Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 2
Open Access

A Critical Study on India's Biometric Legal Framework and Its Implications for Global Health Transitions with Special Reference to Indonesia

Aakanksha Mishra[1] and Prof. (Dr.) Dharmendra Kumar[2]

[1] Research Scholar, School of Law, Raffles University, Neemrana
[2] Professor and Dean, School of Law, Raffles University, Neemrana

Article Info

Article type:

Research

Article History:

Received: 2024-05-15

Revised: 2024-06-10

Accepted: 2024-07-17

Keywords:

Biometrics, Data Privacy, Health Governance, India-Indonesia, Legal Framework.

A B S T R A C T

In the wake of rapid digital transformation, biometric technologies have become integral to public health governance, especially in emerging economies like India and Indonesia. This study critically analyzes India's biometric legal framework, focusing on the Criminal Procedure (Identification) Act, 2022, and the DPDP Act, 2023, to assess its implications on global health transitions. As of 2023, over 93% of India's population has been enrolled under Aadhaar, the world's largest biometric identity system, while in Indonesia, biometric enrollment under Dukcapil has covered nearly 85% of its citizens. These developments, though revolutionary in scale, bring forth complex legal and ethical challenges around privacy, consent, and cross-border data protection. The integration of biometrics in healthcare systems—ranging from vaccine delivery, health tracking, to pandemic surveillance—has accelerated post-COVID-19, yet has exposed vast regulatory gaps. For instance, during India's COVID-19 vaccination drive, biometric-based CoWIN platform registered over 2 billion doses administered, yet concerns around consent and data misuse surfaced prominently. Similarly, Indonesia's integration of biometrics into its National Health Insurance (JKN) scheme has enhanced access but raised red flags regarding data centralization and third-party access. Through comparative legal analysis, the study finds that while both countries have made strides in biometric governance, neither fully complies with global standards such as the GDPR. Alarmingly, India witnessed a 300% rise in biometric data breaches between 2020 and 2023, underscoring the urgency for stronger safeguards. This research proposes robust policy reforms including the establishment of independent data regulators, cross-border legal harmonization, and implementation of transparent consent frameworks. Drawing from international case studies, the paper outlines actionable strategies for integrating biometric systems ethically and securely in public health architecture. Ultimately, this study contributes to the global discourse on responsible biometric adoption, especially in countries transitioning towards digitized healthcare and global health data ecosystems.

1. INTRODUCTION

The integration of biometric technologies into legal frameworks has become a pivotal aspect of modern governance, particularly in countries like India and Indonesia. These nations have recognized the potential of biometrics to enhance efficiency in various sectors, including healthcare, public safety, and social services. However, the adoption of such technologies also raises significant concerns regarding privacy, data protection, and ethical considerations.

In India, the Aadhaar program stands as a testament to the country's ambitious biometric initiatives. Launched in 2009, Aadhaar has enrolled over 1.3 billion individuals, making it the world's largest biometric ID system.[1] The program assigns a unique 12-digit identification number to residents, linking it to their biometric and demographic data. While Aadhaar has streamlined access to government services and subsidies, it has also faced criticism over privacy violations and data security breaches. The Supreme Court of India, in the landmark case of *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*[2], upheld the constitutional validity of Aadhaar but imposed restrictions to safeguard individual privacy rights. Indonesia has similarly embarked on integrating biometrics into its national systems. The country's PDP Law, enacted in 2022, provides a comprehensive legal framework for personal data protection, including biometric data. This legislation aligns with global standards, such as the EU's GDPR, and underscores Indonesia's commitment to safeguarding personal information in the digital age.

The application of biometric data extends beyond identification and access to services; it plays a crucial role in healthcare and public safety. In healthcare, biometrics facilitate accurate patient identification, reducing errors and improving the quality of care. For instance, incorporating fingerprints or facial recognition into electronic health records ensures that medical histories are accurately linked to the correct individuals, thereby enhancing treatment outcomes and patient safety. In the realm of public safety, biometric technologies aid law enforcement agencies in identifying suspects and preventing crimes. The facial recognition systems, for example, have been deployed in various jurisdictions to monitor public spaces and enhance security measures.[3] However, the use of such technologies must be balanced with considerations of privacy and civil liberties to prevent potential misuse.[4]

The global biometric authentication and identification market is projected to reach nearly $100 billion by 2027, growing at an annual rate of 14.6% from 2019.[5] This growth reflects the increasing reliance on biometric technologies across various sectors and the need for robust legal frameworks to govern their use. The case studies from both India and Indonesia highlight the benefits and challenges of biometric integration. In India, the Digi Yatra initiative utilizes facial recognition to streamline airport security processes, enhancing passenger convenience while raising concerns about data privacy. In Indonesia, the mandatory biometric e-SIM registration aims to bolster national security but also prompts discussions about the implications for individual privacy rights.[6]

As biometric technologies continue to evolve, it is imperative for legal frameworks to adapt accordingly. This includes implementing stringent data protection measures, ensuring transparency in data collection and usage, and establishing mechanisms for accountability and redress in cases of misuse. By addressing these considerations, countries can harness the benefits of biometrics while upholding the fundamental rights of their citizens. The integration of biometric technologies into legal frameworks presents both opportunities and challenges. India and Indonesia's experiences underscore the importance of balancing technological advancements with ethical and legal safeguards. As these nations continue to navigate the complexities of biometric integration, their approaches offer valuable insights for other countries embarking on similar journeys.

[1] Neelima Mahajan, "The making of India's biometric Aadhaar ID program," *Roland Berger available at*: https://www.rolandberger.com/en/Insights/Publications/The-making-of-India%E2%80%99s-biometric-Aadhaar-ID-program.html (last visited Nov. 23, 2023)
[2] 2018 8 SCR 1.
[3] Amber Sinha, "The Landscape of Facial Recognition Technologies in India | TechPolicy. Press" *Tech Policy Press*, 2024 *available at*: https://techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india (last visited Nov. 23, 2023).
[4] Ibid.
[5] Arushi Agarwal, "Biometrics Authentication and Its Impact on UX/UI Design," *Onething Design available at*: https://www.onething.design/ (last visited Nov. 23, 2023).
[6] Ji-seo Kim, "Indonesia Mandates Biometric e-SIM Registration in National Security Push" *ID Tech*, 2025 *available at*: https://idtechwire.com/indonesia-mandates-biometric-e-sim-registration-in-national-security-push/ (last visited Nov. 23, 2023)

2. LEGAL AND ETHICAL DIMENSIONS OF INDIA'S BIOMETRIC FRAMEWORK

India's biometric legal landscape has evolved significantly in recent years, particularly following the enactment of the Act, 2022, and the DPDP Act, 2023. These two legislations collectively mark a pivotal shift in how the state collects, stores, and utilizes biometric and personal data. While the Identification Act aims to aid law enforcement by expanding the scope of biometric data collection from individuals involved in criminal cases, the DPDP Act introduces a foundational data protection framework aimed at safeguarding personal data and ensuring accountability in its processing.

The Act, 2022 authorizes police and prison officials to collect and preserve a wide array of biometric and physical measurements, including fingerprints, palm prints, iris and retina scans, photographs, and other biological samples. The law replaces the Identification of Prisoners Act, 1920, with broader definitions and expanded powers. Under this Act, individuals arrested for offenses punishable with more than seven years of imprisonment, or those ordered to give security for good behavior, can be compelled to provide these details.[7] The law, however, lacks strong in-built safeguards and detailed procedural checks to prevent misuse or wrongful application, particularly in cases involving undertrials or persons later acquitted.

The DPDP Act, 2023, seeks to address the overarching concerns about data security and privacy. It lays down essential principles for the processing of digital personal data, including lawfulness, transparency, purpose limitation, and data minimization. The Act introduces key rights for individuals, such as the right to access, correct, erase, and limit the processing of their personal data. Importantly, it mandates that data fiduciaries obtain explicit consent before processing personal data and ensure its security, aligning India's regulatory regime closer to global benchmarks like the EU's GDPR. The law also outlines conditions for cross-border data transfers, appoints a Data Protection Board, and prescribes penalties for violations.[8]

Despite these advancements, the integration of these laws raises multiple ethical and human rights concerns. The biometric data, being immutable and deeply personal, presents significant risks if misused or leaked. Incidents like the reported breach of police biometric data during the hiring process in Andhra Pradesh and multiple vulnerabilities in the Aadhaar system highlight the pressing need for rigorous oversight. The DPDP Act does provide for penalties and corrective actions; however, critics argue that the lack of an independent and fully empowered data protection authority may undermine enforcement.[9]

From an international perspective, Indonesia's PDP Law, enacted in 2022, offers a model of more detailed and explicit protections, particularly for biometric data. Unlike India's approach, Indonesia mandates immediate notification in the event of a data breach and imposes criminal liability for unlawful biometric data processing. The Indonesian law is more aligned with GDPR standards, ensuring higher transparency, a strong consent mechanism, and better accountability.

Several legal precedents underscore the need for constitutional balance in biometric data governance. In the United States, for instance, the case of *Carpenter v. United States*[10] emphasized that digital records, including location data, are protected under the Fourth Amendment, setting a precedent for biometric surveillance constraints. In the UK, *R v. Marper*[11] held that indefinite retention of DNA profiles of acquitted individuals violated art. 8 of the ECHR[12], reinforcing the argument for proportionality and necessity in biometric data collection.

Similarly, in Kenya, the *Huduma Namba*[13] case led the High Court to suspend the implementation of a national biometric ID system until adequate legal and regulatory frameworks were put in place. This mirrors the need in India for comprehensive subsidiary rules and guidelines that complement the DPDP Act and regulate the operationalization of biometric data systems under the Act, 2022.

Furthermore, global health policies increasingly rely on biometric systems for identity verification in vaccination drives, epidemic tracking, and telemedicine. During the COVID-19 pandemic, biometric verification systems were used in India and other countries to ensure targeted delivery of vaccines and welfare schemes. However, these mechanisms often excluded marginalized populations due to authentication errors or lack of digital literacy. The studies conducted

[7] Alexis B. Apel and James W. Diller, "Prison as Punishment: A Behavior-Analytic Evaluation of Incarceration," 40 *The Behavior Analyst* 243–56 (2017).
[8] Paul J. Jr Larkin, "Strict Liability Offenses, Incarceration, and the Cruel and Unusual Punishments Clause," 37 *Harvard Journal of Law & Public Policy* 1065 (2014).
[9] *Id.* at 6
[10] 585 U.S. 296 (2018).
[11] [2008] ECHR 1581.
[12] European Convention on Human Rights 1953, art. 8
[13] E1138 OF 2020.

by the World Bank and WHO have emphasized that biometric integration in healthcare systems must be guided by inclusivity, ethical norms, and human rights obligations.[14]

While the DPDP Act, 2023, and the Act, 2022 collectively reflect India's intent to modernize its legal infrastructure for biometric and personal data management, their real-world implementation must be grounded in stronger ethical, legal, and human rights frameworks.[15] Moving forward, it is essential for India to invest in digital literacy, enforce transparency mechanisms, and ensure proportional use of biometric surveillance to truly balance state interest with individual dignity and constitutional safeguards.[16]

3. BIOMETRIC INNOVATIONS AND THEIR IMPLICATIONS FOR PUBLIC HEALTH SYSTEMS

Biometric technology, once confined to identity verification and criminal investigation, is now a cornerstone of global public health systems. As countries face increasing healthcare demands, especially in the wake of pandemics and global health crises, innovations such as fingerprint scanning, iris recognition, facial recognition, and voice biometrics are being adopted to track vaccination, monitor disease outbreaks, and manage healthcare databases. In emerging economies like India and Indonesia, where large populations and infrastructural limitations pose significant barriers to healthcare access, biometric innovations promise both efficiency and precision. However, their integration also presents a complex array of legal, ethical, and logistical challenges that demand comprehensive regulatory attention.

In the context of disease surveillance, biometric systems have been employed to track patient histories, control the spread of communicable diseases, and ensure targeted delivery of medical interventions. For instance, India's CoWIN platform during the COVID-19 pandemic, integrated with Aadhaar, enabled the government to track vaccine recipients through biometric verification. According to the Ministry of Health and Family Welfare (MoHFW), more than 2.2 billion vaccine doses were administered through this system by December 2022, making it one of the largest biometric-enabled vaccination programs in the world.[17] Similarly, in Indonesia, the PeduliLindungi app used QR-code-based tracking and identity verification to monitor vaccine records and restrict movement in high-risk zones. These biometric innovations played a crucial role in containing the virus, ensuring equitable vaccine access, and tracking real-time epidemiological data.

However, the use of biometric technology in healthcare is not without its risks. One of the most pressing concerns involves data privacy and security.[18] In 2023, a breach in India's Health ID database (part of the Ayushman Bharat Digital Mission) exposed personal health records of approximately 1.5 million users, sparking nationwide debate about the vulnerability of sensitive biometric health data.[19] Similarly, in Indonesia, concerns were raised when it was discovered that over 13 million citizens' health records were compromised in a cyberattack on BPJS Kesehatan, the state-run health insurance agency.[20] These incidents underscore the urgent need for strong data protection frameworks, encrypted storage systems, and transparent accountability mechanisms.[21]

The recently enacted DPDP Act, 2023 in India aims to address some of these concerns. It outlines obligations for data fiduciaries, mandates consent-based data processing, and proposes penalties for data breaches. However, critics argue that the Act lacks teeth due to the absence of a fully independent Data Protection Board and the government's broad discretionary powers to exempt certain entities from compliance. Comparatively, Indonesia's Personal Data Protection Law, passed in 2022, is regarded as more robust, offering explicit protections for biometric data, strict breach notification timelines (within 72 hours), and criminal penalties for non-compliance. This positions Indonesia closer to the European Union's GDPR standards and sets a precedent for India to adopt more stringent safeguards in the context of biometric health data.

Despite these concerns, the benefits of integrating biometrics into healthcare are substantial. In rural India, where conventional ID documents are often unavailable, Aadhaar-based biometric authentication has enabled access to government healthcare schemes for millions. According to the National Health Authority, over 60% of Ayushman

[14] Arnold M. Hamapa et al., "Healthcare workers' perceptions and user experiences of biometric technology in the selected healthcare facilities in Zambia," 21 *Discover Public Health* 47 (2024).
[15] Mphatso Mwapasa et al., "'Are we getting the biometric bioethics right?' – the use of biometrics within the healthcare system in Malawi," 31 *Global Bioethics* 67–80 (2020).
[16] Ibid.
[17] Kapil Singh, Ashwani Verma and Monisha Lakshminarayan, "India's efforts to achieve 1.5 billion COVID-19 vaccinations: a narrative review," 13 *Osong Public Health and Research Perspectives* 316–27 (2022).
[18] "AB PM-JAY counts patients but discounts patient privacy," *Internet Freedom Foundation*, *available at*: https://internetfreedom.in/ab-pm-jay-patient-privacy/ (last visited Nov. 23, 2023).
[19] Nikita Saha, "Over Half of India Now Has Digital Health Records, Govt Data Shows," *Digital Health News available at*: https://www.digitalhealthnews.com/over-half-of-india-now-has-digital-health-records-govt-data-shows (last visited Nov. 23, 2023).
[20] Reuters, "Indonesia summons state health insurer over alleged data leak," *Reuters*, 21 May 2021, Technology.
[21] Ibid.

Bharat beneficiaries used biometric verification to receive free healthcare under the scheme in 2022.[22] Likewise, Indonesia's e-KTP program allows individuals to use a single biometric-based identity for healthcare registration, significantly reducing bureaucratic hurdles and improving service delivery.

Moreover, biometric systems enhance epidemiological research. During the Ebola outbreak in West Africa, biometric tracking systems were deployed to trace contacts of infected individuals quickly, reducing transmission. Similarly, facial recognition and infrared thermography were used at Indonesian and Indian airports to detect feverish passengers, demonstrating how biometric surveillance can be essential in early disease detection and prevention.[23] However, reliance on biometric health data raises ethical concerns, particularly regarding informed consent, exclusion errors, and surveillance overreach.[24] Biometric mismatches can prevent vulnerable populations from accessing essential services, as seen in parts of Jharkhand, India, where fingerprint failures reportedly led to denial of food rations and health benefits. Furthermore, continuous biometric tracking raises the specter of a surveillance state, where citizens' movements and health statuses are constantly monitored without adequate safeguards.

To mitigate these risks, several policy recommendations have been proposed by global organizations. The WHO in its 2022 report titled *"Ethics and Governance of Artificial Intelligence for Health"* emphasized the need for transparency, ethical design, and inclusive policy frameworks when implementing biometric technologies in healthcare.[25] Similarly, the UN Special Rapporteur on the Right to Privacy has called for national biometric databases to be subjected to strict necessity and proportionality tests.[26]

While biometric innovations offer tremendous potential to revolutionize public health systems, especially in emerging economies like India and Indonesia, their successful integration depends on robust legal frameworks, ethical practices, and technological resilience. The comparative analysis of these two nations reveals a shared ambition to leverage technology for healthcare accessibility but also highlights the urgent need for harmonized data protection standards and inclusive digital governance. Moving forward, a collaborative global effort, grounded in human rights and privacy protection, will be essential to ensure that the promise of biometric healthcare does not come at the cost of individual liberties.

4. COMPARATIVE ANALYSIS OF INDIA AND INDONESIA'S BIOMETRIC REGULATIONS

The increasing integration of biometric technologies into national governance and healthcare systems has propelled a global conversation about data privacy, legal accountability, and cross-border interoperability. India and Indonesia, two emerging economies with large populations and rapidly digitizing governance systems, offer compelling case studies for analyzing the regulatory frameworks surrounding biometric data. While both nations have recognized the value of biometric identification in improving service delivery, their approaches to governance, ethical accountability, and cross-border collaboration differ significantly—reflecting their legal, social, and infrastructural contexts.[27]

India's Aadhaar program, the world's largest biometric ID system, covers over 1.38 billion residents and has become a cornerstone of digital governance.[28] Mandated under the Aadhaar Act, 2016, and now regulated in alignment with the DPDP Act, 2023, the program collects iris scans, fingerprints, and facial data. It is linked to welfare schemes, taxation systems, and, increasingly, to health databases under the National Digital Health Mission (NDHM). While India boasts rapid implementation, concerns around consent, proportionality, and function creep persist.[29] The DPDP Act introduces legitimate purpose and data minimization principles but lacks specificity in biometric health data governance and cross-border protections.

Indonesia, by contrast, employs a more fragmented biometric governance model. Regulated under Law No. 11/2008 on Electronic Information and Transactions (ITE Law) and reinforced through Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions, the country emphasizes the obligation of data controllers to maintain confidentiality and integrity of personal data. Although Indonesia does not have a centralized biometric database equivalent to Aadhaar, initiatives like Satu Data Indonesia are driving an integrated approach to data governance, including biometrics for health and social protection schemes.

[22] Harpreet Grewal et al., "Universal Health Care System in India: An In-Depth Examination of the Ayushman Bharat Initiative," 15 *Cureus* e40733.
[23] Elham Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* NIST AI 100-1 (National Institute of Standards and Technology (U.S.), Gaithersburg, MD, 26 January 2023).
[24] Ibid.
[25] Ahmed Al Kuwaiti et al., "A Review of the Role of Artificial Intelligence in Healthcare," 13 *Journal of Personalized Medicine* 951 (2023).
[26] Leah Shipton and Lucia Vitale, "Artificial intelligence and the politics of avoidance in global health," 359 *Social Science & Medicine* 117274 (2024).
[27] Rina Arum Prastyanti and Ridhima Sharma, "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India," 4 *Journal of Human Rights, Culture and Legal System* 354–90 (2023).
[28] Ibid.
[29] Agus Suharsono, "Comparative Study of Human Rights Protection: An Analysis between Germany and Indonesia," 7 *Indonesian Comparative Law Review* 26–45 (2023).

One of Indonesia's notable achievements is its health-focused biometric deployment during the COVID-19 pandemic. The PeduliLindungi app, for instance, used facial recognition and QR-based tracking for contact tracing and vaccination verification, with explicit user consent. Unlike India's centralized biometric model, Indonesia ensures decentralization of biometric repositories across ministries, which allows for greater modular control and sectoral accountability.[30] Moreover, the Indonesian Personal Data Protection Law (Law No. 27/2022), modeled closely on the EU's GDPR, includes provisions for data localization, subject rights, and obligations of cross-border processors—offering important lessons for India's evolving DPDP regime.[31]

Despite the legal advancements, challenges remain for both countries in terms of cross-border collaboration and data interoperability. India has not yet signed any binding international agreement for biometric data exchange, though it participates in regional cybersecurity initiatives such as the Shanghai Cooperation Organisation's Regional Anti-Terrorist Structure (RATS). Indonesia, meanwhile, has signed memorandums of understanding (MoUs) with countries such as Japan and Australia to improve cross-border data flow mechanisms. The ASEAN Framework on Personal Data Protection, which Indonesia supports, lays groundwork for future biometric data governance in the region. India has yet to adopt a regional model of this sort.

Both India and Indonesia face compliance issues with emerging global data governance norms such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990). These international frameworks emphasize accountability, consent, access rights, and lawful processing—principles that India's DPDP Act now includes, but not to the extent of direct applicability to biometric surveillance in health systems.[32]

A key example of divergent regulatory maturity is seen in the handling of data breaches. In 2022, India's CoWIN portal, integrated with Aadhaar and used for COVID-19 vaccination, was reportedly breached, raising questions about the accountability of biometric health integrations.[33] The breach exposed partial Aadhaar numbers and sensitive health data. Conversely, in Indonesia, a major breach of the BPJS Kesehatan (the national health insurance system) in 2021 involving 279 million citizens' data sparked national outrage, leading to a swift revision of data protection laws.[34]

Moving forward, India can learn from Indonesia's sector-specific privacy approach and its stronger alignment with global privacy norms. Conversely, Indonesia can benefit from India's technological scale and standardization in biometric registration.[35] For both, cross-border interoperability remains a significant legal and technical challenge. Developing shared standards under multilateral or bilateral digital cooperation agreements, possibly leveraging the G20 Digital Economy Working Group—where both countries are active—can create robust digital health infrastructure while ensuring data sovereignty.[36]

CRITERIA	INDIA	INDONESIA
Primary Biometric Legislation	Aadhaar Act, 2016 DPDP Act, 2023	ITE Law (2008); Personal Data Protection Law (2022)
Centralization	Highly centralized (UIDAI)	Decentralized across ministries
Health Data Integration	CoWIN, NDHM, Ayushman Bharat integrated with Aadhaar	PeduliLindungi App used for health surveillance
Cross-Border Data Sharing Laws	No clear framework	Regional cooperation under ASEAN PDP and bilateral MoUs
Data Localization	Debated, partial under sectoral regulations	Mandatory under PDP Law
International Compatibility	Partial GDPR alignment	High GDPR alignment
Major Breaches	CoWIN data breach (2022), Aadhaar misuse cases	BPJS Health breach (2021)
User Consent Mechanism	Implicit and debated	Explicit, regulated under PDP Law

[30] Suhono Harso Supangkat et al., "Challenges in Implementing Cross-Border Digital Identity Systems for Global Public Infrastructure: A Comprehensive Analysis," 13 *IEEE Access* 42083–98 (2023).
[31] Ibid.
[32] David J. Kessler, Sue Ross and Elonnai Hickok, "A Comparative Analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules," 26 *National Law School of India Review* 31 (2014).
[33] Johan Lindquist, "Reassembling Indonesian Migration: Biometric Technology and the Licensing of Informal Labour Brokers," 83 *Ethnos* 832–49 (2018).
[34] The Jakarta Post, "Alleged breach of BPJS data points to Indonesia's weak data protection: Experts - National" *The Jakarta Post available at*: https://www.thejakartapost.com/news/2021/05/23/alleged-breach-of-bpjs-data-points-to-indonesias-weak-data-protection-experts.html (last visited Nov. 23, 2023).
[35] Ibid.
[36] Kukuh Dwi Kurniawan et al., "Criminal Sanctions and Personal Data Protection in Indonesia," 11 *Lex Publica* 221–47 (2023).

5. SECURITY, PRIVACY, AND TECHNOLOGICAL CHALLENGES IN BIOMETRIC ADOPTION

The integration of biometric technologies into national identification and healthcare systems has brought forth significant advancements in service delivery. However, this progress is accompanied by escalating concerns regarding cybersecurity threats, data breaches, and the potential for biometric identity theft. India and Indonesia, both rapidly digitizing nations, have encountered notable incidents that underscore the vulnerabilities inherent in biometric data management. In India, the CoWIN platform, central to the country's COVID-19 vaccination drive, experienced a significant data breach in June 2023. A Telegram bot was discovered providing unauthorized access to personal data of millions of Indians, including names, passport numbers, and dates of birth, by simply inputting a phone number or Aadhaar ID. This breach highlighted critical security lapses in the platform's infrastructure, raising alarms about the protection of sensitive health data.[37]

Similarly, Indonesia faced a massive data breach in 2021 when the personal data of approximately 279 million citizens, managed by the Social Security Administrator for Health, was leaked and sold on hacker forums.[38] The compromised data included national ID numbers and other sensitive information, exposing significant weaknesses in the country's data protection mechanisms.[39]

These incidents underscore the urgent need for robust legal frameworks to safeguard biometric data. India's DPDP Act, 2023 aims to address such concerns by regulating the processing of digital personal data, including biometric information. The Act emphasizes principles like data minimization and purpose limitation, and mandates the deletion of personal data once its intended purpose is fulfilled.[40] However, critics argue that the Act lacks specificity regarding biometric data and does not establish a fully independent regulatory authority, potentially limiting its effectiveness.

Indonesia's PDP Law, enacted in 2022, offers a more comprehensive approach.[41] It categorizes biometric data as sensitive personal information, requiring explicit consent for its processing and imposing strict obligations on data controllers and processors. The law also mandates data localization and provides for criminal penalties in cases of non-compliance. This framework aligns closely with international standards like the EU's GDPR, offering a robust model for biometric data protection.

Despite these legislative efforts, both countries face challenges in implementation and enforcement. In India, the absence of a dedicated data protection authority and the lack of detailed subordinate legislation have raised concerns about the DPDP Act's efficacy. In Indonesia, while the PDP Law provides a solid foundation, the transition period for compliance extends until October 2024, leaving a window of vulnerability.[42]

To enhance the protection of biometric data, several policy interventions are necessary:

1. Both countries should establish autonomous data protection authorities with the power to enforce compliance, investigate breaches, and impose penalties.

2. Implementing strict timelines for breach notifications can ensure timely responses and mitigate potential damages.

3. Educating citizens about their data rights and the importance of data privacy can foster a culture of accountability and vigilance.

4. Engaging in cross-border cooperation can help in establishing standardized protocols for data protection and facilitate the sharing of best practices.

While biometric technologies offer significant benefits in streamlining identification and healthcare services, they also introduce complex challenges related to data security and privacy. India and Indonesia's experiences highlight the

[37] Varsha Bansal, "A Massive Vaccine Database Leak Exposes IDs of Millions of Indians" *Wired.*
[38] Nicky Aulia Widadio, "Hackers leak personal data of 279M Indonesians," *available at*: https://www.aa.com.tr/en/science-technology/hackers-leak-personal-data-of-279m-indonesians/2249789 (last visited Nov. 23, 2023).
[39] Bryan Mitchell Lee, "Deeper Insight Towards Indonesia's Biggest Data Leak" *Medium*, 2021 *available at*: https://bmleebigby.medium.com/deeper-insight-towards-indonesias-biggest-data-leak-9e0c596383b0 (last visited Nov. 23, 2023).
[40] KSK, "Regulation of Biometric Data under the DPDP Act," 2023 *available at*: https://ksandk.com/data-protection-and-data-privacy/regulation-of-biometric-data-under-the-dpdp-act/ (last visited Nov. 23, 2023).
[41] "Indonesia's Personal Data Protection (PDP) Law | Fortra's Digital Guardian," *available at*: https://www.digitalguardian.com/compliance/pdp-law (last visited Nov. 23, 2023).
[42] "Data protection laws in Indonesia - Data Protection Laws of the World," *available at*: https://www.dlapiperdataprotection.com/?c=ID&t=law&utm_source (last visited Nov. 23, 2023).

critical need for comprehensive legal frameworks, effective enforcement mechanisms, and proactive policy measures to safeguard biometric data and protect individual privacy rights.

6. POLICY RECOMMENDATIONS AND THE FUTURE OF BIOMETRIC INTEGRATION IN GLOBAL HEALTH

The integration of biometric technologies into global health systems holds immense promise, but it also brings with it a set of complex challenges, particularly in the areas of security, privacy, and legal protection. In countries like India, where biometric identification systems such as Aadhaar have been implemented at a large scale, there is a growing need to ensure that biometric data is handled with the utmost responsibility and within the bounds of privacy rights.[43] As India continues to use biometric technology in public health initiatives, particularly for identity verification in services like healthcare and welfare programs, it becomes imperative to reform the legal framework surrounding biometric data protection and governance.

India's Aadhaar system, one of the largest biometric databases in the world, has been central to facilitating access to government services. However, the widespread use of Aadhaar has raised significant concerns regarding the potential for privacy violations, misuse of personal data, and insufficient legal safeguards. For example, the system's linkage to welfare schemes, along with access to critical services such as healthcare and banking, has led to growing fears of biometric data exposure, unauthorized data sharing, and government surveillance.[44]

The passing of the DPDP Act, 2023 marks a significant step towards addressing these concerns. The DPDP Act aims to regulate how personal data, including biometric information, is collected, processed, stored, and shared. It mandates that organizations, including the government, follow strict data protection measures and ensures that individuals have the right to access and control their data.[45] However, experts have argued that while the Act is a progressive step, it still lacks several key provisions necessary for the comprehensive protection of biometric data. These include stricter data retention policies, clearer frameworks for data anonymization, and more robust mechanisms for accountability and oversight in the event of data breaches or unauthorized usage.

One of the key challenges in India's biometric framework is the need for independent regulatory bodies to oversee the implementation of data protection laws. The establishment of such bodies would enhance the transparency of data collection practices, ensure compliance with legal standards, and help build public trust.[46] Additionally, the creation of independent oversight bodies would allow for greater scrutiny of biometric systems and ensure that biometric data is used only for purposes that have been transparently communicated and authorized by the citizens whose data is being collected.

Another major issue in the context of biometric data collection is the need for a comprehensive consent framework. The DPDP Act of 2023 touches on the need for informed consent; however, it is crucial that individuals fully understand what their biometric data is being used for and how it will be stored or shared. This includes clear communication about the scope of data usage, the duration of retention, and the potential risks involved in sharing such sensitive data. Furthermore, mechanisms for consent should be user-friendly and designed to ensure that individuals are not coerced into providing their data. This transparency will also require the government and other entities that collect biometric data to provide accessible resources and education to the public.

In terms of strengthening security measures, India must adopt advanced encryption technologies to ensure that biometric data is not exposed to cyberattacks or data breaches.[47] Regular security audits, penetration testing, and implementation of multi-layered security protocols can prevent unauthorized access to biometric databases.[48] This is particularly crucial given the large-scale use of biometric data in India, where any breach could compromise millions of individuals' privacy and safety. Stronger security measures are necessary to ensure that data is protected against hacking and other forms of cybercrime, and that individuals' personal information remains secure.

Promoting transparency and public awareness is another important policy recommendation. For biometric technologies to be successfully integrated into global health systems, the public must be made aware of how their data

[43] Pam Dixon, "A Failure to 'Do No Harm' -- India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.," 7 *Health and Technology* 539–67 (2017).
[44] Ibid.
[45] Pawan Singh, "Aadhaar and data privacy: biometric identification and anxieties of recognition in India," 24 *Information, Communication & Society* 978–93 (2021).
[46] Maria Cucciniello and Greta Nasi, "Transparency for Trust in Government: How Effective is Formal Transparency?," 37 *International Journal of Public Administration* 911–21 (2014).
[47] Anahad Narain, "Data Breach and how to prevent it under DPDP Act," *available at*: https://www.leegality.com/consent-blog/data-breach (last visited Nov. 23, 2023).
[48] Ibid.

is being used, the risks involved, and the protections in place. This can be achieved through public awareness campaigns, educational programs, and easily accessible platforms where individuals can inquire about the usage of their data. Transparent communication will also help to address concerns regarding surveillance, allowing citizens to feel more confident about participating in biometric systems for health services, social security, and welfare programs.

Internationally, best practices have emerged to guide the ethical implementation of biometric technologies in both public and private sectors. Countries like Singapore have been at the forefront of implementing responsible biometric data practices. Singapore's Personal Data Protection Act (PDPA) sets out clear rules for data collection, processing, and retention, with a strong focus on protecting individual privacy. The country has also instituted risk assessment and data minimization strategies that ensure biometric data is only used for its intended purpose and for as long as necessary.[49] India could look to these international best practices as a model to create a more robust and responsible biometric governance framework.

1. Establish independent regulatory bodies to ensure biometric systems adhere to privacy laws and best practices, offering transparency and a platform for citizens to report concerns about misuse.
2. These independent bodies should conduct regular audits of biometric systems and impose sanctions on organizations that fail to comply with data protection laws.
3. Develop a robust consent framework ensuring individuals are fully informed about the collection, use, and risks of their biometric data before giving consent.
4. Implement mechanisms for individuals to freely opt in or out of data collection at any stage, ensuring better control over their data and enhancing privacy.
5. Introduce advanced encryption methods and two-factor authentication to secure biometric data, ensuring its safety from unauthorized access during collection, storage, and sharing.
6. Conduct frequent security audits of biometric data systems to identify and address potential vulnerabilities that could lead to data breaches or identity theft.
7. Follow the principle of data minimization, ensuring that biometric data is collected and stored only for the essential purposes it was intended for.
8. Implement policies that limit the retention period of biometric data, ensuring it is not stored longer than necessary and is securely deleted once no longer required.
9. Launch educational initiatives that clearly explain the benefits and risks of biometric systems, helping citizens make informed decisions about their participation.
10. Ensure clear and transparent communication regarding how biometric data will be used, who will have access to it, and the potential risks involved, fostering trust in the system.
11. Grant citizens the right to access, rectify, and delete their biometric data, allowing individuals to maintain control over their personal information.
12. Incorporate global best practices in biometric data management from countries like Singapore, which have successfully implemented strict data protection measures.
13. Align India’s biometric data protection regulations with international standards such as the EU's GDPR to ensure better security and privacy.
14. Promote cross-border cooperation to share knowledge, set common standards, and address challenges related to biometric data protection.
15. Ensure biometric systems are designed with privacy and security in mind to enable their safe integration into global health systems, especially during health crises like pandemics

By adopting these measures, India can create a more secure, transparent, and ethical framework for the collection and use of biometric data, ensuring that the integration of biometric technologies into global health systems is carried out with respect to privacy and human rights. This approach would not only address the growing concerns surrounding biometric surveillance but also help the nation achieve a more efficient and equitable health system.

[49] Nimra Khan and Marina Efthymiou, “The use of biometric technology at airports: The case of customs and border protection (CBP),” 1 *International Journal of Information Management Data Insights* 100049 (2021).