership. World Bank. The Centre for Internet & Society. World Economic Forum.

Regional Observations

Analysis of BDI Legal Frameworks

Across the five GIF regions, all 27 GIF countries reviewed have either enacted **civil registration and vital statistics (CRVS) laws, population registration laws, or identification laws**. These laws ***mandate*** the collection of vast amounts of personal data for use by the state, and in some regions, private sector entities. To reflect evolving ICT priorities, digital economy and transformation drives, and e-government and e-business programmes outlined in **country-level policy documents prioritizing BDI initiatives**, GIF countries have either:

- Amended or reviewed existing CRVS, population, and ID laws to facilitate the adoption of digital IDs, or
- Repealed old laws and enacted entirely new laws to accommodate the use of digital identities.

The **prioritization of individuals' privacy and personal data protection** has gained traction in the overarching BDI legal framework. It is important to clarify that the enactment of the European Union's General Data Protection Regulation (GDPR)[76] has **spurred GIF countries' adoption of stand-alone data protection laws.**

However, BDI data collection for identification, CRVS, and population registration purposes predates the GDPR. Based on this, it is clear that GIF countries were already centering the protection of individuals' privacy and personal data protection as prescribed in national constitutions and sectoral laws. This was informed by sensitivities around personal and sensitive data collection.

Based on the GIF reports, **18 out of the 27 researched GIF countries have enacted stand-alone laws regulating the collection and processing of personal and/or biometric data**, including data contained in BDI databases.

[76] European Union (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).

Table 7: GIF Countries with Data Protection Laws

Regional Breakdown

- **Africa:** 4 countries, including Angola, Tanzania, Uganda, and Zimbabwe.
- **The Balkans:** 5 countries, including Albania, Bosnia & Herzegovina, Kosovo, North Macedonia, and Serbia.
- **Central Asia:** 4 countries, including Kyrgyzstan, Tajikistan, and Uzbekistan.[77]
- **Latin America and the Caribbean:** 2 countries, including Brazil and Ecuador.
- **South and Southeast Asia:** 3 countries, including Indonesia, Philippines, and Sri Lanka.

Source: GIF reports.

Complimenting these laws are ***sectoral laws and regulations*** that are essential to form a robust and comprehensive legal framework for BDI systems. The sectoral laws identified in the GIF reports include those relating to consumer protection, cybersecurity, election management, electronic transactions, immigration, law enforcement, mobile equipment registration, privacy, security and surveillance, SIM card registration, amongst others. Notably, in the Balkan region, the prevalence of sophisticated ransomware attacks targeting BDI systems operated by businesses and public institutions is galvanizing legal and regulatory efforts to address these cybersecurity and data protection challenges.

Legal Challenges and Court Rulings

The challenges to BDI legal frameworks demonstrate that concerns have been raised about their validity or constitutionality, either due to inadequate safeguards or the potential risk of violating established standards, principles, rights or constitutional provisions. Legal challenges brought against BDI systems typically revolve around allegations of human rights violations, civil rights infringements, constitutional breaches, a review of administrative action or inaction, and criminal complaints, amongst others.

One of the cross-cutting challenges observed in the five researched GIF regions is the **inadequacy of BDI legal frameworks** and the **provision of broad penalties for access to digital data for 'law and order purposes' resulting in mission creep.**

[77] One country name is withheld.

In the Africa region: the GIF regional report noted a lack of clarity and precision in laws governing personal identity and biometric data, leaving room for ambiguity and misinterpretation. The report notes the existence of outdated legal and institutional frameworks for civil registration which do not cater for BDI systems in the CAR and Mozambique, whose laws were last updated in 1964 and 1967, respectively. Further, some countries last amended their civil registration laws almost a decade ago, meaning these may still not be optimized for new BDI programmes (Angola, DRC, Tanzania and Uganda).

The privacy and data protection landscape in the GIF African countries is still developing. Notably, two out of the seven researched GIF countries (CAR and Mozambique) do not have stand-alone, comprehensive data protection laws. Further, two GIF countries (Tanzania and Zimbabwe) have not yet fully operationalised their data protection laws, whereas one GIF country (Uganda) has not yet established an *independent* data protection authority. In this region, it was concluded that the ongoing biometric data collection processes are not subject to independent oversight.[78] Without a robust data protection law, citizens may not trust how their data is handled and may be skeptical of how their personal data is being used.

Other issues noted in the report include (i) limited accountability mechanisms, which make it difficult to hold government and private entities accountable for misuse of personal data, (ii) lack of transparency and public participation in the development and implementation of digital identity systems undermining trust and confidence in the system, and (iii) inadequate measures to ensure data security, which puts personal information at risk of theft or misuse. (*Africa regional report*)

In the Balkans region: focusing on the intersection between BDI systems and cybersecurity, the GIF regional report noted that enforcing outdated or unenforceable laws is a core challenge, given the rapidly evolving digital landscapes. Further, the report revealed the 'need to support law enforcement agencies and regulators with additional resources, capacity-building support, and clear jurisdictional frameworks for pursuing and prosecuting cybercriminals effectively.' It was noted that the 'lack of sufficient investment in cybersecurity

[78] In Uganda, while the Personal Data Protection Office claims to be an independent office, we note that it is situated under the National Information Technology Authority, Uganda (NITA-U). See: ARTICLE 19, KICTANet and Pollicy (2021). Unseen Eyes, Unheard Stories: Surveillance, Data Protection and Freedom of Expression in Kenya and Uganda during COVID-19.

measures… leads to inadequate protection of critical infrastructure, businesses, and citizens from cyber threats.' All five researched GIF countries in the region have enacted stand-alone data protection laws, but the 'enforcement of these laws and overall awareness about data protection and privacy remain inconsistent across the region'. (*Balkans regional report*)

In the Central Asia region: the GIF regional report called for a review of biometric registration laws to address gaps, clarify legal frameworks for data protection, and ensure compliance with international standards. Specifically, this includes (i) establishing strict regulations and penalties for misuse or unauthorized access to biometric data (ii) enhancing the interoperability of biometric national ID cards, particularly for regional travel, (iii) promoting transparency and accountability in the collection, storage, use, and transfer of biometric data, (iv) clearly defining the term 'biometric data' to ensure consistency in its regulation and management, (v) addressing operational challenges faced during implementation, (vi) strengthening enforcement mechanisms to ensure compliance with personal data protection laws, including increasing penalties for non-compliance, conducting regular audits, and establishing dedicated authorities or agencies with sufficient resources and authority to enforce data protection laws effectively. (*CA regional report*)

In the LAC region: the GIF regional report noted the need to amend identity laws to make the collection of biometric data optional and delink individuals' access to public and private services from the mandatory provision of biometric data. Further, the report decried the ambiguity latent in the 'digital ID' concept which enables LAC countries to continuously expand the legal remit of their digital ID databases beyond identification to encompass any purposes marked as a state need, including migration control, and the delivery of social security programs. The failure to impose limits on the purpose and scope of digital ID systems prevents stakeholders, such as CSOs, charged with ensuring transparency, accountability, and the protection of individuals' rights, from assessing the level of threats and risks to human rights against pre-set limits. (*LAC regional report*)

In the SSE Asia region: the GIF regional report observed that the 'deployment of BDI systems was not accompanied with the enactment of comprehensive personal data protection laws or

comprehensive governing laws for identification systems.' The report noted that some of the established legal frameworks lack clearly-defined provisions to properly collect and store personal and sensitive data, in a transparent and accountable manner. The main issues noted in many of the existing policies and regulations were centered around the collection and management of people's biometric data, accountability systems, and grievance redressal systems.' Further, the report observed that the expansion or reduction of national ID data points (i.e., the *collection of personal or demographic data*) in countries like Sri Lanka is designated as an executive, rather than a legislative, function. While this is common in other digital ID systems around the world, it is still a concerning practice, because it permits the addition of new categories of data to be collected without undergoing the legislative process. (*SSE Asia regional report*)

The GIF reports reference **in-region and cross-jurisdictional legal challenges** impacting the validity and constitutionality of BDI systems.[79] This trend analysis draws attention to two cases filed in Kyrgyzstan, the Central Asia region,and the Philippines, SSE Asia, reflecting the scope of legal challenges affecting BDI legal frameworks and systems (*see table 8 below*).

Table 8: Court Rulings Impacting BDI Legal Frameworks

Central Asia Spotlight – Validity of Law Mandating Biometric Registration

The constitutionality of Kyrgyzstan's law on biometric registration of citizens (2014) (last amended in July 2022)[80] was challenged in November 2014 before the Constitutional Chamber of the Supreme Court.

- Core Challenge: violation of Kyrgyzstan's constitutional provisions on the inviolability of the person and private life. Notably, mandatory biometric registration implies the possibility of coercion during the submission of biometric data, which carries a risk of physical violence. Further, the applications argued that the mandatory requirement for all biometric data carriers to provide their biometric data contradicts the consent principle.
- Finding: In September 2015, the court concluded that the requirement of mandatory biometric registration of citizens is aimed at satisfying the interests of

[79] The cross-jurisdictional challenges are succinctly summarized here: Centre for Internet and Society, India (2020). Judicial Trends: How Courts Look at Digital ID Programs, pp. 18-20.
[80] On Biometric Registration of Citizens of the Kyrgyz Republic. Erkin-Too § 56 (2014). http://cbd.minjust.gov.kg/act/properties/ru-ru/205357/15

both citizens and society. The registration was held to be within the limits of constitutional requirements, while such restriction of the right is proportional.

Sources: Akbarovich v. Dzhumakovna. Central Asia Regional Report.

SSE Asia Spotlight – Validity of BDI Laws

Prior to the enactment of the Philippine Identification System Act in 2018, the government had attempted to introduce laws governing different BDI systems on two occasions. These laws were challenged as follows:

- **1996:** an attempt to legislate on a computerized national ID reference system with biometrics via Administrative Order No. 308 (AO 308) was **struck down by a divided Supreme Court** on two grounds: 1) a violation of the constitutional right to privacy, and 2) exclusive power of Congress to institute a national ID.
- **2005/2006:** an attempt to introduce a Unified Multi-Purpose ID system under Executive Order No. 420 (EO 420) was challenged in Court but found to be valid. The constitutionality of EO 420 was contested for infringing on the right to privacy and usurping legislative functions by the executive branch of the government. In dismissing the petition, the court held that:
  - "Issuance of EO 420 does not constitute usurpation of legislative power";
  - The right to privacy does "bar the adoption of reasonable ID systems by government entities." Specifically, the right to privacy was not infringed because the EO 420 "narrowly limits the data that can be collected, recorded and shown compared to the existing ID systems of government entities. EO 420 further provides strict safeguards to protect the confidentiality of the data collected, in contrast to the prior ID systems which are bereft of strict administrative safeguards."

Sources: SSE Asia regional report. Inquirer. Manila Supreme Court.

Key Findings

- States are obliged to develop and implement a robust and proportionate legal framework for BDI systems consisting of policies, laws, regulations, codes of practice etc.
    - All 27 researched GIF countries have either amended existing civil registration and vital statistics (CRVS) laws, population registration laws, or identification laws, or enacted new laws to accommodate the introduction of a digitized ID system.
    - In some GIF countries, this was triggered by evolving ICT policy priorities, or digital economy and transformation policy changes. These changes are detailed in country-level policy documents prioritizing BDI initiatives.
    - Sectoral laws and regulations on consumer protection, cybersecurity, privacy, electronic transactions, amongst others, complement these BDI laws.
- 18 out of the researched 27 GIF countries have enacted a stand-alone law on the protection of personal data that applies to BDI systems. The remaining countries rely on sectoral laws, which are inadequate to comprehensively protect individuals' data.
- The legal framework governing BDI systems is largely dependent on context. For example, countries in the Africa region, such as the CAR and DRC, that have experienced political instability generally have weaker legal frameworks.
- The inadequacy of legal frameworks to robustly and comprehensively govern BDI systems is a cross-cutting issue raised in all five researched GIF regions.
- Documented legal inadequacies have triggered court challenges about validity or constitutionality of BDI legal frameworks. These have been centered on the mandatory nature of biometric data collection and the risk to the constitutional right of privacy (*these court cases are not exhaustive with numerous legal challenges being observed in non-GIF countries).*

Trend 4: 'Concerns' in the BDI Fields

The implementation of tech-centric BDI systems, incorporating emerging and advanced biometric and digital ID technologies, coupled with heightened awareness among BDI users of their rights and associated risks, has provided ***depth and complexity to prevailing concerns within the BDI ecosystem, rather than altering the nature of the concerns***. The concerns explored below are a cross-cutting feature in all researched GIF regions, in varying degrees, tempered by regional and in-country priorities amongst stakeholder groups and contextual realities.

As observed by Canadian privacy regulators, *"[t]he benefits of a digital identity ecosystem must not come at unacceptable consequences, such as: the collection of personal information beyond that which is necessary, proportional or justified; increased risk of discrimination; heightened incidence of identity theft, fraud and other harms; or diminished roles for individual users."*[81] To this end, states and private sector entities deploying digital ID systems must ensure that human rights risks/concerns and digital ID principles are respectively mitigated and integrated throughout the digital ID lifecycle, at the design, operation and ongoing evolution stages.[82]

Privacy, Security, and Ethical Concerns

As societies embrace digital transformation and governments and organizations increasingly adopt biometric identification methods, the potential risks to individual and communal privacy, as well as the safety and security of BDI systems occupy a central role in the BDI field. Notably, privacy, security and ethical concerns will continue to share the future of BDI, given the inevitability of technological advancements and the emergence of attendant challenges. While BDI systems and technologies present numerous benefits, the need to address privacy and security risks and ensure robust security safeguards and measures is crucial.

The Biometrics Institute Privacy Guidelines and the ID4D Principles on Identification urge entities to (i) 'protect user privacy and control through system design, and (ii) build trust in

[81] Office of the Privacy Commissioner of Canada (2022). Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight.
[82] Office of the Privacy Commissioner of Canada (2022). Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight; World Bank Group and Center for Global Development (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.

BDI systems by safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.'[83] In the researched GIF countries, the increasing adoption of BDI technologies and systems in various sectors continues to raise concerns about the protection of individuals' personal data and the security of BDI systems. This is due to the growing reality of privacy breaches and cyber attacks on state and private BDI systems.[84]

Table 9: Cyber Attacks in the Balkans Region

Balkans Spotlight – Cyber Security and BDI

- The Balkans GIF regional report reported a significant surge in cyberattacks, particularly phishing and ransomware, followed by exploit-based attacks, malware and DDoS attacks, in all five Balkan countries between 2020-2023.
    - Phishing attacks: cybercriminals are targeting individuals and organizations to obtain sensitive personal information with an impact on individuals' right to privacy and data protection.
    - Insider threats or employee negligence: pose significant risks in all researched GIF countries in the region. Specifically, individuals within an organization with access to sensitive information and systems were identified as a vulnerability.
- The most targeted entities included the public sector, banks, and individual citizens, with malicious actors exploiting 'vulnerabilities in the digital infrastructure and security measures of both private and public entities.' Core challenges to the development and implementation of robust security measures included limited resources, lack of skilled cybersecurity professionals, and insufficient investments in technology and infrastructure.
- The GIF regional report underscored the importance ofraising cybersecurity awareness and education among the general population and organizations; strict access controls; stringently enforced security protocols and policies; stronger infrastructure protection, amongst others.

Source: Balkans Regional Report.

Notably, BDI users increasingly require assurance that their personal and biometric data is being legally collected and processed in a lawful, necessary, legitimate, ethical, and responsible manner. Concerningly, the collection of these vast data points on individuals raises fears of monitoring and surveillance, which can have a chilling effect on other human

[83] Biometrics Institute (2023). Privacy Guidelines for biometrics; World Bank Group and Center for Global Development (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.

[84] In 2018, India's biometric ID database, the Aadhaar, was "breached via a security gap at a state-owned organization. As a result, every registered Indian citizen had their information leaked. Their identity numbers, names, bank details, and other personal information were put up for sale on WhatsApp for less than £6." Similarly, in 2021, Estonia's Identity Documents Database (KMAIS) was breached via an exploitation of a "government photo transfer service vulnerability to download ID scans of 286,438 Estonians." See: Masha Komnenic (2023). 98 Biggest Data Breaches, Hacks, and Exposures; Sergiu Gatlan (2021). Estonia arrests hacker who stole 286K ID scans from govt database.

rights, such as the ability of individuals' to express themselves freely online without the fear of profiling and tracking.

On the ethical front, there has been a widespread push from entities such as the ID2020 and the WEF to conceptualize "ethical approaches to digital identity," particularly at the standards level, as stakeholders push for more decentralized forms of BDI.[85] Ethical concerns impacting BDI have evolved with technological advances and widespread adoption. Key areas of ethical debate have evolved from focusing on transparency, accountability, inclusivity, and privacy, to encompass surveillance, consent, data minimisation, data ownership and control, cross-border data sharing, the integration of ethical standards into emerging technologies, algorithmic bias and accountability, and examining long-term societal implications, amongst others. Addressing these concerns requires proactive measures, including robust regulations, transparent practices, audits and assessments, and ongoing dialogue among stakeholders.

Regional Observations

Across all five researched GIF regions, concerns about the **misuse of personal and biometric data**, including the potential for this data to be used for **unlawful tracking and surveillance purposes or to violate individual privacy**, were identified as key concerns. This reveals that entities are not promoting ethical standards that require a proportionate balance between individuals' rights and security and law enforcement needs.

Expanding on this challenge, the **issue of tech-vendor and supplier dominance** was flagged in the LAC, Africa and SSE Asia regions, raising concerns of **vendor lock-in, potential biases in tech, data sovereignty, and data security concerns**. In the LAC region, the GIF regional report noted that there is **no distinction between the suppliers of biometric technologies** and the suppliers of surveillance technologies. Similarly, in the SSE Asia region, Cambodia's upcoming facial recognition project in collaboration with Local Conglomerate HSC Group has also come under scrutiny. This is due to the fact that HSC Group has been involved in various government identification and surveillance projects, such as running the current system for national ID cards, printing passports and providing border checkpoint technology.[86]

[85] ID2020. Manifesto; World Economic Forum (2023). Reimagining Digital ID: Insight Report; Biometrics Institute (2019). Ethical Principles for Biometrics.
[86] Fiona Kelliher (2023). Cambodian Facial Recognition Effort Raises Fears of Misuse.

In the Africa region, the GIF country reports document a **heavy reliance on external expertise provided by foreign BDI vendors and tech providers**. In Uganda and Zimbabwe, governments engaged private vendors to provide a biometric national identity card system *(Mühlbauer ID Services GmbH, a German company*) and a National Biometric Database for the production of e-passports, national identity cards and birth certificates (*unknown entity*). In the CAR, local activists have raised concerns about foreign corporations' control of locals' identities, citing the delegation of the ID prerogative to a foreign company as impacting data and national sovereignty.[87]

Further, the use of **centralized databases** in a majority of the GIF countries remains a central privacy, security and ethical concern. Significantly, both government and private sector **security measures and safeguards for these databases were found to be either weak or inadequate,** as evidenced by reports of data leaks. Concerningly, data breaches are not a one-off occurrence, with individuals being exposed to indefinite risks of identity theft, phishing attacks, and other malicious cybercrimes. These weaknesses reveal that GIF countries are not adopting ethical considerations that mandate entities to ensure the protection, respect and promotion of individuals' privacy rights.

Table 10: Summary of Key Privacy, Security and Ethical Concerns in GIF Regions

Region	Key Concerns
Africa	**Misuse of personal and biometric data in contravention of purpose limitation**, resulting in data protection violations, such as unsolicited targeted electoral messaging, and privacy risks and infringements (CAR, Mozambique, Zimbabwe) **Surveillance concerns** due to: • Mass data collection exercises under BDI programs coupled with advanced real-time monitoring capacities. This has resulted in the state's enhanced capacity to engage in real-time communications surveillance and tracking targeting journalists, activists, student association leaders, opposition politicians (Tanzania, Uganda, Angola, Zimbabwe) • Linkage of ID databases with private sector entities (e.g., telecommunications companies) without appropriate privacy policies (Tanzania)

[87] RFI (2020). Centrafrique: Al Madina, la société qui pose question à Bangui.

	Use of c**entralized databases posing risks for the safe storage of critical and sensitive data**, such as biometric data. **Collaboration with foreign suppliers** impacting data and national sovereignty
Balkans	Documented **cybersecurity concerns** targeting BDI infrastructure vulnerabilities at the public sector, banking, and individual citizen levels
Central Asia	Privacy concerns stemming from **mandatory biometric registration,** including **inappropriate data handling procedures** observed in at least two out of the four researched GIF countries: • Kyrgyzstan: inappropriate handling of biometric data resulting in loss of biometric data contained in stolen computers and lost USB flash drives • Kazakhstan: incidents of personal data leaks from the Central Election Commission's database and a shared medical information database
Latin America and the Caribbean	**Collection and processing of biometric data** in one or multiple digital ID databases without prior human rights assessment Use of **centralized databases** posing risks for the safe storage of critical and sensitive data, such as biometric data Similarity between **vendors supplying surveillance technologies and BDI technologies** to LAC governments **Ambiguity in BDI concept resulting in mission creep** (i.e., expansion of legal remit of digital ID databases beyond identification to encompass any purposes marked as a state need)
SSE Asia	**Collection and processing of personal and biometric data** permitting privacy violations *at scale* Concerns of **unauthorized data access** framed against reported leaks of citizens' personal identification data in at least two out of the seven researched GIF countries • Philippines: leak of "over 1.2 million records... [containing] highly sensitive personal information such as passports, birth and marriage certificates, drivers' licenses, academic transcripts and security clearance documents"[88]

[88] Davinci Maru (2023). Over 1.2M records from NBI, PNP, other agencies leaked, firm says.

	• Bangladesh: leak of "personal information of citizens, including full names, phone numbers, email addresses and national ID numbers"[89] Concerns of **weak and insufficient security systems** for digital ID infrastructure and poor cybersecurity measures posing a risk to data protection and data privacy.
	Source: GIF Reports.

Accountability and Transparency Concerns

Accountability and transparency are mutually-reinforcing principles that impact governance processes, specifically affecting decision-making and oversight.[90] The principle of accountability imposes responsibility on BDI stakeholders, including states, private entities and tech vendors. Notably, the ID4D Principles note that there should be "clear accountability and transparency around the roles and responsibilities of identification system providers," with governments retaining the "ultimate accountability for legal identification."[91]

The principle of transparency facilitates "inclusive and collaborative stakeholder engagement… [supporting] alignment with users' needs and expectations."[92] Transparency is closely linked to freedom of information and the right to access information held by both state and private entities, enabling stakeholders to hold BDI system providers and operators accountable for a range of issues, such as resource misappropriation, unlawful practices such as mission creep, data mishandling and poor processing activities, algorithmic bias, vendor lock-in, anti-competitive practices, abuse of power, amongst others.[93]

Based on the foregoing, these two principles are a gateway for the promotion and realization of a wide range of human rights, such as the right to privacy and access to information, and other BDI principles such as participation and inclusion. Further, these two principles are integral to the promotion of trust in BDI systems, enabling stakeholders, including BDI users,

[89] Lorenzo Franceschi-Bicchierai (2023). Bangladesh government website leaks citizens' personal data.
[90] World Bank Group and Center for Global Development (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.
[91] World Bank Group and Center for Global Development (2017). Principles on Identification for Sustainable Development: Toward the Digital Age.
[92] OECD (2023). Recommendation of the Council on the Governance of Digital Identity.
[93] UN Office of the High Commissioner for Human Rights (2022). Freedom of opinion and expression : report of the Office of the United Nations High Commissioner for Human Rights; UNESCO. Right to Information; ARTICLE 19 (2012). International standards: Right to information.

to participate in the design and implementation of BDI systems that heavily rely on their personal and biometric data, thereby promoting data ownership and control.

Regional Observations

Across all five researched GIF regions, **gaps in accountability and transparency mechanisms for the regulation of BDI systems, technologies and procedures were** major limitations impacting the integration of the accountability and transparency principles into deployed BDI systems.

Specifically, in the SSE Asia region, the GIF regional report noted gaps in the legal frameworks providing grievance, redressal, and oversight mechanisms. The report calls for the 'creation of accountability and grievance redressal mechanisms to (i) ensure proper oversight over entities collecting identification data, (ii) clearly delineate relevant parties' responsibilities, (iii) provide individuals with mechanisms for filing and resolving ID-related complaints, (iv) create mechanisms to ensure transparency and protect citizen data from unauthorized access or misuse, including constituting *independent* data protection authorities and equipping them with sufficient resources.'

These challenges were also observed in the Africa region, with the GIF regional report highlighting that 'oversight institutions face challenges such as insufficient budgetary allocations, capacity gaps, and limited skilled human resources to effectively discharge their mandates, including outreach and awareness to the public and stakeholder engagement.'

Building on this central challenge, the Africa, LAC, and SSE Asia regional reports noted the **opaque, ongoing collaboration between governments and third-party private entities** impacting accountability and transparency principles.[94] Concerningly, the provision of non-transparent access rights to BDI systems to providers of BDI infrastructure or in-country private actors raises three central concerns. These include the failure to provide a clear, definitive legal basis for public-private partnership or collaboration agreements between state entities and private sector players, raising queries about public scrutiny and oversight.

[94] This concern intersects with the first concern.

The second concern revolves around the limits imposed on corporations' access to individuals' personal and sensitive data, revealing the poor delineation of the roles and responsibilities of ID system stakeholders. This concern also impacts data privacy and security, as in many cases, information on who has access to the data, for how long, and for what purposes is not clearly spelled out in publicly-accessible transparency materials, such as transparency reports, disclosure documents or even privacy policies or notices.

The third concern is centered on the scarce information on the **broader biometric tech infrastructure (*see trend 2 above*).** In the LAC region, the GIF regional report observed that the companies offering surveillance and biometric technologies show a lack of appreciation for the consequences that their utilization will have on target populations.[95] Furthermore, they generally **display disinterest in establishing transparent standards, accountability mechanisms, and safeguards for human rights within their industry**. This suggests that many BDI tech providers and vendors do not adhere to the UN Guiding Principles on Business and Human Rights, particularly regarding their commitment to respect human rights, implement due diligence processes to identify and prevent significant harm to human rights, and openly disclose information on their compliance with existing laws.[96]

In the Africa region, the CAR country report noted that local activists are denouncing the government for failing to integrate transparency and accountability into its efforts to rebuild its ID database in partnership with Al Madina. Al Madina is a registered Omani company operated by a Lebanese management firm and holds multiple contracts for the production and issuance of identification documents in the CAR.[97]

Specifically, the award of the national ID contract to Al Madina is marred by (i) concerns about centralized decision-making between some government entities and one private sector entity without the involvement of citizens, which is evidence of limited external oversight, (ii) recorded objections on grounds of non-compliance with procurement laws by the Director General (DG), Public Procurement, Ministry of Finance and Budget, (iii) the monopoly that Al Madina has over CAR's identification market, and (iv) reports that the costs of issuing the

[95] ITS Río (2020). Good ID in Latin America: Strengthening appropriate uses of Digital Identity in the region, page 11.
[96] Access Now (2023). Vigilancia biométrica remota en América Latina: ¿las empresas están respetando los derechos humanos?
[97] Africa Intelligence (2021). Central African Republic: Lebanese firms battle over passport contract.

national identity card do not appear in the state's revenues leading to the conclusion that the management of funds generated by Al Madina are not subject to public accountability or oversight, despite their collections being generated from CAR citizens.'

.Table 11: Key Accountability and Transparency Concerns and Regional impact

Regional Concerns	Regional Risk/Impact
Africa	
Centralized decision-making processes between state and foreign corporations	Limited oversight by responsible state entities and limited public accountability
Lack of accountability and transparency in data sharing practices	Misuse of data by data collectors (government, private entities) and repurposing of data in databases for unlawful surveillance and law enforcement
Lack of appropriate BDI oversight by *independent* data protection authorities to promote compliance with data protection laws	Limited monitoring of BDI systems by independent authorities with risk of inappropriate use of data and systems
Limited transparency reporting on BDI programs	Failure to promote and fulfill BDI users' right to access information
Lack of transparency and accountability in BDI data collection exercises	Interference with BDI users' right to informed consent
Balkans	
Poor regional cooperation and information sharing on cybersecurity best practices	Limited intra-stakeholder collaboration impacting protection of BDI programs/systems. Erosion of public trust
Limited resources and capabilities to sufficiently handle cyber attacks on BDI	Inadequate support of monitoring and compliance entities resulting in lack of accountability of malicious actors
Lack of harmonization of existing laws	Uncertainty and ambiguity in legal (compliance) framework
Limited public awareness on cyber hygiene and cybersecurity	BDI users' vulnerability to cyber attacks impacting data ownership and control
Central Asia	

Poor compliance with data protection principles on accountability and transparency during biometric data collection, processing and transfer	Limited data ownership and control by BDI users and impaired informed consent
Poor compliance with recognized biometric standards for evaluating the quality and reliability of biometric technologies	Insufficient monitoring and oversight (audit and performance evaluations) and impacted BDI users' confidence and trust
Weak enforcement mechanisms	Limited monitoring of BDI systems by independent authorities with risk of inappropriate use of data and systems
Latin America & the Caribbean	
Lack of multi-stakeholder participation in BDI processes	Trust deficit and exclusion of external oversight stakeholders
Lack of established standards on accountability and transparency by system providers and vendors of BDI technologies and systems	Non-compliance with UN Guiding Principles on Business and Human Rights
South and Southeast Asia	
Lack of accountability and transparency for unauthorized disclosure of citizen information	Trust deficit by users in BDI technologies and reduced confidence in systems
Lack of transparency and accountability in BDI programs that use biometrics for verification and authentication	Inaccurate verification and authentication
Failure to institute grievance redressal systems	Lack of accountability and transparency of regulatory authorities for errors or losses Restricted access to services and authentication errors due to inaccurate information resulting in exclusionary harms Failure to provide BDI users with redress for errors or omissions
Weak enforcement and oversight mechanisms	Non-compliance with laws promoting misuse of data, discrimination, and unauthorized data sharing

Source: GIF Reports.

Accuracy and Reliability Concerns

Accuracy and reliability are critical considerations in adopting BDI systems and technologies as they directly impact the effectiveness and trustworthiness of BDI systems and technologies. Accuracy informs reliability, and where BDI systems and tech demonstrate high accuracy in their identification and authentication processes, this builds confidence and trust in their reliability. Where the adoption of BDI is instituted by the government, public trust and confidence are necessary for implementation.

Further, accuracy and reliability inform the implementation of other standards such as safety, security, and accountability. Lack of accuracy and reliability consideration in BDI systems gives rise of ethical concerns rooted in the implications and consequences of ineffective identification and authentication of BDI users and false positives/negatives,[98] resulting in users' inability to access BDI systems and services and exacerbating system security vulnerabilities. Further, accuracy and reliability issues can give risk to cases of fraud, identity theft, and data breaches.

Regional Observations

Across all five researched GIF regions, there is a general consensus about the benefits of BDI in enhancing accuracy and reliability in identification and authentication processes. However, the **inaccuracy of data is a central issue** that is reflected across different thematic areas, namely regulation, limitation of use, security, and integrity. The **ethical concerns regarding accuracy and reliability** are most visible in legal and regulatory processes (LAC and SSA Asia region), adoption, implementation, and use (Central Asia region), security and integrity (Africa and Balkans regions).

Notably, the inadequacy of BDI legal frameworks observed in Trend 3 above, directly impacts accuracy and reliability concerns. **Comprehensive and clear laws are the bedrock of establishing lawful data processing methods that incorporate accuracy and reliability.**

[98] "A "false positive" occurs when the system incorrectly matches an input to a non-matching template, while in a "false negative", the system fails to detect a match between an input and a matching template."Office of the Victorian Commissioner (2019). Biometrics and Privacy - Issues and Challenges.

Legal framework inadequacies can result in data errors, poor quality data or incomplete data. Further, weak legal frameworks directly impact seamless interoperability between state-state and state-private sector databases, giving rise to reliability concerns.

Table 12: Key Accuracy and Reliability Concerns and Regional Impact

Regional Concerns	Regional Impact
Africa	
Lack of integrity in data collection and processing	Minimized probability of accurate and reliable identification and verification, undermining their credibility. Compromised quality of data leading to instances of false positives/negatives. Users' inability to access BDI systems and services creating exclusionary harms.
Balkans	
Cybersecurity vulnerabilities compromise security and integrity of BDI systems affecting their accuracy and reliability	Higher risk of cybersecurity breaches and inaccuracy in authentication limiting access to relevant services.
Central Asia	
Limitations in the use of behavioral biometrics affecting accuracy and reliability due to changes in environment or health conditions	Potential inaccuracy in authentication and identification **Note:** *this does not serve as an endorsement for the collection of behavioral biometrics, such as DNA data. This report echoes the position held by the Kenyan High Court that this data is unnecessary and intrusive.*[99]
Latin America & the Caribbean	
Lack of clear legal, regulatory and supervisory frameworks	Non-effective remedies to breaches leading to negative human rights impacts, such as unauthorized BDI database access .
South and Southeast Asia	
Lack of clear legal frameworks on data retention and deletion	Accumulation of outdated or irrelevant

[99] *Nubian Rights Foundation & Ors. v. Attorney General of Kenya & Ors.* [2020] eKLR.

	personal and biometric data. Limited data ownership and control by BDI data.
	Source: GIF Reports.

Key Findings

Various factors, such as the implementation of tech-centric BDI systems, incorporating emerging and advanced biometric and digital ID technologies, are providing depth and complexity to prevailing concerns within the BDI ecosystem, rather than altering the nature of the concerns being raised. The concerns explored are tempered by regional and in-country priorities and contextual realities.

- **Privacy, Security and Ethical Concerns:**
  - Observed misuse of personal and biometric data giving rise to mission creep for law enforcement and security purposes, resulting in unlawful tracking, surveillance, and individual privacy violations.
  - Observed tech-vendor and supplier dominance in at least three out of the five GIF regions, giving rise to fears of vendor lock-in, potential biases in tech, impaired data sovereignty, and weakened data security.
  - Observed reliance on centralized databases by both government and private sector, despite weak or inadequate security measures and safeguards.
- **Accountability and Transparency Concerns:**
  - Observed gaps in accountability and transparency mechanisms for the regulation of BDI systems, technologies and procedures.
- **Accuracy and Reliability Concerns:**
  - Observed risk of data **inaccuracy** reflected across different thematic areas, namely regulation, limitation of use, security, and integrity.

Trend 5: Workforce Considerations and the BDI Fields

The embrace of BDI systems and technologies has had, and will continue to impact, jobs, skills, and tasks. This will have an impact on the global workforce, with the following key groups expected to experience radical workforce-related changes: the individuals responsible for developing BDI systems; individuals tasked with deploying BDI tools and systems for service delivery; and individuals who incorporate these services into their daily tasks. These vital individuals are critical stakeholders in the BDI fields, but their role is rarely examined in research reports.

In May 2023, the WEF published its 'Future of Jobs' report that predicts "significant labour market disruption, with substantial proportions of companies forecasting job displacement in their organizations" impacting digital platforms and apps, e-commerce, and AI, all of which are integral to the BDI fields.[100] However, the report notes that "encryption and cybersecurity are expected to be the biggest drivers of job growth,"[101] with these two considerations steering BDI concerns including privacy and security.

Framed against the projected and optimistic market expansion in the biometric tech and digital ID fields documented in Trend 1 above, this report finds that exponential **digital transformation specialists roles** will be created, driven by technology and digitization efforts.

[100] World Economic Forum (2023). Future of Jobs Report: Insight Report.
[101] *Ibid.*

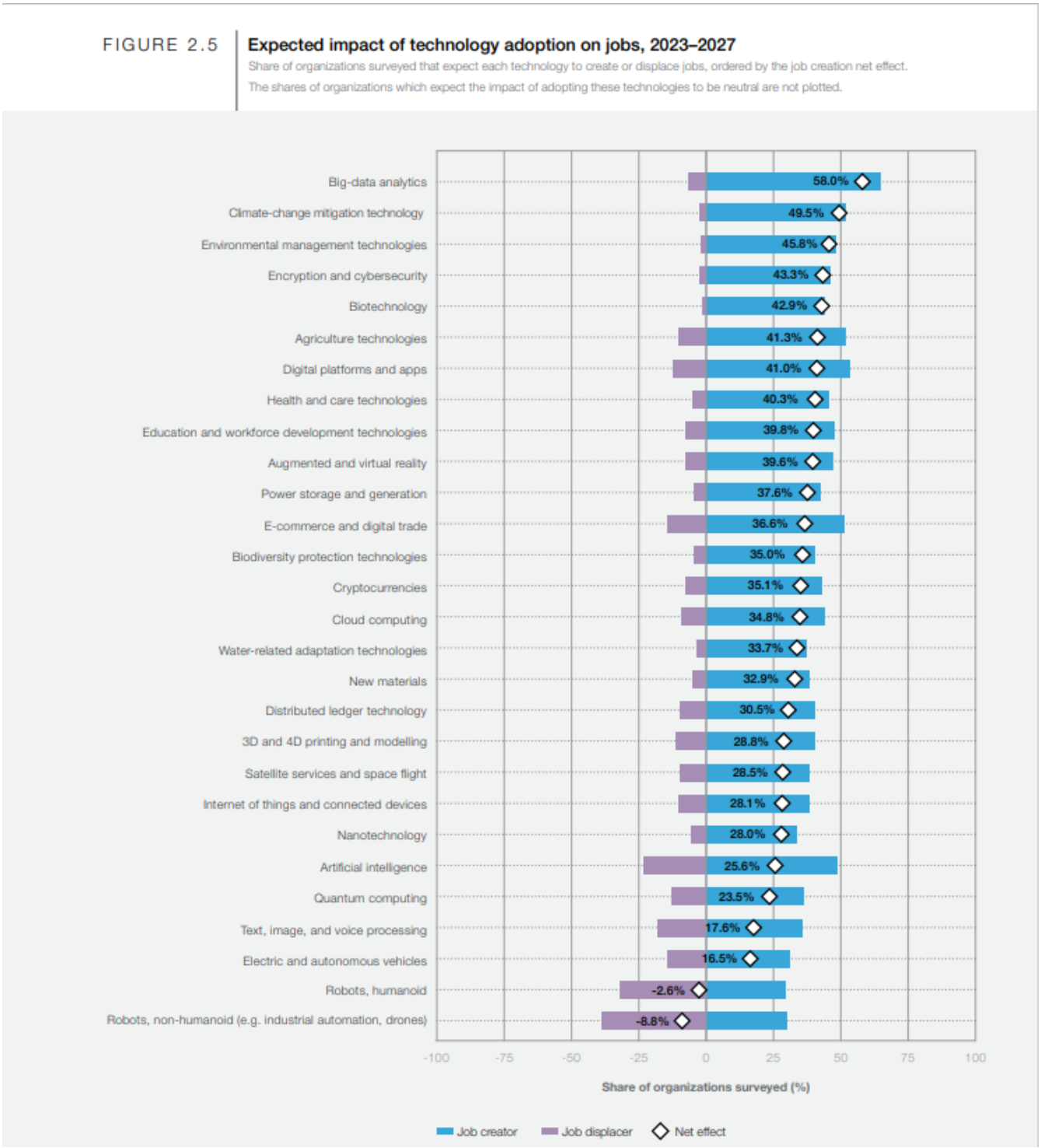

Figure 3: [World Economic Forum](#).

On the tasks front, task automation by AI technologies is projected to impact '50% of the workforce,' with tasks involving information and data processing, which are integral to the

BDI fields, projected to be 'automated by up to 65% by 2027.'[102] Another task that is anticipated to be impacted by digitization is monitoring and evaluation. Specifically, biometrics integrated with AI technology has enabled employers to keep track of worker productivity, through the deployment of sensor movement or keyboard logging.[103] Workplaces are increasingly adopting biometric security devices to monitor workers. Fingerprint-based attendance tracking systems have been widely used to check employee attendance.

On the skills front, the WEF notes that tech skills have increased in importance in BDI-related sectors including financial services, focusing on "Insurance and Pensions Management and Financial Services and Capital Markets."[104] Further, 'growing consumer awareness and ethical demands resulting from the adoption of frontier technologies is set to give rise to a growing demand for ethical skills in the workforce.' However, we note that this will not be cross-cutting across all GIF regions, with some regions prioritizing upskilling of the labor force on biometric technologies and digital ID, including skills such as authentication verification procedures, biometric systems and patterns, and computer security architecture.

[102] Ibid.
[103] ibid
[104] *Ibid.*

Trend 6: BDI and Stakeholder Engagements

Generally, there is a need to break down siloed conversations between governments, international institutions, and private infrastructure providers of biometric and/or digital identity management solutions resulting in the exclusion of all other stakeholders, including end-users. International institutions and governments are urged to involve and engage *all* stakeholders in the BDI ecosystem *prior to the implementation* of these systems, and only *if* it is determined that biometric adoption is required and appropriate.

To promote more stakeholder diversity and inclusion, responsible BDI entities must align themselves with the interests of all stakeholders involved. This requires a comprehensive understanding of the diverse perspectives, concerns, and needs of stakeholders in foundational ID systems, risk identification and mitigation, with a focus on potential or actual social, legal, political, and ethical implications, the promotion and fulfillment of a wide range of human rights, and the prioritization of BDI principles, such as accountability, transparency, and trust.'[105]

Regional Observations

On the **collaboration and partnerships front**, there has been a shift in the level of collaboration and partnership between governments and private players, development partners, and other nations through **multilateral financing agreements, bilateral agreements, and public-private partnerships (PPPs)** to deploy projects for the design, implementation and maintenance of biometric and digital ID systems across the regions.

Across four GIF regions, including Africa, Central Asia, LAC, and SSE Asia, international development/financial institutions, such as the World Bank, have aggressively provided funds to governments for the development of digital ID ecosystems. Illustratively, in **Africa**, the World Bank has provided a USD 150 million grant to Mozambique. Mozambique is also a beneficiary of the UN Legal Identity Agenda, where the UN selected it as a pilot country for modification of the national registration and identity database. Anecdotal information indicates that the United Nations Children's Fund (UNICEF) and World Food Programme

[105] CAR Country Report.

(WFP) have collaborated with the government of Zimbabwe through its Ministry of Labour and Social Welfare to roll out a trial digital ID system in Rushinga District.

In the **SSE Asia region**, the World Bank has provided financial assistance worth **approximately USD 2.7 trillion** to six out of the seven GIF countries in the form of either loans or grants between 2011-2022, with the funds being actively disbursed between 2021-2022.

Bilateral agreements between states are also on the rise, with countries such as the United Kingdom, India, and Japan providing financial support for the development of digital ID systems in Bosnia, Sri Lanka, and Zimbabwe respectively, through grants and donations. Illustratively, Sri Lanka has received a grant from the government of India, worth USD 3.8 million.

Intra-agency collaboration within governmental bodies has also increased, resulting in the creation of new ministries and bodies for digital development and digital ID. For instance, the Mozambique EDGE Project with the World Bank is a collaborative effort among the National Institute of Electronic Government (INAGE), the Ministry of Science and Technology (MOST), and the Project Implementation Steering Committee involving ministries of Interior, Finance, and Justice. The Minister for Digital Affairs in the DRC advises the l'Office National d'Identification de la Population (National Office for Population Identification/ONIP) on the digitization of data, including biometric data collected for the database of citizens' digital ID records, in a show of intra-governmental collaboration among relevant ministries and bodies.

Additionally, the National Institute of Statistics (INS), the Independent National Electoral Commission (CENI), and the National Identification and Population Office (ONIP) of DRC have signed a Memorandum of Understanding (MOU) to allow CENI to share voter registration data with INS and ONIP, which is necessary for the issuance of biometric national ID cards, in preparation for their 2023 elections. A multi-agency collaboration is also observed in Tanzania, where citizens must engage with the National Identification Authority (NIDA), the district office, and the local government in the process of obtaining their digital ID.

On the public-private partnerships (PPPs) & multi-stakeholder initiatives front, private sector players have aggressively expanded their geographical reach beyond North America, LAC and the Asia-Pacific regions. These private sector players are actively involved in the development of digital ID systems by providing digital identity-related technology products and services and biometric technologies leveraging public-private partnerships (PPPs).

Illustratively, **in Africa,** private companies are providing biometric election and BDI end-to-end systems, inclusive of biometric authentication, identification, and verification solutions to the governments of Angola, the DRC, and Mozambique. The government of DRC announced a EUR 400 million (USD 428 million) contract with various private players in the country, while the Mozambique government's bid for the provision of digitized voter management and voter rolls systems for the government has attracted the attention of global private companies such as Idemia, Thales, and Veridos.

In Tanzania, the government has interfaced its digital ID system with 74 private and public institutions. The National Identification Authority (NIDA) authorizes private mobile network operators (MNOs), such as Airtel, Halotel, Smile, Tigo, TTCL, and Vodacom, to act as an official partner for ID enrolment. Through the government directive to re-register all citizens' SIM cards using biometric authentication and national ID cards, NIDA leveraged MNOs extensive coverage to expedite the enrollment of citizens onto the national ID platform.

This move effectively transformed MNOs into the largest private sector stakeholder in the digital identity field in the country, "supporting the inclusion of several million people who had been previously unregistered."[106] In Uganda, the Ugandan National Identification and Registration Authority (NIRA) contracted the German company Mühlbauer ID Services GmbH to supply mass biometric national ID card registration systems.

In the Balkans, North Macedonia partnered with MasterCard to provide digital ID services such as verification and signing capabilities. Similarly, PPPs are seen as an appropriate approach to the implementation of digital ID systems in Serbia, where the Cyber Security Nexus PPP was established through the efforts of the Organization for Security and

[106] Yiannis Theodorou (2022). On the Road to Digital-ID Success in Africa: Leveraging Global Trends.

Cooperation in Europe (OSCE) Mission to Serbia, Petnica Research Center, Geneva Centre for Security Sector Governance and the Diplo Foundation.

In **SSE Asia**, the Maldives encourages private sector entities to rely on the national digital ID platform, facilitated through the National Centre for Information Technology (NCIT) and the Department of National Registration (DNR).

On the **public awareness and engagement front,** a significant trend has emerged in the Africa, LAC, and SSE Asia regions concerning public opinion and understanding of digital identity. Citizens are expressing concerns about various aspects, including delays in document issuance, lack of transparency regarding contracted companies, and the exorbitant costs associated with obtaining identity documents. Further, citizens expressed concerns about them being forced to bribe civil servants to overcome chronic delays when expecting identity documentation, and facing discrimination during the issuance of digital IDs.

Table 13: Public Concerns in the GIF Regions

Country-Specific Public Concerns

- **Angola:** interviewed citizens revealed that getting their digital identity documents takes months or years, is expensive, and can often only be obtained through bribes.
- **CAR:** the civil society working group protested the government's decision to award the contract for the issuance of digital identity cards to Al Madina Company, a private supplier that charged citizens 6,000 CFA francs instead of 4,500 as prescribed in the finance law.
- **Indonesia:** the Ahmadiyah community faces discrimination concerns since their religion is not recognized among the accepted six religions when registering for digital ID.
- **Tajikistan:** public outcry followed the government's decision to re-register citizens' SIM cards with the new biometric identity cards in Tajikistan, due to the expenses of re-registration and prior issuance delays.

Sources: Africa, Central Asia, SSE Asia Regional Reports.

Further, the **risk of data breaches** is another emerging trend that is giving rise to public sentiments regarding BDI systems. Citizens in Africa, Central Asia and SSE Asia have expressed frustration over the vast collection of biometric data, personal data leaks and irregular data sharing by government bodies. Illustratively, Ugandan respondents indicated that they are afraid of the government using their personal and biometric data to silence critics and facilitate surveillance activities. In Central Asia, the leak of citizens' data in Kazakhstan and Kyrgyzstan elicited responses from citizens who are concerned about their data privacy.

On the **regulation and policy development front,** the core mandate of developing legal frameworks for BDI systems is largely restricted to government ministries (including newly-created digital ministries) and ICT authorities/agencies. However, in some countries internal affairs and security ministries and statistics authorities possess BDI policy and regulation powers.

Illustratively, in Kazakhstan, the Ministry of Digital Development, the Committee on Personal Data Protection, the Ministry of Internal Affairs, and the National Security Committee (KNB) each perform a different role such as collection, storage, and processing of biometric data, registration of the biometric data of foreigners and stateless people and developing and maintaining biometric identity control systems. This development was necessitated by the emergence of digital citizenship and the need for expanded service delivery by governments in biometrics and digital identity.,

Further sectoral agencies and entities charged with promoting cybersecurity and data protection compliance play a critical role in the BDI policy and regulation front. Some critical entities include cybersecurity entities, such as National Computer Emergency Response Teams charged with developing cybersecurity strategies, and data protection authorities, responsible for promoting data protection policy development and regulatory compliance.

Unfortunately, there is **limited public participation in the design, implementation and maintenance of BDI systems** documented in the GIF reports. Public participation mainly arose in the form of **opposition to government decisions**, such as protests by civil society and police officers in CAR, in response to the government's intention to work with the Al Madina company. Reports indicate that in Mozambique, citizens find it difficult to exercise their right to inspect data and raise objections about data processing, especially as it pertains to the deletion and security of their personal data.

On the **stakeholder diversity and inclusion front,** the majority of the GIF regional reports note that there is no tangible shift to engage all stakeholders in BDI ecosystems prior to their design or implementation. Many GIF countries still treat public participation, where this is prioritized, as a tick-box exercise that is mandated in law, rather than as an ongoing process. The central stakeholders who typically steer BDI design and implementation conversations

have remained unchanged, and are restricted to governments, international development partners, and the private sector. Civil society is mainly involved in oversight, where they partner with citizens to denounce unfavorable BDI decisions by governments.

Key Findings

- **On the collaboration and partnerships front**, multilateral financing agreements, bilateral agreements, and public-private partnerships (PPPs) are being used as legal vehicles to deploy BDI projects across all five researched GIF regions.
- On the **public awareness and engagement front,** citizens are expressing concerns about various aspects of BDI design and deployment. These include delays in document issuance, lack of transparency regarding contracted companies, exorbitant costs associated with obtaining identity documents, the need for facilitation payments, and discrimination and exclusion.
- On the **regulation and policy development front,** the core mandate of developing legal frameworks for BDI systems is largely restricted to government ministries (including newly-created digital ministries) and ICT authorities/agencies. In some countries, internal affairs and security ministries, and statistics authorities possess BDI policy and regulation powers. Sectoral agencies, such as data protection authorities also play an integral role in policy and regulatory development.
- On the **stakeholder diversity and inclusion front,** public participation arises mainly as opposition to government decisions regarding BDI systems. Further, there has been no observable change in the siloed stakeholder engagements revolving exclusively around governments, international development partners, and the private sector, to the exclusion of all other stakeholders.

Geographic Assessment

Regional Observations: Definitions, Purpose, Types and Use Cases

On **definitions,** most GIF regional reports adopted the definition of digital ID and biometrics advanced by entities such as the World Bank or the National Institute of Standards and Technology (NIST).[107] However, this must be framed against the well-acknowledged stance that there is no globally agreed-upon definition of digital ID. This definitional adoption is driven by the recognition that the World Bank's definition is the most commonly adopted, in its capacity as one of the central international organizations driving the global digital ID initiative.

On the **purpose** of digital ID systems, all regions have established foundational and functional ID systems, with observable differences at the deployment stage. This reveals that across all five researched GIF regions, the expanding use of BDI is an established phenomenon across countries and industries.

Notably, socio-economic, infrastructural capacity, and political contexts play a central role in the uptake and varying purposes of ID systems across the regions. For instance, the deployment of BDI systems and tech in the LAC region is contextualized around expanding state-surveillance efforts, leading to the general conclusion that BDI systems are an *extension* of the surveillance machinery. In Africa, the CAR and DRC's BDI ecosystem is marred by political instability resulting in BDI practices, such as flawed procurement processes, that fall short of the intended BDI purpose or goal.

On the **types of data collected**, all researched GIF countries collect both personal and biometric data, with differences observed between regions exclusively collecting physiological biometrics, and those that promote the collection of both physiological and behavioral biometrics. Among biometric technologies, fingerprint identification stands as the most widely utilized type.

[107] World Bank Group. Brief on Digital Identity; World Bank. Glossary; NIST. Glossary – Biometrics.

All GIF regions favor **centralized identity management systems,** with governments generally acting as the primary custodian of data collected in state ID systems. The commonality in centralized ID systems can be attributed to the fact that BDI adoption is largely driven by ongoing government initiatives across the five regions.

Table 14: Regional Breakdown

Region	Purpose/Use Cases	Type of Data Collected	Key Factors
Africa	- National identification - Government services - Authentication - Verification - Voter registration - Surveillance (*GIF report observation)* - Civil registration	Personal Data (e.g., demographics) Biometrics	**Encouraging BDI Adoption** Advanced technological infrastructure and internet connectivity Robust regulatory frameworks Political will for BDI adoption **Impeding BDI Adoption** Political instability Censorship Lack of internet connectivity Low level of digital skills Lack of access to digital devices Low rate of internet penetration Centralised personal registries increase digital ID systems implementation
Balkans	- National identification - Online banking - E-government services - Border control	Personal data (e.g., demographics) Biometrics	
Central Asia	- National identification - Voter registration - Authentication - Access to e-government services	Personal data (e.g., demographics) Biometrics	
Latin America and the Caribbean	- National Identification - Authentication - Surveillance (*GIF report observation)* - Access to social services	Personal data (e.g., demographics) Biometrics	
South and South East Asia	- Authentication for online transactions and services - E-government services - Verification - Civil Registration	Personal Data (e.g., demographics) Biometrics	

Regional Observations: Risks in BDI systems and Recommended Solutions

BDI systems carry inherent risks that apply across five researched GIF regions. This section advances solutions to mitigate some of them.

Table 15: BDI Risks and Solutions

Region	Risk in BDI Systems	Recommended Solutions
Africa	**Privacy and Data Security Risks**: Risks include unauthorized access, data breaches, and identity theft. Additionally, the misuse of biometric data for surveillance purposes can infringe on individuals' privacy rights. **Exclusion and Inequality**: Biometric and digital identity systems may unintentionally exclude certain segments of the population, particularly those who lack access to technology or official identification documents. This can further exacerbate existing inequalities and marginalized vulnerable groups. **Inaccurate Data and Identity Fraud**: Biometric systems may encounter challenges in accuracy, especially in cases of poor data quality or technical issues. Inaccurate data can lead to misidentification and errors in service delivery. Additionally, there is a risk of identity fraud if biometric data is compromised or duplicated. **Cybersecurity Vulnerabilities**: Digital identity systems are susceptible to cybersecurity threats, including hacking, phishing, and ransomware attacks. Breaches in these systems can lead to unauthorized access to personal data and undermine public trust in the technology. **Lack of Legal and Regulatory Frameworks**: Inadequate legal and regulatory frameworks governing the use of	**Comprehensive Data Protection Laws**: Implement robust data protection laws and regulations to safeguard biometric data from unauthorized access, misuse, and breaches. Data protection laws should provide clear guidelines on data collection, storage, sharing, and retention. **Privacy by Design**: Adopt a privacy-by-design approach when developing and implementing BDI systems. Privacy considerations should be embedded throughout the entire system's lifecycle, from design to implementation to ongoing maintenance. **Inclusive Design**: Ensure that biometric and digital identity systems are designed to be inclusive and accessible to all segments of the population, including marginalized and remote communities. Allow other forms of alternative identification in digital ID systems and alternative authentication methods for individuals who may not have biometric data. **Accuracy and Quality Assurance**: Regularly assess the accuracy and reliability of biometric data and systems to minimize errors and misidentifications. Implement quality assurance measures to maintain data integrity. **Cybersecurity Measures**: Strengthen cybersecurity measures to protect digital identity systems from cyber threats. This includes regular security audits, encryption of data, and continuous monitoring for potential vulnerabilities. **Local Expertise and Capacity Building**: Invest in local expertise and capacity building to develop and maintain biometric and digital

	biometric and digital identity systems risks infringing the rule of law. The absence of clear guidelines can lead to data, system and tech misuse and potential human rights violations. **Dependency on External Suppliers**: Many GIF countries rely on external vendors for biometric and identity technologies. This dependency can lead to challenges in data ownership, data sovereignty, and potential exploitation by foreign entities.	identity systems. Reducing reliance on external vendors can enhance data sovereignty and increase local ownership. **Transparent Governance**: Establish transparent and accountable governance structures for biometric and digital identity projects. Involve multiple stakeholders, including civil society organizations, in oversight and decision-making processes. **Public Awareness and Participation**: Educate the public about the benefits, risks, and safeguards of biometric and digital identity systems. Encourage public participation and consultation in the design and implementation of these systems.
Balkans	**Privacy Concerns**: Biometric data, such as fingerprints and facial images, are highly sensitive and unique to individuals. The collection and storage of such data raise privacy concerns, as there is a risk of unauthorized access, misuse, or potential breaches that could compromise individuals' privacy rights. **Data Security**: Biometric and digital identity systems store large volumes of personal data. Inadequate security measures could make these systems vulnerable to cyberattacks, data breaches, or insider threats, leading to the compromise of sensitive information. **Surveillance and State Control**: The widespread use of biometric technologies for identification and surveillance purposes could raise concerns about state control and mass surveillance. Excessive biometric data collection and tracking may lead to the infringement of citizens' rights and freedoms. **Exclusion and Discrimination**: Biometric systems may not be accessible or inclusive for certain groups of individuals, such as the elderly, disabled, or marginalized populations, who may face challenges with biometric enrollment or authentication, leading to exclusion from services.	**Comprehensive Data Protection Regulations**: Implement robust data protection laws that govern the collection, storage, and use of biometric data. The legislation should include provisions for informed consent, data minimization, purpose limitation, and data retention periods. **Encryption and Security Measures**: Employ strong encryption and security protocols to protect biometric data from unauthorized access or data breaches. Regular security audits and assessments can help identify vulnerabilities and address them promptly. **Ethical Use and Transparency**: Ensure transparency in the use of biometric technologies and communicate clearly with the public about the purpose and scope of their implementation. Demonstrate ethical considerations and responsible use of biometrics to build public trust. **Inclusive Design and Accessibility**: Ensure that biometric and digital identity systems are designed to be inclusive and accessible to all citizens, regardless of age, disability, or socio-economic status. Alternative authentication methods should be available for those unable to use biometrics. **Privacy Impact Assessments**: Conduct Privacy Impact Assessments (PIAs) before implementing biometric and digital identity projects. PIAs can identify potential risks to privacy and inform mitigation strategies to safeguard individuals' rights. **Cross-Border Collaboration**: Facilitate cross-border collaboration and

	Lack of Legal Frameworks: In some cases, the legal framework governing the use of biometric and digital identity systems may be inadequate or unclear. The absence of comprehensive legislation could result in a lack of oversight and accountability in data handling and use. **Cross-Border Data Sharing**: In the Balkans, cross-border data sharing between countries may raise concerns about data sovereignty and protection. Ensuring secure and transparent data exchange is essential to prevent unauthorized access or misuse of biometric information.	information sharing among Balkan countries to address common challenges and establish uniform standards for biometric data protection and sharing. **Independent Oversight**: Establish independent oversight mechanisms to monitor the implementation of biometric and digital identity systems. Independent agencies can ensure compliance with data protection laws and act as a check on potential abuses. **Public Awareness and Engagement**: Conduct public awareness campaigns to educate citizens about the benefits and risks of biometric and digital identity technologies. Engaging with the public and involving stakeholders in the decision-making process can foster understanding and support for these systems.
Central Asia	**Privacy and Data Security**: Biometric and digital identity systems collect sensitive personal data, such as fingerprints, facial images, and iris scans. The risk of unauthorized access, data breaches, and identity theft can pose significant privacy and data security concerns for individuals. **Surveillance and State Control**: The widespread use of biometric technologies in Central Asia may raise concerns about mass surveillance and government control. Biometric data can be misused for tracking citizens' movements, monitoring activities, and suppressing dissent, leading to potential human rights violations. **Inaccuracies and False Positives**: Biometric systems are not entirely infallible and may lead to inaccuracies or false positives, especially in large-scale implementations. This could result in wrongful identification or exclusion of individuals from accessing essential services. **Lack of Data Protection Frameworks**: Some countries in Central Asia may lack robust data protection	**Comprehensive Data Protection Laws**: Central Asian countries should enact comprehensive data protection laws that govern the collection, storage, and use of biometric data. These laws should include strict penalties for unauthorized access and data breaches. **Privacy by Design**: Implementing a "privacy by design" approach when developing biometric and digital identity systems can help ensure that privacy and security considerations are integrated from the outset. **Transparent Policies**: Governments should establish transparent policies regarding the use of biometric and digital identity data, ensuring clear guidelines on its scope, purpose, and limitations. **Independent Oversight and Auditing**: Central Asian countries should establish independent oversight bodies to monitor the use of biometric data and conduct regular audits to assess compliance with data protection and privacy regulations. **Public Awareness and Education**: Governments should conduct public awareness campaigns to educate citizens about the benefits and risks of biometric and digital identity systems, empowering them to make informed decisions. **Interoperability and Standards**: Central Asian states should work towards establishing interoperable biometric systems and adherence

	frameworks to govern the collection, storage, and sharing of biometric data. The absence of proper regulations can leave individuals vulnerable to privacy violations. **Cross-Border Data Sharing**: Central Asian states may engage in cross-border data sharing for law enforcement or security purposes, raising concerns about the misuse or mishandling of biometric data by foreign entities. **Technological Vulnerabilities**: Biometric and digital identity systems may be vulnerable to hacking, data manipulation, or unauthorized access. Weak cybersecurity measures could expose these systems to exploitation by malicious actors. **Exclusion and Discrimination**: Central Asian countries' digital identity systems may inadvertently exclude certain populations, such as marginalized communities or individuals without access to biometric enrollment centers. This could exacerbate existing social inequalities.	to international standards to enhance cross-border cooperation while safeguarding data privacy. **Ethical Use of Data**: Policymakers and stakeholders must ensure that biometric data is only collected and used for legitimate and ethical purposes, avoiding any misuse or discrimination based on the data. **Collaborative Regional Efforts**: Central Asian countries can collaborate on sharing best practices, experiences, and expertise in the responsible use of biometric and digital identity technologies. This regional cooperation can facilitate collective efforts to address common challenges and enhance cybersecurity measures.
LAC	**Privacy and Data Security Risks**: One of the primary risks associated with biometric and digital identity systems is the potential compromise of individuals' privacy and security. Biometric data is highly sensitive, and if not adequately protected, it can lead to identity theft, fraud, or unauthorized access to personal information. **Surveillance and Human Rights Concerns**: The widespread adoption of biometric technologies for surveillance purposes raises concerns about potential violations of human rights, such as the right to privacy and freedom of movement. The collection and use of biometric data without proper legal safeguards can lead	**Comprehensive Data Protection Framework**: Governments should establish comprehensive data protection laws and regulations that specifically address the collection, storage, and use of biometric data. Clear guidelines on consent, data retention, and data sharing should be enforced to protect individuals' privacy rights. **Transparent Governance and Oversight**: Biometric and digital identity systems should be subject to transparent governance and oversight mechanisms. Independent bodies or regulatory authorities should monitor system implementation to ensure compliance with ethical standards and human rights principles. **Privacy by Design**: Implementing a privacy by design approach can help mitigate risks from the outset. Privacy considerations should be integrated into the design and development of BDI systems to

	to excessive state surveillance and potential abuse of power. **Exclusion and Discrimination**: There are concerns that certain populations, such as marginalized communities or undocumented individuals, may face exclusion from essential services if they lack access to biometric or digital identity systems. Biased algorithms or improper implementation may result in discrimination and unequal treatment. **Lack of Data Protection Laws and Regulations**: Many countries in the region may lack robust data protection laws and regulations to govern the use of biometric data. The absence of clear guidelines can lead to inadequate safeguards and expose individuals to privacy risks. **Cybersecurity Vulnerabilities**: Biometric and digital identity systems are vulnerable to cyberattacks and data breaches. If not properly secured, these systems could become targets for malicious actors seeking to access sensitive biometric data.	prioritize data protection and minimize potential vulnerabilities. **Inclusive Design and Impact Assessments**: Governments should conduct thorough impact assessments to understand the potential consequences of biometric and digital identity systems, especially on marginalized populations. Inclusive design principles should be employed to ensure that systems do not lead to exclusion or discrimination. **Ethical Use of Biometrics**: There should be clear guidelines on the ethical use of biometric data, ensuring that it is used solely for legitimate and specified purposes. Governments and organizations should avoid using biometrics for mass surveillance or without transparent justifications. **Cybersecurity Measures**: Robust cybersecurity measures must be implemented to safeguard biometric and digital identity systems from cyber threats. Regular security audits, encryption of data, and continuous monitoring can help protect against data breaches and unauthorized access. **Public Awareness and Engagement**: Governments should engage in public awareness campaigns to educate citizens about biometric and digital identity systems, their rights, and the importance of data protection. Transparent communication can build trust and promote responsible use of these technologies.
SSE Asia	**Data Privacy and Security Risks**: One of the primary risks associated with biometric and digital identity systems is the potential compromise of sensitive biometric data. Unauthorized access, data breaches, or improper handling of biometric information can lead to identity theft and fraud, compromising individuals' privacy and security. **Exclusion and Inclusion Risks**: There is a risk of exclusion when implementing biometric and digital identity systems, especially in remote and marginalized communities. Lack of access to enrollment centers or	**Comprehensive Data Protection Laws and Regulations**: Countries should enact comprehensive data protection laws to safeguard biometric data and ensure its secure handling, storage, and sharing. Implementing clear guidelines on data access, retention, and destruction can help mitigate the risks of data breaches and unauthorized access. **Privacy Impact Assessments (PIAs)**: Conducting Privacy Impact Assessments before implementing biometric and digital identity systems is crucial. PIAs assess the potential privacy risks and provide recommendations to minimize privacy intrusions and protect citizens' rights.

	technical literacy may result in certain populations being excluded from obtaining identification, limiting their access to essential services. Additionally, there may be inclusion risks if the systems fail to adequately verify the identities of certain individuals due to factors like age, disabilities, or changes in physical appearance. **Accuracy and Error Risks**: Biometric systems are not infallible, and false matches or errors in identification may occur, leading to misidentification and potential denial of services or benefits to legitimate individuals. The accuracy of biometric matching algorithms and the quality of biometric data collected are critical factors in mitigating these risks. **Surveillance and Misuse Risks**: The use of biometric technologies for surveillance purposes may raise concerns about privacy and potential misuse by authorities. Mass data collection exercises without proper oversight and legal safeguards may lead to excessive surveillance, infringing on citizens' rights and freedoms. **Single Point of Failure**: Relying heavily on biometric and digital identity systems for various services may create a single point of failure. Technical glitches or system failures could disrupt critical services and cause inconvenience to citizens. **Lack of Interoperability**: In the absence of interoperable systems, data sharing and exchange between different government agencies may be challenging. This can result in duplication of efforts, delays in service delivery, and inefficiencies in the identification process.	**Inclusive Design and Accessibility**: Governments should ensure that biometric and digital identity systems are designed to be inclusive and accessible to all citizens, regardless of their location, age, or physical abilities. Mobile biometrics and multiple enrollment centers can be employed to reach remote and marginalized communities. **Independent Audits and Reviews**: Regular independent audits and reviews of biometric systems can help identify vulnerabilities and assess their accuracy, performance, and compliance with privacy and security standards. **Public Awareness and Consent**: Raising public awareness about biometric and digital identity systems is essential. Citizens should be educated about the benefits and risks, and informed consent should be obtained for the collection and use of biometric data. **Interoperability Frameworks**: Governments should work towards establishing interoperable systems and data sharing frameworks to ensure seamless data exchange between various agencies, reducing duplication and improving service delivery. **Strong Governance and Oversight**: Establishing strong governance structures and oversight mechanisms is critical to ensure accountability, transparency, and responsible use of biometric and digital identity technologies.
		Sources: GIF Regional Reports

Conclusions and Recommendations

The "*Biometrics and Digital Identity: Trend Analysis and Comparative Assessment*" global report reveals an expanded adoption and use of biometrics technologies and digital ID systems in a variety of sectors and for numerous societal needs and interests. Based on the trend analysis, this report observes the following:

- The adoption of biometrics and digital ID for public (government) sector and private services is a growing phenomenon across all five researched GIF regions.
- The benefits of adopting biometric and digital ID technologies must be weighed against the risks associated with the collection of biometric data. All five regions document BDI benefits, but have not addressed 'unacceptable consequences,' impacting privacy, ethics, security, accountability, transparency, accuracy, and reliability.
- Among researched GIF countries, nine countries including the CAR, have not enacted comprehensive data protection laws for the safe regulation of BDI data.
- The uptake of BDI technologies in the regions is not concurrent with the development of BDI-specific regulation. Only Kyrgyzstan, in the Central Asia region, has BDI-specific regulations.
- Public participation across all five researched GIF regions is low, with the demonstration of minimal or no involvement prior to the adoption and implementation of BDI technologies.

The geographical assessment observes the following:

- All five researched GIF regions favor a centralized system of identity management as opposed to either a federated or decentralized system.
- Despite the growing momentum to adopt and implement digital ID, some regions experience weak infrastructural capacity and the lack of well-established institutional and technical ID systems.

- The utilization of BDI technologies is increasingly popular in facilitating access to government services through the implementation of e-government initiatives. Governments in all regions have shown efforts to digitize their services and make them more accessible through these technologies.

Based on this, the report proposes the following recommendations to stakeholders in the five researched GIF regions:

Recommendations

Recommendations Guided by Key Findings

GIF Governments are urged to:

Develop and implement a robust and proportionate legal framework for BDI systems consisting of policies, laws, regulations, codes of practice etc. The nine GIF countries without comprehensive, stand-alone data protection laws should immediately adopt frameworks to protect personal data.

Address the core concerns of data privacy, security, transparency, accuracy and reliability through well-established implementation procedures and redress mechanisms.

The International Community operating in GIF regions is urged to:

Ensure that technical and financial support for BDI programs granted/loaned to governments incorporates a public awareness budget line. This should sensitize BDI users on both the risks and benefits of BDI technologies and encourage participatory and inclusive multi-stakeholder engagement across the ID lifecycle.

GIF CSOs are urged to

Leverage a range of soft (e.g., press releases) and hard (e.g., public interest litigation) tactics to introduce rights-respecting reforms into BDI systems across all five regions, including leveraging the capacities of the GIF Consortium to engage in advocacy and policy efforts.

Promote digital rights and Internet freedom in the BDI ecosystem, through policy engagements, advocacy and awareness campaigns, research, and collaborations and partnerships.

Regional Recommendations

GIF Africa Countries are urged to:

Embrace expanded stakeholder engagements to generate public buy-in rather than opposition to BDI programs.

Publicize transparency reports on deployed BDI technologies and systems.

GIF Balkans Countries are urged to:

Implement strong cybersecurity measures to address cyber attacks that jeopardize BDI systems.

Enhance regional cooperation and information sharing among Balkan countries.

GIF Central Asia Countries are urged to:

Review and update biometric registration laws to address gaps, clarify legal frameworks, and ensure compliance with international standards.

Increase accessibility of biometric national ID cards, particularly for vulnerable populations.

GIF Latin America and the Caribbean Countries are urged to:

Conduct human rights impact assessments (HRIAs) prior to implementing digital ID systems and monitor their implementation to respond to human rights impacts.

GIF South and Southeast Asia Countries are urged to:

Allow other forms of alternative identification in digital ID systems to end the continued exclusion and marginalization of vulnerable groups.

Establish well-designed and accessible grievance and redressal frameworks.

Reference List

GIF Partner Reports

Africa Region

Regional Report: Biometrics and Digital Identity in Africa

Biometric Identification in Angola

Biometric Identification in the Central African Republic

Biometric Identification of the Youth Population in the Democratic Republic of Congo

Biometric Elections in Mozambique

Biometric Identity and SIM Card registration and Telecoms in Tanzania

BDI Programs and Independence of Journalism in Uganda

Biometric and Digital Identity in Zimbabwe

Balkans Region

Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity

Central Asia Region

Biometric and Digital ID Programs in Central Asia

Latin America and the Caribbean Region

Digital ID in Latin America: Current Situation, Trends and Issues

South and Southeast Asia Region

Report: Digital Identification Systems in South and Southeast Asia