

Data-Driven Governance in India: A Review of Aadhaar, Direct Benefit Transfers, and Data Infrastructure in Welfare, Health and Education

Kiran Chougule

¹Public Policy and Governance Research, India

Corresponding Author: Kiran Chougule

Abstract

India's public administration has undergone a significant transformation over the past decade through the integration of biometric identity (Aadhaar), Direct Benefit Transfer (DBT), and, more recently, health and education data infrastructures - the Ayushman Bharat Digital Mission (ABDM) and the Automated Permanent Academic Account Registry (APAAR). This paper reviews the design, statistical performance, and legal-regulatory context of this data-driven governance model using secondary data drawn from government assessments, parliamentary records, judicial pronouncements, and peer-reviewed and policy literature. Reported cumulative DBT savings of ₹3.48 lakh crore (2013–2024) and a fall in subsidy share of government expenditure from approximately 16% to 9% are examined alongside independent evidence of biometric authentication failure rates of approximately 6.5% of monthly transactions, disproportionately affecting elderly, disabled, and manual-labour populations. The paper further reviews the extension of this identity-linked data model into the ABDM (over 104 crore linked health records) and APAAR (over 233 million enrolled students), and evaluates the adequacy of India's Digital Personal Data Protection Act, 2023 in governing these systems. The study finds a consistent pattern of infrastructure preceding regulation across all three domains and proposes a three-part framework - outcome-linked auditing, statutory exception-handling, and regulatory sequencing - for more accountable data governance design.

Keywords: data governance, Aadhaar, Direct Benefit Transfer, digital public infrastructure, e-governance, biometric authentication, ABDM, APAAR, data protection.

Date of Submission: 22-09-2026

Date of acceptance: 02-10-2026

I. INTRODUCTION

1.1 Background

Public administration in India has historically been described as data-poor at the point of service delivery even where it was document-heavy in process [1]. Beginning with the rollout of the Unique Identification (Aadhaar) project in 2009–2010 and accelerating through the “JAM trinity” of Jan Dhan bank accounts, Aadhaar, and mobile connectivity, the Indian state has built a layered digital identity and data infrastructure - internationally described as a Digital Public Infrastructure (DPI) or “India Stack” model [2] - that now underpins subsidy transfer, health record-keeping, and educational credentialing.

This data-driven model has since been extended well beyond its original welfare-delivery use case, into the Ayushman Bharat Digital Mission (ABDM) in the health sector and the Automated Permanent Academic Account Registry (APAAR) in school and higher education, raising questions about the transferability of an identity-and-authentication logic first designed for subsidy de-duplication into more sensitive and rights-intensive domains.

1.2 Objectives of the Study

This paper has four objectives: (i) to statistically document the fiscal and administrative outcomes of Aadhaar-linked DBT; (ii) to review independent and parliamentary evidence on authentication-related exclusion; (iii) to assess the extension of this data model into health (ABDM) and education (APAAR); and (iv) to evaluate the adequacy of India's data-protection legal architecture in governing these systems.

1.3 Scope and Structure

The paper is structured as follows: Section II reviews the relevant literature; Section III describes the research methodology; Section IV presents the statistical and data overview; Section V discusses the results; Section VI critically analyses the key governance challenges; and Section VII concludes with recommendations for policy and further research.

II. LITERATURE REVIEW

2.1 Digital Public Infrastructure and E-Governance

The World Bank's Digital Dividends framework characterises identity-linked digital infrastructure as a foundational layer of state capacity, capable of improving the efficiency of public service delivery when paired with adequate analogue institutions - regulation, capacity, and accountability [2]. Dreze and Khera's review of India's social security architecture similarly finds that the pre-Aadhaar delivery system suffered chronic leakage and duplication, providing the administrative rationale for a unique, de-duplicated identity layer, while cautioning that technology alone does not resolve delivery failures rooted in weak grievance redress [1].

2.2 Studies on Aadhaar, DBT, and Welfare Delivery

A substantial empirical and government literature has since evaluated Aadhaar-linked DBT. The most recent government-commissioned quantitative assessment reports cumulative savings of ₹3.48 lakh crore over 2013–2024, attributing more than half of this figure to authentication-driven leakage reduction in the Public Distribution System [3], [4], [5]. This official efficiency literature is counterbalanced by a body of independent and parliamentary evidence. Testimony before India's Public Accounts Committee has documented persistent biometric authentication failure linked to worn fingerprints among manual labourers and iris changes among elderly beneficiaries [6]. A 2026 policy analysis quantifies this at approximately 6.5% of all monthly Aadhaar-based authentication attempts across welfare, banking, and public services - a rate essentially unchanged over the past decade despite high laboratory-controlled accuracy rates [7]. Field-based scholarship in the *Economic and Political Weekly* has developed a typology of Aadhaar-linked exclusion, and independent audits of state-level ration card deduplication drives have found that a large majority of cards cancelled as “duplicate” or “ghost” entries in fact belonged to genuine, eligible beneficiaries [8], [9].

2.3 Legal and Regulatory Literature

The constitutional literature on Aadhaar centres on the Supreme Court's two Puttaswamy judgments: the 2017 recognition of informational privacy as an aspect of the fundamental right to life and personal liberty under Article 21 [10], and the 2018 Constitution Bench ruling upholding the Aadhaar Act, 2016 while applying a proportionality standard and striking down private-sector use of Aadhaar authentication [11]. Justice D.Y. Chandrachud's dissent in the latter judgment - holding that mandatory biometric linkage for subsistence entitlements is disproportionate - remains a frequently cited minority position in subsequent critique [11]. On the regulatory side, legal-practice literature documents that the Digital Personal Data Protection Act, 2023, though enacted in August 2023, remained without an operative enforcement mechanism until the notification of the DPDP Rules, 2025 in November 2025, with full compliance obligations phased through May 2027 [18], [19].

2.4 Literature on Health and Education Data Governance

Government and policy-tracking literature on the ABDM documents its scale - over 104 crore linked health records by mid-2026 - and its stated function of generating anonymised datasets for disease surveillance and public health planning [12]. Comparable literature on APAAR documents both its rapid national rollout, covering over 233 million students across more than 1.47 million schools [17], and civil-society legal analysis identifying that the scheme was deployed without a standalone parliamentary law or notified data-protection policy specific to student data, relying instead on administrative circulars [16].

2.5 Research Gap

The reviewed literature reveals a clear analytical gap: government efficiency assessments (Section 2.2) and independent exclusion studies are rarely triangulated within a single framework, and the extension of Aadhaar's identity logic into health and education (Section 2.4) has been documented descriptively but has not been systematically evaluated against the constitutional proportionality standard established in the Aadhaar judgment (Section 2.3). This paper addresses that gap by synthesising fiscal, exclusion, and legal-regulatory evidence across all three domains within a single analytical structure.

III. RESEARCH METHODOLOGY

This is a doctrinal and documentary review paper based entirely on secondary data. Data sources comprise: (a) government and government-commissioned reports (Ministry of Finance/BlueKraft Digital Foundation DBT assessment; Ministry of Health and Family Welfare ABDM reporting; Ministry of Education/UDISE+ data); (b) primary legal sources (the Aadhaar Act, 2016; the Digital Personal Data Protection Act, 2023; and the 2017 and 2018 Supreme Court judgments in Puttaswamy); and (c) independent and policy literature, including parliamentary committee testimony, the *Economic and Political Weekly*, and civil-society legal analysis. Statistics reported in Section IV are drawn directly from these sources and are presented with their original attribution; no primary survey or field data collection was undertaken for this paper. Where government-

sourced efficiency data and independently sourced exclusion data address the same programme, both are reported side by side to allow triangulation, consistent with the research gap identified in Section 2.5.

IV. DATA AND STATISTICAL OVERVIEW

4.1 Sector-wise DBT Savings (2013–2024)

Table 1 summarises the sector-wise savings attributed to Aadhaar-linked DBT authentication by the 2025 government-commissioned assessment [3], [4], [5].

Table 1: Sector-wise DBT Savings and Outcomes, 2013–2024

Scheme / Sector	Reported Outcome	Value
Public Distribution System (PDS)	Share of total DBT savings	₹1.85 lakh crore (53%)
MGNREGS (wage payments)	Reported savings / on-time disbursal	₹42,534 crore; 98% on-time
PM-KISAN	Ineligible beneficiaries removed / savings	2.1 crore beneficiaries; ₹22,106 crore
All DBT schemes (cumulative)	Total reported savings, 2013–2024	₹3.48 lakh crore
Subsidy share of govt. expenditure	Change, 2013 to 2024	~16% → ~9%
Welfare Efficiency Index (composite)	Change, 2014 to 2023	0.32 → 0.91

Source: BlueKraft Digital Foundation (2025), as reported in *Business Today* (2025) and *The Tribune* (2025) [3], [4], [5].

4.2 Aadhaar Authentication Failure Statistics

Table 2 presents independently reported authentication failure data, which stands in contrast to the efficiency figures in Table 1 and substantiates the exclusion literature reviewed in Section 2.2.

Table 2: Aadhaar Authentication Volume and Failure Rate

Metric	Reported Value
Estimated monthly authentication attempts (welfare, banking, public services)	~312 million
Estimated monthly authentication failures	~20.3 million (~6.5%)
Laboratory-controlled biometric accuracy rate	98–99%
Trend in failure rate over past decade	Largely unchanged
Populations disproportionately affected	Elderly, manual labourers, persons with disabilities

Source: Policy Circle (2026) [7]; *Biometric Update* (2025), citing Public Accounts Committee testimony [6].

4.3 Health and Education Data Infrastructure Coverage

Table 3 reports the scale of data-linkage in the two domains into which the Aadhaar-linked identity model has most recently been extended.

Table 3: ABDM and APAAR Coverage Statistics

Programme	Metric	Reported Value
ABDM (health)	Linked digital health records (as of mid-2026)	> 104 crore
ABDM (health)	Enrolment basis	Voluntary, consent-based (Health ID)
APAAR (education)	Enrolled students	> 233 million
APAAR (education)	Schools covered (UDISE+, 2024–25)	> 1.47 million
APAAR (education)	Standalone data-protection law/policy at rollout	None identified

Source: IAS Parliament (2026) [12]; *Education For All in India* (2025), citing UDISE+ 2024–25 data [17]; Internet Freedom Foundation (2024) [16].

4.4 Legal and Regulatory Timeline

Table 4: Key Legal and Regulatory Milestones

Year	Milestone
2016	Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act enacted
2017	Supreme Court recognises privacy as a fundamental right (Puttaswamy I) [10]
2018	Supreme Court upholds Aadhaar Act; strikes down Section 57 private use (Puttaswamy II / Aadhaar judgment) [11]
2021	Ayushman Bharat Digital Mission launched
2023	Digital Personal Data Protection Act enacted (August); APAAR launched
2025	DPDP Rules, 2025 notified (13 November); Data Protection Board operationalised [18], [19]
2027 (projected)	Full DPDPA compliance timeline concludes (May)

V. RESULTS AND DISCUSSION

5.1 Efficiency Gains in Welfare Delivery

The data in Table 1 indicate a substantial, government-documented efficiency gain from Aadhaar-linked DBT, with the Public Distribution System accounting for the majority of reported savings. The Welfare Efficiency Index's near-tripling between 2014 and 2023 suggests a consistent scaling of these gains over time. However, because this index and the underlying savings figures are drawn from a non-independently audited, government-commissioned report, they should be read as an official efficiency narrative that measures fiscal leakage reduction rather than beneficiary-level access outcomes - a distinction elaborated in Section 5.2.

**Figure 1: Sector-wise DBT Savings, 2013-2024
(Total: ₹3.48 lakh crore)**

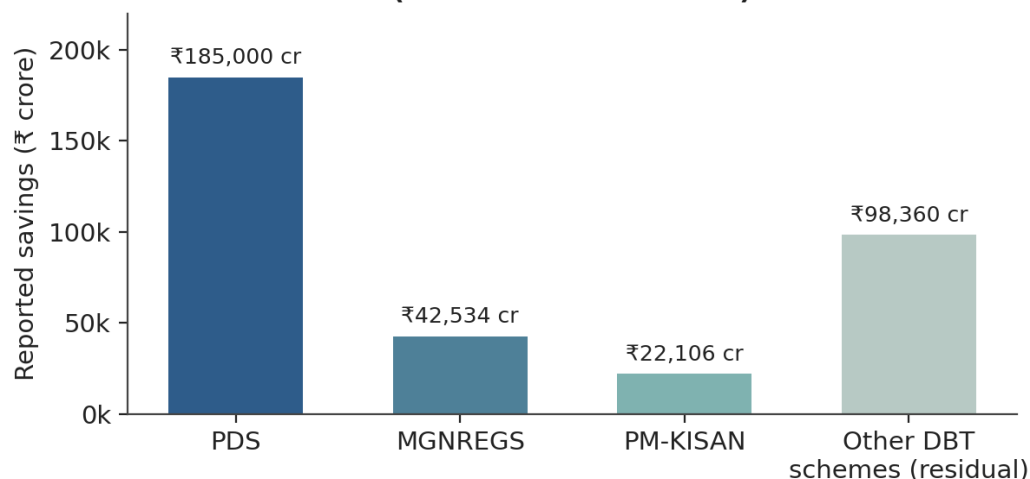


Figure 1 source: BlueKraft Digital Foundation (2025), as reported in *Business Today* (2025) and *The Tribune* (2025) [3], [4], [5]; “Other DBT schemes” is a residual calculated as total reported savings minus the three named schemes.

5.2 Exclusion Costs and Authentication Failure

Table 2 shows that authentication failure affects an estimated 6.5% of all monthly Aadhaar-based transactions, a rate that has not materially improved over a decade despite high controlled-environment accuracy. Read against Table 1, this indicates that fiscal savings and beneficiary-level exclusion are simultaneous, not sequential, outcomes of the same authentication architecture: the mechanism that removes ineligible or duplicate beneficiaries (Table 1) is the same mechanism that denies access to a meaningful share of eligible beneficiaries (Table 2), particularly among elderly, disabled, and manual-labour populations whose biometric characteristics are most likely to fail matching. This finding directly substantiates the exclusion typology developed in the literature reviewed in Section 2.2 and Justice Chandrachud's proportionality concerns in the 2018 judgment (Table 4).

Figure 2: Monthly Aadhaar Authentication Outcomes (~312 million attempts)

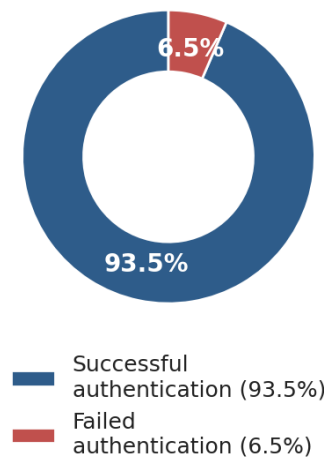


Figure 2 source: Policy Circle (2026) [7]; Biometric Update (2025) [6]. A 6.5% monthly failure rate across ~312 million attempts implies roughly 20.3 million failed authentications each month.

5.3 Health Data Governance: ABDM

With over 104 crore linked health records (Table 3), ABDM has achieved a scale broadly comparable to Aadhaar's own identity coverage, despite being formally voluntary. Its stated function of generating anonymised datasets for public health planning replicates the third “data aggregation” function identified in the conceptual framework of this paper, but - unlike DBT - without an equivalent efficiency-versus-exclusion evidence base of the kind presented in Tables 1 and 2. This represents a specific gap for future empirical research: no comparable authentication-failure or exclusion dataset for ABDM currently exists in the public domain.

5.4 Education Data Governance: APAAR

APAAR's coverage of over 233 million students across 1.47 million schools (Table 3) was achieved without a standalone data-protection law or notified policy at the time of rollout [16], a regulatory gap that is particularly significant because the data subjects are, in the large majority of cases, minors. This mirrors the “infrastructure preceding regulation” pattern documented for DBT and ABDM (Table 4) and represents the most acute version of the sequencing concern identified in this paper, given the heightened protections the DPDP Act, 2023 assigns to children's data once the Act becomes fully operative.

5.5 Legal and Regulatory Adequacy

Table 4 shows that all three data infrastructures examined in this paper - Aadhaar/DBT (2009–2013), ABDM (2021), and APAAR (2023) - were launched and substantially scaled before India's general-purpose data protection statute became operationally enforceable in November 2025. This consistent sequencing across three independently governed domains suggests a structural, rather than domain-specific, pattern in Indian digital governance design, in which infrastructure deployment routinely precedes regulatory capacity.

VI. CRITICAL ANALYSIS AND CHALLENGES

Three cross-cutting challenges emerge from the data and discussion above:

- (a) Authentication-linked exclusion is structural, not incidental. The 6.5% authentication failure rate (Table 2) has persisted for over a decade despite technical accuracy improvements, indicating that the exclusion problem is one of policy design - specifically, the absence of a statutorily guaranteed, non-discretionary alternative authentication route - rather than a solvable technical defect.
- (b) Regulatory sequencing has been consistently reversed. In welfare, health, and education alike (Table 4), data infrastructure preceded enforceable data protection regulation by several years, creating an accountability gap during each system's highest-growth phase. Figure 3 quantifies this gap across the three systems examined in this paper: Aadhaar/DBT operated for sixteen years, ABDM for four years, and APAAR for two years before the DPDP Rules, 2025 made India's data-protection statute enforceable. The shrinking gap across successive systems suggests policymakers have partially internalised the sequencing problem, but even the shortest gap (APAAR) covers the scheme's entire high-growth enrolment phase.

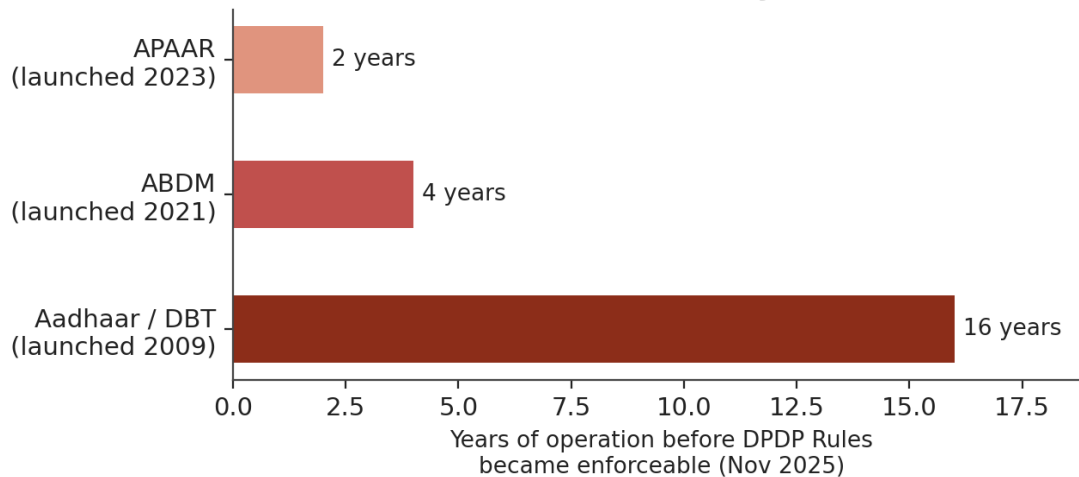
Figure 3: Infrastructure-Ahead-of-Regulation Gap Across Three Data Systems

Figure 3 source: constructed by the author from programme launch dates and the DPDP Rules, 2025 notification date [11], [18], [19] (Table 4).

(c) Function creep follows a repeatable “voluntary-mandatory” design pattern. APAAR's civil-society-documented shift from formally voluntary to practically compulsory enrolment [16] echoes early Aadhaar enrolment dynamics and is a pattern policymakers should anticipate and pre-empt in future digital-identity extensions, including further scaling of ABDM.

VII. CONCLUSION AND RECOMMENDATIONS

This review finds that India's Aadhaar-linked data governance model has delivered measurable, government-documented fiscal efficiency in welfare delivery, while simultaneously sustaining a persistent and independently documented exclusion cost among vulnerable populations, and extending - largely unaudited on the exclusion dimension - into health and education. The consistent pattern of infrastructure preceding regulation across three independently governed domains (Table 4) is the paper's central finding and its primary contribution to the literature synthesised in Section II.

Figure 4 summarises the two headline efficiency indicators discussed in Section 5.1 at a glance: the fall in subsidy share of government expenditure from 16% (2013) to 9% (2024), and the near-tripling of the composite Welfare Efficiency Index from 0.32 (2014) to 0.91 (2023). Read alongside Figures 2 and 3, this snapshot illustrates the paper's core tension - genuine fiscal efficiency gains, achieved through an authentication architecture with a persistent exclusion cost, deployed years ahead of enforceable data-protection regulation.

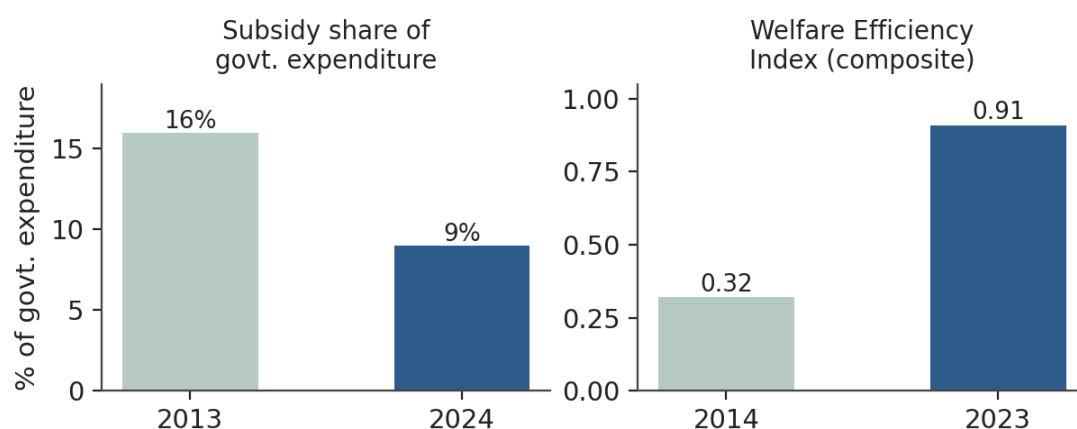
Figure 4: Reported Efficiency Gains — Before vs. After DBT Scale-Up

Figure 4 source: BlueKraft Digital Foundation (2025), as reported in *The Tribune* (2025) [3], [5] (Table 1).

Based on this analysis, the paper recommends: (i) mandatory, independently audited (CAG-level) beneficiary-exclusion reporting alongside all future DBT efficiency assessments; (ii) statutory, non-discretionary exception-handling routes for biometric authentication failure in welfare, health, and education; and (iii) sequencing future digital-identity extensions after, not ahead of, an operative data-protection enforcement mechanism, with particular urgency where data subjects are minors, as in APAAR. Future doctoral research should prioritise independent, field-based quantification of ABDM and APAAR exclusion - an evidence base that, unlike DBT, does not yet exist - and doctrinal analysis of how the DPDP Act's state exemptions will be tested against the proportionality standard set out in the 2018 Aadhaar judgment.

REFERENCES

- [1] Dreze, J., & Khera, R. (2017). Recent social security initiatives in India. *World Development*, 98, 555–572.
- [2] World Bank. (2016). *World Development Report 2016: Digital Dividends*. World Bank Group.
- [3] BlueKraft Digital Foundation. (2025). *A Quantitative Assessment of India's DBT System* [Policy report].
- [4] Business Today. (2025, April 23). DBT system delivers big: Rs 3.48 lakh crore saved, subsidy share falls to 9%. <https://www.businesstoday.in/latest/economy/story/dbt-system-delivers-big-rs-348-lakh-crore-saved-subsidy-share-falls-to-9-473240-2025-04-23>
- [5] The Tribune. (2025, April 21). DBT saves Rs 3.48 lakh crore, records 16-fold surge in beneficiaries: Report. <https://www.tribuneindia.com/news/business/dbt-saves-rs-3-48-lakh-crore-records-16-fold-surge-in-beneficiaries-report/>
- [6] Biometric Update. (2025, July 18). High rates of Aadhaar biometric verification failure leads to UIDAI scrutiny. <https://www.biometricupdate.com/202507/high-rates-of-aadhaar-biometric-verification-failure-leads-to-uidai-scrutiny>
- [7] Policy Circle. (2026). Aadhaar authentication failures trigger an invisible exclusion crisis. <https://www.policycircle.org/opinion/aadhaar-authentication-failures/>
- [8] Economic and Political Weekly. (2019, April 5). Aadhaar failures: A tragedy of errors. EPW Engage. <https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare>
- [9] India Stack Exclusion Tracker. (2026). Human cost of India Stack: Deaths, denials, exclusion. <https://indiastack.in/exclusion/>
- [10] Supreme Court of India. (2017). *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (right to privacy judgment).
- [11] Supreme Court of India. (2018). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar judgment, decided 26 September 2018).
- [12] IAS Parliament. (2026). Ayushman Bharat Digital Mission (ABDM). <https://www.shankariaspakistan.com/current-affairs/ayushman-bharat-digital-mission-abdm>
- [13] Vajiram & Ravi. (2024). APAAR ID – One Nation, One Student ID initiative. <https://vajiramandravi.com/current-affairs/apaar-id/>
- [14] Business Today. (2024, December 5). One nation, one student ID: What is APAAR card? <https://www.businesstoday.in/amp/technology/news/story/one-nation-one-student-id-what-is-apaar-id-card-what-every-parent-should-know-benefits-and-more-456236-2024-12-05>
- [15] IAS Gyan. (2024). Automated Permanent Academic Account Registry (APAAR). <https://www.iasgyan.in/daily-current-affairs/automated-permanent-academic-account-registry-apaar>
- [16] Internet Freedom Foundation. (2024, May 1). One nation, one student ID, zero law or policy to back it up. <https://www.internetfreedom.in/student-id-zero-law-or-policy/>
- [17] Education For All in India. (2025). CBSE's relaxed guidelines on APAAR IDs amid data integration challenges. <https://educationforallindia.com/cbse-relaxed-guidelines-on-apaar-ids-amid-data-integration-challenges-2025/>
- [18] Hogan Lovells. (2025). India's Digital Personal Data Protection Act 2023 brought into force. <https://www.hoganlovells.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force->
- [19] Mondaq. (2025). Notification of Digital Personal Data Protection law in India: Certain key timelines. <https://webiis10.mondaq.com/india/privacy-protection/1710998/notification-of-digital-personal-data-protection-law-in-india-certain-key-timelines>

Author's Note (remove before submission): Formatted to match the structure of the attached journal template - title/author block, Abstract/Keywords, submission-date rule, Roman-numeral sections, and bracket-numbered references. Please (a) insert your actual institutional affiliation and email, (b) verify Tables 1–4 against the primary BlueKraft Digital Foundation report and any CAG audit before submission, and (c) confirm the exact font, spacing, and citation style required by your specific target journal, as these vary across UGC-CARE/Scopus-indexed outlets even where the general template structure is similar.