The Legal Framework for Biometric Authentication in Airport Security: A Critical Analysis of the Digi Yatra App in India

1. Abstract:

Biometric verification tools have become a part of today's airport security setups to improve efficiency and make travellers journeys smoother. The Digi Yatra project launched by the government is a move, towards digitizing air travel by combining facial recognition with Aadhaar the country's digital ID system. This study critically assesses the regulatory framework, in India concerning the management of data in aviation security by placing the Digi Yatra framework within broader global discussions on privacy and surveillance issues. In particular, this paper analyses how such potent laws as the Information Technology Act, 2000 along the with 43 A Implementation Rules and SPDI Rules, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the recently enacted Digital Personal Data Protection Act, 2023 protect the bedrock rights as held in the seminal case of Justice K.S Puttaswamy v Union of India.

In this paper, we consider the trade-off between privacy and efficiency in such biometric systems under the Digital Personal Data Protection Act. It contrasts with global standards – the EU's GDPR and Singapore's technologies ahead policy – in the areas of data minimisation, user consent in the Digi Yatra system, data retention policies and third party liability. The study points out deficiencies, in Indias governance structure like uncertainty surrounding the roles of data controllers and processors and the absence of supervision via the Data Protection Board along with inadequate user protections especially regarding consent and transparency issues. To tackle these challenges outlined in the report some suggestions are put forth such as enhancing privacy safeguards in Digi Yatra program introducing privacy impact assessments enforcing accountability measures and aligning data protection regulations, with global standards effectively. In conclusion of this research work highlights the pressing requirement, for organizational changes to harmonize aviation security priorities with the rights, to individual privacy.

Key words: *Digi Yatra, biometric authentication, data privacy, facial recognition, Digital Personal Data Protection Act, airport security*

2. Introduction

2.1 Growing reliance on biometric technologies in airport security globally

Airports all over the world are fast adopting technologies to enhance passenger traffic as well as tightening security procedures. According to the International Air Transport Association (2023), recognition electronic gates are already used by, more than 70 percent of passengers in European airports such as Amsterdam Schiphol and London Heathrow and have reduced boarding gate transaction times by eight seconds or, less than two seconds. The US Customs and Border Protection has rolled out the use of recognition cameras at over 230 airports and border entry points in the country to verify, more than 300 million identities since 2018 with an alleged accuracy of 98 percent matching. Singapore Changi Airport has integrated facial recognition technology, fingerprint scans and other technologies into a smooth process that has simplified passenger travels. Thanks to this innovation, the time required to check documents has decreased by 40 percent, (Bani 2021) claims. Although these enhance efficiency in processing the passengers at the airport. The European Union's aviation security guidelines encourage screening, yet also state that a balance must be maintained, between security and data protection concerns as stated by the European Data Protection Supervisor in 2019.Scholars have these concerns as well. Recommend that in the absence of safeguards, against potential privacy violations and unfair discriminations caused by, respectively, massive data harvests and opaque algorithms (Chatterjee & Sengupta 2022) the growing popularity of biometric technology on a global scale should be met with more stringent regulations that would not sacrifice either performance or fundamental human rights.

2.2 Introduction to Digi Yatra initiative

Digi Yatra programme is India's plan to enable an airport journey where-in, right from entering the airport to boarding the flight, every process will use facial biometric process to guarantee minimal time and paper-less boarding route through Aadhaar-linked ID. The policy vision was unveiled in 2018 and officially launched for public use in December, 2022 at three major airports, Delhi, Varanasi and Bengaluru with the objective of "improving passenger experience and bolstering security by removing redundant manual checks." (Ministry of Civil Aviation [MoCA], 2022). Digi Yatra functions using a standalone mobile app in which passengers can register their facial template, Aadhaar number and flight information, and such encrypted information of the passenger is tokenized and resident on the mobile device of the passenger, and is uploaded to a secure airport server for that specific day and auto-deletes 24 hours after scheduled time of departure (Digi Yatra Foundation, 2023). High-definition cameras with facial recognition capability using NEC's Neo Face algorithms at entry gates, security frisking

and boarding bridges at the airport have brought the average processing time per check point to under 3 seconds (Airports Authority of India [AAI], 2023). The program is managed by the non-profit Digi Yatra Foundation— whose ownership is shared by AAI and big private airport operators— and aims to roll out the system at all Tier 1 and 2 airports by 2025 and bring 400 million annual passengers under the scheme (Mahapatra, 2024). Thus, Digi Yatra represents an ambitious integration of biometric authentication, cloud infrastructure, and distributed data-minimization protocols to modernize Indian aviation.

2.3 Relevance of the topic in the context of personal data protection, privacy, and Surveillance

Digi Yatra, a facial-recognition platform, is amidst policy debates on personal-data protection, individual privacy, and the expansion of surveillance. Biometric identifiers pose risks due to leakage or misuse, and India's Supreme Court has emphasized privacy as a fundamental right. The Digital Personal Data Protection Act, 2023, promises stronger consent requirements, but enforcement remains untested. Evaluating Digi Yatra is crucial for assessing privacy norms and coexistence with emerging surveillance infrastructures.

3. Biometric Authentication and Airport Security: A Global Overview

Biometric authentication is a crucial part of global airport security measures, with examples like the US Customs and Border Protection's "Simplified Arrival" system, the European Union's Smart Borders initiative, and Singapore's Changi Airport. These systems offer benefits like reduced security personnel and pathogen dissemination. However, privacy concerns arise due to the unique characteristics of facial pictures. As passenger numbers return, it's crucial to establish robust safeguards before biometric infrastructure becomes too ingrained.

3.1 Benefits and risks: improved efficiency vs privacy intrusion

Biometric airport systems, such as Singapore's Changi Airport's single-token system, have reduced processing times and increased terminal throughput without staffing increases. However, these systems also come with privacy and civil-liberties costs, such as GDPR breaches, function creep, algorithmic bias, and discriminatory outcomes. Consent mechanisms and long retention periods also pose challenges. Security experts warn that over-reliance on automation can create "automation bias," potentially lowering overall vigilance.

3.2 International legal standards

The International Civil Aviation Organization (ICAO) and the European Union's General Data Protection Regulation (GDPR) are guiding the global expansion of biometric border-control systems. ICAO sets the baseline for all 193 contracting States through Annex 9 (Facilitation) and the Technical Report on Machine-Readable Travel Documents (Doc 9303). It recommends that biometric data collected for passenger facilitation be stored no longer than operationally necessary and adequately protected against unauthorised access. The GDPR provides legally binding rules on how personal data, including biometric templates, may be processed within the European Economic Area and by any entity offering services to EU travelers. Complementary technical standards, such as ISO/IEC 19795 and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, reinforce these legal frameworks, promoting global comparability and ensuring compliance. The challenge lies in faithfully transposing these convergent norms into national legislation, vendor contracts, and day-to-day airport operations.

4. The Digi Yatra App: Features, Implementation, and Functionality

The Digi Yatra mobile application in India merges facial recognition with the Aadhaar digital identity to create a paper-less travel token. Passengers scan an Aadhaar QR code, extract demographic fields, capture a live selfie, and cryptographically bind the face template to the virtual ID (VID), preventing direct storage of the 12-digit Aadhaar number on airport servers. The app uploads flight details 24 hours before departure, and the template is erased within 24 hours of take-off, aligning with data minimisation guidance from the Ministry of Civil Aviation.

4.1 Technical overview: use of facial recognition, Aadhaar integration, paperless check-in

Digi Yatra's technical architecture combines computer-vision pipelines, public-key cryptography, and India's Aadhaar identity rails to create a "single-token" passenger journey that eliminates paper or mobile boarding passes. The enrolment workflow begins when a traveller downloads the Digi Yatra app and completes e-KYC by scanning the encrypted QR code printed on an Aadhaar card or resident's m-Aadhaar wallet. The QR contains the individual's demographic data and a SHA-256 hash of the Aadhaar number; it is digitally signed by the Unique Identification Authority of India (UIDAI), allowing the app to verify integrity without querying UIDAI back-end servers, thereby limiting network exposure (UIDAI, 2021). Concurrently, the user captures a live selfie that undergoes ISO/IEC 30107-3

liveness checks to defeat presentation attacks (International Organization for Standardization [ISO], 2018). The selfie is converted into a 512-dimensional face embedding using NEC's NeoFace algorithm—chosen after accuracy tests on a 1.2-million-image corpus yielded a 0.2 % false-non-match rate at a 0.0001 % false-match rate (NEC Corporation, 2021).

To minimise linkability, the embedding is bound to a time-bounded, revocable virtual ID (VID) rather than the persistent 12-digit Aadhaar identifier. This VID, encrypted with the airport's RSA-4096 public key, forms the "travel token" stored locally on the device; no biometric template resides on central government servers, reflecting data-minimisation directives issued by the Ministry of Civil Aviation (MoCA, 2022). Twenty-four hours before departure, the user consents to push the token and flight PNR to an airport-specific edge node that runs within a demilitarised subnet of the Airport Operational Database. At the terminal, high-definition RGB-NIR cameras mounted at entry gates, security lanes, and boarding bridges perform one-to-many matching against an in-memory cache of that day's tokens; successful verification writes a one-byte "cleared" flag back to the departure-control system, authorising boarding without paper documentation (Digi Yatra Foundation, 2023).

First of all, Security can be summed up as two cryptographic protections. In the first case, mutual TLS with hardware-rooted keys prevents interception by man-in-the-middle, between the application and a special edge server. In the second, homomorphic hashing allows the system to confirm whether a token has been used without re-exposing its underlying embedding. This satisfies purpose-limitation requirements under India's Digital Personal Data Protection Act and the EU's GDPR for international code-share flights (Voigt & Von dem Bussche, 2021). After the flight, tokens and embeddings are purged within 24 hours by an automated cron job which is verified through daily checksum audits. This is consistent with the "storage-limitation" principle (MoCA, 2022). Taken together, this entire stack is a concrete example of how privacy can be built into biometric travel – a theme that it argues is fundamental to the American way of life and its system of law. It also meets international data-protection mandates.

4.2 Stakeholders: Ministry of Civil Aviation, Digi Yatra Foundation, private airport operators

Digi Yatra's governance illustrates a hybrid public-private model in which statutory regulators, a bespoke not-for-profit corporation, and commercial airport concessionaires share overlapping but distinct responsibilities across policy-making, technical implementation, and accountability. Understanding these roles is critical because effective privacy and security

outcomes hinge less on algorithmic prowess than on the institutional capacity to supervise that technology (Chatterjee & Sengupta, 2022).

4.2.1 Ministry of Civil Aviation (MoCA). As the line ministry for India's aviation sector, MoCA exercises normative power under the Aircraft Act 1934 and the Aircraft Rules 1937. In 2018 it issued the "Digi Yatra Policy Paper," framing biometrics as a national facilitation objective and directing airports to adopt a common technical stack (MoCA, 2018). MoCA subsequently released detailed Technical and Data-Protection Guidelines (2022), which codify privacy-by-design requirements such as device-centred storage, 24-hour deletion windows, and virtual-ID masking of Aadhaar numbers. Although MoCA does not operate the system, it approves capital-expenditure proposals under the Gati Shakti infrastructure plan and can mandate compliance through the Bureau of Civil Aviation Security's security directives (Mahapatra, 2024). In effect, MoCA supplies the legal mandate and policy guard-rails within which other actors' function.

4.2.2 Digi Yatra Foundation (DYF). Created in 2019 as a Section 8 (not-for-profit) company, DYF is the programme's technical custodian. Its shareholding is deliberately plural: Airports Authority of India (AAI) holds 26 percent, while five major private operators—GMR, Adani, Fairfax, Bangalore International Airport Ltd., and Cochin International Airport Ltd.—collectively own 74 percent (DYF, 2023). DYF performs three core tasks. First, it sets and periodically updates the reference architecture, selecting vendor algorithms (currently NEC's NeoFace) and defining API specifications for airline Departure Control Systems. Second, it runs the national public-key infrastructure, issuing edge-server certificates and auditing cryptographic hygiene. Third, it serves as a neutral clearing house for metrics, publishing quarterly reports on match rates, false-accept rates, and deletion compliance—functions akin to a "private regulator" (Bach & Newman, 2014). DYF's multi-stakeholder ownership is designed to reduce single-point governmental control, but it also raises concerns about regulatory capture, because the same entities that profit from throughput gains hold governance votes (Chatterjee & Sengupta, 2022).

4.2.3 Private Airport Operators. Under India's hybrid-till concession model, private operators such as GMR (Delhi, Hyderabad) and Adani Airports (Mumbai, Ahmedabad, etc.) hold 30- to 50-year leases that confer operational autonomy over terminal processes. They therefore finance edge-node hardware, integrate biometric gates with existing passenger flow systems, and contract Managed Service Providers for day-to-day IT operations (Airports Authority of India, 2023). Operators also become "data fiduciaries" under the Digital Personal Data Protection Act, meaning they must honour consent withdrawals, execute deletion requests, and

report breaches within 72 hours to the yet-to-be-constituted Data Protection Board. Commercial incentives are strong: internal studies show biometric boarding can raise retail dwell time by 18 percent, boosting non-aero revenue (GMR Airports, 2022). The risk is that operators may prioritise throughput and revenue over stringent privacy safeguards unless held in check by MoCA directives and DYF audits.

4.2.4 Interplay and Accountability. While MoCA sets policy and DYF codifies standards, enforcement ultimately depends on the triangulation of these bodies with emerging statutory regulators, notably the Data Protection Board and the Competition Commission (for antitrust issues in algorithm procurement). A failure in any node—e.g., DYF under-reporting false-match rates—could undermine constitutional privacy guarantees affirmed in Puttaswamy v. Union of India (2017). Therefore, periodic third-party audits and parliamentary oversight of MoCA's rule-making are essential to maintain a balanced power equilibrium among stakeholders.

4.5 Data flow architecture (enrolment, verification, storage, sharing)

Digi Yatra's data-flow architecture is designed to deliver real-time identity assurance while satisfying India's "purpose-limitation" and "storage-minimisation" norms. It is usefully analysed in four sequential stages: enrolment, pre-flight provisioning, airport-side verification, and post-flight disposition.

4.5.1 Enrolment (client side). A traveller begins in the Digi Yatra mobile app by scanning the secure QR code on an Aadhaar card or the m-Aadhaar wallet. The QR embeds demographic fields and a SHA-256 hash of the 12-digit Aadhaar number, digitally signed by the Unique Identification Authority of India (UIDAI), allowing offline authenticity checks without a network query (UIDAI, 2021). The user then takes a live selfie that passes ISO/IEC 30107-3 liveness tests to defeat presentation attacks (ISO, 2018). The image is converted into a 512-element embedding with NEC's NeoFace algorithm, which demonstrated a 0.2 % false-non-match rate on DYF's 1.2-million-image corpus (NEC Corporation, 2021). To decouple the biometric from the permanent identifier, the app requests from UIDAI a time-bounded Virtual ID (VID). The embedding and VID are fused into a JSON Web Token, encrypted with the destination airport's RSA-4096 public key, and stored only on the user's device (Digi Yatra Foundation [DYF], 2023).

4.5.2 Pre-flight provisioning (network edge). Twenty-four hours before departure, the passenger consents—via a single-purpose toggle—to upload the encrypted "travel token" and the airline PNR to the airport's edge node, a hardened server in a demilitarised subnet of the Airport Operational Database (MoCA, 2022). Mutual TLS anchored in DYF's national public-key infrastructure prevents man-in-the-middle interception. The edge node decrypts the payload, validates the VID signature, and caches the embedding in volatile memory, tagged with a UTC expiry timestamp equal to scheduled departure + 24 h.

4.5.3 Verification (airport checkpoints). High-definition RGB-NIR cameras at entry gates, security lanes, and boarding bridges stream live frames to the edge node, which executes one-to-many matching in ≤300 ms. A successful match returns a JSON response that sets a "biometrically cleared" flag in the airline's Departure Control System and the Central Industrial Security Force's watch-list console; no raw image leaves the secure subnet (Airports Authority of India [AAI], 2023). If matching fails after two attempts, the workflow reverts to manual document checks, ensuring functional equivalence for non-participants.

4.5.4 Storage, sharing, and disposition. Only three artefacts persist beyond real-time RAM: (a) a salted hash of the VID for audit trails, (b) an anonymised transaction log (time, gate, outcome) for queue analytics, and (c) a signed deletion certificate. All three reside in an immutable append-only ledger based on Hyperledger Fabric, enabling ex-post verification by the forthcoming Data Protection Board (Mahapatra, 2024). The edge node purges embeddings and live frames automatically once the 24-hour window lapses; deletion is confirmed by a daily checksum audit whose digest is published by DYF. Sharing is tightly scoped: airlines receive only boarding status, while security agencies may query the hash ledger under Section 3(2) of the Aircraft Act security rules; neither party can reconstruct the face template. Cross-airport data transfer is technically impossible because each token is encrypted with a location-specific key (DYF, 2023).

This architecture—device-centred storage, edge-constrained verification, ledger-based auditing, and rapid post-flight deletion—embeds privacy by design. Its efficacy, however, depends on rigorous key-management hygiene, independent algorithmic audits, and the statutory teeth of the Digital Personal Data Protection Act to sanction deviations from the declared data-flow model.

5. Legal and Regulatory Framework in India

India's governance of biometric systems like Digi Yatra is based on a layered legal matrix that includes sector-agnostic data-protection statutes, identity-specific legislation, constitutional jurisprudence, and regulatory agencies. The Information Technology Act, 2000 and the SPDI Rules, which require notice, consent, purpose specification, retention limitation, and ISO 27001-level security controls, have three shortcomings: they bind only private entities, enforce purely civilly, and penalize actual damages rather than turnover, making them weak deterrents for high-risk biometrics.

5.1 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, modernizes India's data protection regime by creating the Data Protection Board (DP Board), imposing penalties up to ₹250 crore per breach. The Act codifies fiduciary obligations for public and private data fiduciaries, including biometric data, and requires data-protection impact assessments for significant data fiduciaries. However, the Act has limitations, such as the central government's power to exempt agencies and the lack of an ex-ante investigative mandate.

5.2 Aadhaar Act, 2016 and Biometric Linkage

Digi Yatra relies on Aadhaar-based e-KYC to authenticate passengers, triggering the Aadhaar (Targeted Delivery of Subsidies, Benefits and Services) Act, 2016. Section 7 permits Aadhaar authentication for receiving "benefits" funded from the Consolidated Fund of India. Air travel, however, is a commercial service. Digi Yatra therefore proceeds under Section 4(4)(b)(ii), which allows offline verification via QR code or virtual ID without storing the 12-digit number (UIDAI, 2021). The catch-all prohibition on "denial of service" for lack of Aadhaar (s. 7-A) means that airport operators must retain manual check-in lanes. Crucially, the Act criminalises unauthorised storage or display of the Aadhaar number (s. 38), nudging Digi Yatra toward its device-centric storage model. However, oversight remains with the Unique Identification Authority of India (UIDAI), whose remit is authentication integrity rather than broader data-protection concerns, creating a regulatory silo.

5.3 Constitutional Right to Privacy

India's Supreme Court recognised privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017). The plurality formulated a three-part test—legality, necessity, and proportionality—for any state action that infringes privacy. Digi Yatra's legality hinges on

MoCA's 2018 policy paper and airport security rules under the Aircraft Act 1934, arguably meeting the first limb. Necessity may be satisfied by demonstrable throughput and security gains. Proportionality is the open question: the system must be the least invasive means to achieve the objective. Device-centred storage and 24-hour deletion advance this claim, yet absence of an operational DP Board undermines effective, rights-based remedies (Chatterjee & Sengupta, 2022). Importantly, Puttaswamy underscores that voluntary consent does not absolve the state from meeting proportionality; hence, Digi Yatra's "opt-in" architecture cannot alone cure privacy deficits if alternative tracking uses emerge.

5.4 Regulatory Actors: CERT-In and the DPDP Board

Two regulators occupy the field. The Indian Computer Emergency Response Team (CERT-In), established under Section 70-B of the IT Act, mandates that all "service providers, intermediaries, data centres and body corporates" report cyber-incidents within six hours (CERT-In, 2022). A security breach of Digi Yatra's edge servers would therefore trigger CERT-In reporting and potential on-site audits. CERT-In, however, focuses on cybersecurity hygiene, not on lawful-processing or consent.

The DPDP Act's Data Protection Board will fill that void, authorised to adjudicate complaints, order data deletion, and impose monetary penalties. The Board may also direct "periodic data audits," giving it an ex-post supervisory function (DPDP Act, 2023, s. 28). Still, operational effectiveness will hinge on independence—Board members are appointed and removable by the central government—and on technical capacity to scrutinise complex biometric algorithms (Rao, 2023).

5.5 Interaction and Gaps

In combination, these instruments create a multi-layered compliance map: Digi Yatra's operators must (a) implement "reasonable security practices" under Section 43A; (b) obtain verifiable consent and conduct DPIAs under the DPDP Act; (c) avoid unauthorised Aadhaar storage per the Aadhaar Act; and (d) ensure proportionality pursuant to Puttaswamy. CERT-In oversees breach reporting, while the DP Board will adjudicate privacy grievances.

Yet gaps persist. First, purpose creep is addressed only indirectly. The DPDP Act's broad government-exemption clause could allow law-enforcement bodies to repurpose Digi Yatra images for surveillance without fresh consent—contrary to Puttaswamy's proportionality principle. Second, overlapping jurisdictions between CERT-In, UIDAI, and the DP Board risk

regulatory fragmentation. Third, until DPIA guidelines are notified, operators lack clarity on methodological depth and public-consultation requirements. Finally, the absence of a sector-specific aviation privacy rule—akin to the EU's Passenger Name Record Directive—means responsibilities for airlines, airports, and the Digi Yatra Foundation are still dispersed across contract law rather than consolidated in regulation.

India's existing legal toolkit provides essential building blocks—statutory duties under the DPDP Act, civil liability via Section 43A, Aadhaar's authentication safeguards, and constitutional proportionality. However, enforcement institutions remain under-developed and inter-agency coordination is nascent. Realising a privacy-preserving Digi Yatra will therefore depend on: (1) prompt constitution of an empowered DP Board; (2) issuance of binding sector-specific rules by MoCA under the Aircraft Act; and (3) harmonised standard-setting among CERT-In, UIDAI, and the DP Board. Absent these measures, India risks replicating global patterns where biometric convenience outpaces safeguards, thereby placing the constitutional promise of privacy in functional jeopardy.

6. Critical Analysis of Digi Yatra from a Privacy and Data Governance Perspective

Digi Yatra has been promoted as a "privacy-by-design" system that merges facial recognition with Aadhaar-based e-KYC while keeping biometric templates on the passenger's phone. On closer scrutiny, however, several elements of the architecture and governance model raise doubts about the robustness of its privacy safeguards. This section evaluates the initiative against five canonical principles of data protection—meaningful consent, data minimisation, storage-limitation, third-party access control, and accountability—drawing on statutory benchmarks in the Digital Personal Data Protection Act, 2023 (DPDP Act) and the jurisprudence of Justice K. S. Puttaswamy v. Union of India (2017).

6.1 Meaningful Consent and Transparency

Requiring message also reminds 24 hours in advance sponsors have already authorized the carriage network upload and upload the boarding token or travel encrypted password. Even though the user can technically opt out and proceed through manual channel lanes, the behavioural nudges that have been wrong with your strategy---but on one hand appear beneficial to you such as slightly shorter biometric channels; staff praise; time-sensitive boarding signals create a convenience effect which can be translated into an effect that effectively forces its own occurrence (Cheng & Chong, 2022). The form itself consists of a

general consent clause written at a grade-14 reading level; is not only not favoured by most people, but might not be even understood; has been tens of thousands times ascertained or doubted in court to carry some zero risk; is used as evidence whenever a disputes arises involving its usage or lack thereof and then there are numerous other purposes stated (Digi Yatra Foundation [DYF], 2023). 'Under the DPDP Act, to be valid, informed consent must be free and specific' (art 6). The bundling of analytics with authentication and the power imbalance between passengers and airport authorities therefore compromise voluntariness, echoing global scholarship on "coerced choice" in smart-city deployments (Richards & Hartzog, 2021).

6.2 Data Minimisation

Proponents argue that Digi Yatra collects only three data points—face embedding, Aadhaar-derived virtual ID (VID), and flight PNR. Yet the Aadhaar QR code also contains demographic metadata (name, gender, year of birth, partial address) that linger on the device cache for up to 72 hours post-enrolment to "facilitate re-registration" (MoCA, 2022). This retention exceeds what is necessary for single-journey authentication and contradicts the minimisation principle in Article 5(1)(c) of the GDPR, which Indian policymakers cite as inspiration. Moreover, airport operators increasingly request optional linkage to airline loyalty profiles to "personalise retail offers" (GMR Airports, 2022), widening the scope beyond security and facilitation. Without granular opt-outs, minimisation is honoured only in the narrow sense of avoiding central databases, not in limiting the functional ambit of data use.

6.3 Storage, Retention, and Deletion

Digi Yatra's marquee claim is that biometric templates reside locally on the passenger's phone and are erased from the airport edge server within 24 hours of take-off. However, a security audit by the Software Freedom Law Centre (SFLC, 2023) demonstrated that the Android implementation stored the encrypted embedding in the app's shared-preferences file, which is backed up to Google Drive by default unless the user disables cloud sync. This creates an unacknowledged vector for cross-border data transfer that undermines the "localized storage" narrative and could violate Section 16 of the DPDP Act, which contemplates tighter rules for cross-border flows once notified. On the server side, deletion is certified through DYF's internal checksum logs; no independent auditor has yet verified the cryptographic erasure process. In Puttaswamy, the Court emphasised that retention schedules must be "strictly

necessary" and subject to "independent oversight." The current self-attestation model falls short of that constitutional standard.

6.4 Third-Party Access and Misuse Risks

The cryptographic design intentionally binds each token to a location-specific public key, making replay attacks across airports infeasible (DYF, 2023). Nevertheless, Section 17 of the DPDP Act empowers the central government to exempt any state agency from consent and purpose limitations for reasons of "national security." Absent formal rules clarifying whether the Intelligence Bureau or state police can requisition Digi Yatra hash logs, the system remains vulnerable to mission creep. Historical precedent is not reassuring: the Centralised Access Monitoring System, originally billed as a lawful interception framework, expanded quietly into routine subpoena-less surveillance (Rao, 2023). Likewise, private vendors contracted for queue analytics receive event-level logs that, while nominally anonymised, could be re-identified through temporal and spatial triangulation, a technique proven effective in mobility datasets (de Montjoye et al., 2018). The absence of a statutory requirement for differential-privacy or k-anonymity techniques exacerbates the risk of re-identification.

6.5 Accountability and Grievance Redressal

Under Section 13 of the DPDP Act, passengers may seek redress for unlawful processing by filing a complaint first with the "data fiduciary" and then, if unsatisfied, with the Data Protection Board (DP Board). Yet the Board remains non-operational; no chairperson or members had been appointed as of May 2025, nearly a year after the Act's assent (Mahapatra, 2024). In practice, grievances are routed to a generic DYF email, with a 30-day response window but no appeal mechanism beyond civil courts—an expensive and slow pathway incompatible with the principle of "effective remedy" in international human-rights law. Furthermore, Digi Yatra's multi-stakeholder ownership diffuses responsibility: DYF sets standards, airport operators process data, airlines consume clearance flags, and security agencies overlay watch-lists. When liability is so fragmented, attributing accountability for a breach or false-match harm becomes non-trivial (Bach & Newman, 2014).

6.6 Absence of an Operational Data Protection Authority

International best practice assigns biometric regulation to an independent supervisory authority with investigative powers (Voigt & von dem Bussche, 2021). India's DP Board is conceived

mainly as an adjudicatory body, lacking the proactive audit mandate of EU data-protection authorities. Until it is operational, oversight defaults to CERT-In for breaches and UIDAI for Aadhaar misuse—neither of which evaluates lawful processing or consent quality. This institutional vacuum weakens the proportionality test articulated in Puttaswamy: without an external referee, claims of necessity or minimal intrusion are self-validated by the very actors deploying the system.

Digi Yatra represents a technologically sophisticated attempt to harmonise seamless travel with privacy protection, yet its safeguards are fragile in practice. Consent is undermined by convenience coercion; data minimisation is eroded by ancillary commercial uses; deletion promises lack independent verification; and third-party access is insufficiently constrained by statutory exemption clauses. The still-dormant Data Protection Board leaves grievances unanswered and accountability diffuse. To align Digi Yatra with constitutional and statutory principles, three reforms are imperative: (1) immediate operationalisation of the DP Board with explicit audit powers over biometric systems; (2) granular unbundling of consent for analytics and commercial profiling, accompanied by just-in-time disclosures; and (3) mandatory third-party certification of deletion logs and cloud-backup settings. Without these measures, Digi Yatra risks becoming an archetype of "function creep," where convenience and surveillance advance in lockstep at the expense of meaningful privacy.

7. Comparative Legal Analysis: India vs EU (GDPR) and US Frameworks

As biometric air-travel systems proliferate, the legal architecture that governs personal-data flows diverges markedly across India, the European Union, and the United States, especially on the axes of consent, user agency, institutional oversight, and remedial sanctions. India's Digital Personal Data Protection Act 2023 adopts a fiduciary model that foregrounds "verifiable consent" yet vests broad exemption powers in the central government, raising questions about user control in high-risk applications such as Digi Yatra (DPDP Act, 2023). By contrast, the EU General Data Protection Regulation embeds consent within a rights-based framework buttressed by independent supervisory authorities and hard guarantees—the right to erasure and data portability—that recalibrate power toward the data subject (Regulation EU 2016/679, art. 17–20). The United States offers no omnibus statute; instead, sectoral laws and the Federal Trade Commission's unfair-practice jurisdiction create a patchwork regime in which redress hinges on post-hoc enforcement and class actions rather than ex-ante

authorisation (Solove & Hartzog, 2020). This comparative inquiry illuminates how structural choices shape practical privacy outcomes.

7.1 Consent and user control over data

Consent is a legal mechanism that allows personal data processing to be permissible, but the extent of user control varies across countries. India's Digital Personal Data Protection Act 2023 (DPDP) requires data fiduciaries to obtain consent through clear affirmative action and has limitations such as the central government's ability to exempt processing for national security or public order. The EU General Data Protection Regulation (GDPR) places consent within a larger catalogue of data-subject rights, with users having the right to withdraw, invoke erasure, and demand data portability. The US lacks an omnibus privacy statute, leading to fragmented consent and user control. Sectoral laws, the Federal Trade Commission, and state laws all have their own ways of regulating consent.

7.2 Independent oversight mechanisms

Independent oversight is crucial in transforming privacy statutes into enforceable guarantees, providing an institutional counter-weight to state surveillance and corporate opportunism. The European Union's Data Protection Authority (DPA) is a paradigmatic model, with robust powers under Article 58. However, India's Digital Personal Data Protection Act 2023 promises similar machinery in the form of the Data Protection Board of India. The Board may impose penalties and order data deletion ex post, but lacks explicit ex-ante audit or rule-making authority. The central government's power to appoint, reappoint, and remove members further diluted independence. Implementation delays compound these design weaknesses, leaving oversight to CERT-In and sectoral regulators. The United States relies on a patchwork of sectoral oversight supplemented by the Federal Trade Commission's Section 5 authority to police "unfair or deceptive" data practices. The absence of a specialized privacy regulator means systemic risk assessments occur only after public controversy or data breaches. The EU's deeply institutionalized, rights-based oversight yields the most comprehensive ex-ante governance, while the U.S. offers reactive, litigation-driven control.

7.3 Penalties for data breaches and misuse

Penalties for data breaches and misuse are the coercive backbone of any privacy regime, signalling both political resolve and the true cost of non-compliance. The legal landscapes of

the European Union, India, and the United States display markedly different sanction architectures, each with direct implications for high-risk biometric programmes such as Digi Yatra.

7.31 European Union.

Article 83 of the General Data Protection Regulation (GDPR) empowers supervisory authorities to levy administrative fines of up to €20 million or 4 % of a firm's worldwide annual turnover—whichever is higher—graduated according to gravity, duration, negligence, and mitigation (Regulation EU 2016/679, art. 83). These headline figures are no mere threat: in 2021 the U.K. Information Commissioner's Office fined British Airways £20 million after a cyber-intrusion exposed 400 000 payment cards; the French CNIL penalised Clearview AI €20 million for illicit face scraping in 2022. Beyond monetary sanctions, DPAs may impose corrective orders—algorithmic suspensions, mandatory deletion, or processing bans (art. 58). Because multiple Member-State DPAs can coordinate through the "one-stop-shop" mechanism, multijurisdictional breaches incur compound reputational and operational costs. The certainty and transparency of these penalties have fostered a robust market for GDPR compliance audits and cyber-insurance, effectively internalising the externalities of data misuse (EDPB, 2022).

7.3.2 India.

Until recently, liability derived mainly from Section 43A of the Information Technology Act 2000, which limits compensation to "actual damages"—a low deterrent threshold rarely exceeding ₹5 crore (≈US $600 000) (Chander, 2022). The Digital Personal Data Protection Act 2023 (DPDP) upends this calculus by authorising the Data Protection Board (DP Board) to impose penalties up to ₹250 crore (≈US $30 million) per breach, scalable on factors parallel to the GDPR (§33). Specific ceilings are prescribed: failure to adopt reasonable security safeguards may attract ₹150 crore, while breaches involving children's data can reach the statutory maximum (§37). Crucially, the Act permits "continuing penalties" for ongoing violations. However, efficacy hinges on the DP Board's operationalisation; as of mid-2025 the Board remained unconstituted, meaning real-world enforcement still reverts to civil litigation and reputational harm (Mahapatra, 2024). For Digi Yatra operators, this lull creates a compliance-cost asymmetry: airports face immediate capital expenses for biometrics but only hypothetical future fines for lapses, potentially skewing risk calculus.

7.3.3 United States.

The absence of an omnibus privacy statute produces a patchwork of penalty regimes. The Federal Trade Commission (FTC) may secure injunctive relief and monetary disgorgement for "unfair or deceptive" practices under Section 5 of the FTC Act. Although civil penalties are technically capped at US $51 744 per violation per day (17 C.F.R. §1.98), consent decrees often impose multi-million-dollar settlements coupled with 20-year monitoring. In 2021, Everalbum paid penalties and agreed to delete facial templates improperly retained; Amazon's Ring settled for US $5.8 million plus algorithm deletion in 2023. State statutes add layers: California's CCPA/CPRA grants the Attorney General penalty authority of up to US $7 500 per intentional violation and establishes a private right of action with statutory damages (Cal. Civ. Code §1798.155). Yet, without per-se turnover-linked fines, U.S. sanctions are episodic and negotiated, lessening predictability.

7.4 Comparative Implications for Digi Yatra.

Should Digi Yatra suffer a breach—say, compromise of edge-server embeddings—EU code-share airlines operating Indian sectors could trigger GDPR "extraterritoriality" under Article 3, exposing Indian airport operators to parallel EU fines even if DPDP enforcement lags. Conversely, U.S. carriers would face FTC scrutiny primarily for misleading privacy assurances rather than for the breach per se, unless passenger data of Californians is involved, invoking CCPA. The divergent penalty scales influence corporate behaviour: European airports invest heavily in ISO/IEC 27001 and ISO/IEC 27701 certifications; Indian operators are still weighing the probability-adjusted cost of DPDP fines amid regulatory uncertainty; and U.S. entities prioritise breach notification and class-action mitigation.

In sum, the EU's turnover-indexed penalties create a high-certainty, high-severity deterrent; India's new DPDP Act aspires to similar heft but, pending institutional activation, remains a paper tiger; and the U.S. enforces through negotiated settlements that, while occasionally hefty, lack systemic predictability. The strength of any privacy regime, Digi Yatra included, is ultimately measured by how painfully it can punish non-compliance—on that metric, Europe currently leads, India is in transition, and the U.S. remains fragmented.

Right to erasure and data portability

The twin rights to erasure and data portability crystallise the idea that informational self-determination extends beyond a single moment of consent to an ongoing power to retract or relocate personal data. Their legal articulation, however, varies sharply across jurisdictions, with direct implications for biometric programmes such as Digi Yatra.

7.4.1 European Union.

Articles 17 and 20 of the General Data Protection Regulation (GDPR) entrench "the right to be forgotten" and "the right to data portability." Erasure may be invoked when data are no longer necessary, when consent is withdrawn, or when processing is unlawful (Art. 17(1)). Controllers must honour the request "without undue delay," and, where data have been made public, must take "reasonable steps" to inform downstream processors (Art. 17(2)). Portability obliges controllers to provide data "in a structured, commonly used, machine-readable format" and to transmit them directly to another controller where technically feasible (Art. 20(2)). Because biometric templates are "special-category data," supervisory authorities scrutinise refusals stringently, as illustrated by the 2022 CNIL order requiring Clearview AI to delete all French subjects' facial vectors (CNIL, 2022). Together, these rights not only enable exit from exploitative ecosystems but also foster market competition by lowering switching costs.

7.4.2 India.

The Digital Personal Data Protection Act 2023 (DPDP) omits an explicit portability guarantee and frames erasure more narrowly than the GDPR. Section 6 permits data principals to request deletion once the original purpose is fulfilled or consent withdrawn, yet two caveats erode efficacy: (1) processing mandated by law—potentially including aviation security—trumps the erasure request (§7); and (2) compliance is subject to unspecified "technical feasibility," leaving room for fiduciaries to plead incompatibility with legacy systems. Moreover, the absence of a portability right denies passengers leverage to migrate their biometric credentials to alternative identity providers, entrenching Digi Yatra as a de-facto monopoly (Mahapatra, 2024). Until the Data Protection Board is operational, enforcement relies on fiduciary goodwill and civil litigation, attenuating practical access to erasure.

7.4.3 United States.

U.S. federal law confers no general erasure or portability rights. Sectoral statutes provide partial analogues—HIPAA grants individuals a right to obtain medical records in electronic form, while the Fair Credit Reporting Act mandates deletion of stale negative credit data—yet neither applies to aviation biometrics. California's Consumer Privacy Rights Act (CPRA) offers the closest equivalent, empowering residents to request deletion and to "access data in a portable format" (Cal. Civ. Code §1798.100). Nevertheless, numerous exemptions exist for "security and fraud-prevention," a category broad enough to encompass facial-recognition systems at airports. Crucially, enforcement hinges on private litigation or actions by the state's Privacy Protection Agency; no federal oversight body harmonises portability standards (Solove & Hartzog, 2020).

7.4.4 Comparative Assessment.

The GDPR operationalises erasure and portability as enforceable, default entitlements—backed by potent supervisory authorities and interoperability norms—thereby redistributing power to data subjects. India gestures toward erasure but tempers it with statutory carve-outs and offers no portability, risking lock-in and function creep. The U.S. provides only patchwork rights, largely inapplicable to biometric aviation contexts. For Digi Yatra users, this means that withdrawing from the system or porting credentials remains straightforward in Europe, conditional and bureaucratic in India, and virtually unavailable under U.S. federal law, underscoring how jurisdictional design choices shape the effective autonomy of the digital traveller.

8. Challenges and Concerns

Despite Digi Yatra's aspiration to embody "privacy by design," its operational rollout exposes four systemic fault-lines that threaten to erode passenger trust and constitutional safeguards. First, the scheme blurs the boundary between "data controller" and "processor": Digi Yatra Foundation sets standards, private airport operators ingest biometrics, airlines consume clearance flags, and security agencies overlay watch-lists, creating a diffusion of accountability that contravenes the single-point responsibility principle in global privacy norms (Chatterjee & Sengupta, 2022). Second, the integration of facial recognition with Aadhaar rails heightens the danger of function creep, enabling repurposing for law-enforcement or targeted advertising once statutory exemptions are invoked (Mahapatra, 2024). Third, public-awareness surveys show fewer than 30 % of Indian travellers understand that participation is voluntary, signalling a consent deficit (DYF, 2023). Finally, code audits reveal plaintext storage of session tokens and inadequate certificate pinning, leaving edge servers vulnerable to interception and template theft (SFLC, 2023). Collectively, these challenges foreshadow a drift toward pervasive surveillance unless rectified through clearer governance and stronger technical safeguards.

8.1 Ambiguity around data controller vs processor roles

Ambiguity over who is a "data controller" and who is a "processor" in Digi Yatra stems from its hybrid public-private governance and from India's still-evolving statutory vocabulary. Under the Digital Personal Data Protection Act 2023 (DPDP), a "data fiduciary" decides "purpose and means" of processing, whereas a "data processor" acts solely on the fiduciary's instructions (§2). Europe's GDPR uses analogous terminology ("controller" and "processor,"

Art. 4). Yet Digi Yatra divides these functions among at least four actors, none of which fits neatly into either box.

8.1.1 Digi Yatra Foundation (DYF).

DYF specifies the technical architecture, selects the facial-recognition algorithm, issues public-key certificates, and prescribes deletion schedules (DYF, 2023). These are quintessential "means" decisions, indicating fiduciary status. Yet DYF holds neither the biometric templates (stored on devices and airport edge servers) nor the passenger manifest (provided by airlines), complicating the argument that it alone controls the "purpose." DPDP's explanatory notes do not clarify whether a standards-setting body without direct data access can nonetheless be a fiduciary, leaving DYF in a grey zone (Mahapatra, 2024).

8.1.2 Airport Operators.

Private concessionaires such as GMR and Adani ingest the encrypted travel token, decrypt it on their edge nodes, and execute one-to-many facial matches. Operationally, they decide camera placement, retention logs, and analytics add-ons (e.g., dwell-time heat maps). These discretionary choices suggest fiduciary authority. However, operators argue they merely process tokens "on behalf of" DYF and MoCA, claiming processor status to minimise liability under §33 DPDP's penalty provisions (Chatterjee & Sengupta, 2022). The absence of published Data Processing Agreements (DPAs) fuels the uncertainty.

8.1.3 Airlines.

Carriers receive only a binary "cleared/not cleared" flag, ostensibly making them processors. Yet they determine whether to deny boarding to passengers who refuse Digi Yatra enrolment, thereby influencing the purpose of processing (queue facilitation versus mandatory screening). GDPR jurisprudence (e.g., Wirtschaftsakademie Schleswig-Holstein, C-210/16) shows that even limited data access can confer joint-controller status if the entity benefits from or shapes the processing objective—a logic unsettle-ling for airlines.

8.1.4 Security Agencies.

The Central Industrial Security Force overlays no-fly watch-lists onto the live match process. Because national-security exemptions under §17 DPDP can nullify consent, the agency effectively dictates a second purpose—security vetting—beyond the facilitation goal communicated to passengers. That duality engenders covert joint-controller roles, reminiscent of the "purpose creep" that European courts have condemned in Schufa (C-634/21).

8.2 Legal and Practical Consequences.

Controller ambiguity fragments accountability: breach notifications under §8 DPDP or Art. 33 GDPR must be filed by the controller, yet each actor can plausibly deny primacy, delaying disclosure. Data Subject Requests—for erasure or access—may bounce between DYF, airports, and airlines, frustrating rights and contravening the "single point of contact" principle endorsed by the European Data Protection Board (EDPB, 2022). Liability dilution also weakens deterrence; penalties up to ₹250 crore under DPDP or 4 % of global turnover under GDPR become harder to apply when fault is diffuse (Rao, 2023).

8.3 Pathways to Clarity.

First, MoCA should issue binding rules under the Aircraft Act 1934 that assign fiduciary status to both DYF (for architectural decisions) and individual airport operators (for on-site processing), mirroring GDPR's joint-controller regime (Art. 26). Second, mandatory, public DPAs should delineate processors' obligations, audit rights, and breach-notification chains. Third, the forthcoming Data Protection Board should publish guidance—akin to the UK ICO's facial-recognition code—clarifying controller tests for biometric ecosystems. Absent such measures, Digi Yatra risks perpetuating a "Many Hands" problem in data governance, where everyone touches the data but no one bears full legal responsibility.

9. Risks of function creep and surveillance state

Biometric programs in airports are often presented as a matter of cost-benefit analysis: Facial-recognition e-gates have cut passenger processing times by 30-60% and have boosted terminal capacity without comparable staff increases. Singapore Changi Airport has rolled out a multimodal "single-token" solution that is saving passengers an average 15 minutes per journey, between kerb and gate, with a false-match rate of less than 0.1 percent. An automated check of identities has caught close to 1,800 impostors since implementing the feature in 2018 to weed out terrors that might have slipped through manual checks. Airlines also gain from biometric boarding with cost saving to the industry of US $2.2 billion per annum for IATA carriers. Yet those gains come at the price of privacy and civil-liberties concerns. Facial images are classified as "special-category" data under the EU General Data Protection Regulation (GDPR) and breaches can pose lifelong risks. Centralised galleries run the risk of function creep and algorithmic bias while providing a discriminatory result. Consent mechanisms were also sketchy, with biometric lanes that have "optional" signs being subverted through queuing differentials. Long retention periods sometimes conflict with data-

minimisation and purpose-limitation norms. Security experts warn that over-reliance on automation can create "automation bias," potentially lowering overall vigilance. Large-scale biometric roll-outs expand surveillance beyond identity verification.

9.1 Lack of awareness among passengers

Although Digi Yatra is marketed as an “opt-in, privacy-preserving” alternative to conventional boarding, empirical evidence suggests that most travellers do not comprehend either its voluntariness or its data-governance implications. In a nationwide survey administered by Digi Yatra Foundation, only 29% of participants were aware that manual check-in lanes are still in operation and only 18% were aware that facial embedded images are stored in the server of airport for certain period of time (Digi Yatra Foundation, 2023). Chatterjee and Sengupta (2022) in qualitative interviews found that as passengers commonly associate biometric lanes with required security compliance, a conceptualisation reinforced by speed-focused signage that fails to mention alternative purposes. Behavioural-economics scholarship has demonstrated that such ‘choice structures’ can create pseudo-consent by nudging people into taking the path of least resistance (Richards & Hartzog, 2021). The concomitant information asymmetry undermines the DPDP Act semi’s reliance on “informed” and “specific” consent (§6) and complicates the proportionality assessment required by Justice K.S. Puttaswamy v. Union of India, which presumes that individuals can effectively weigh the trade-offs when trading off privacy (Mahapatra, 2024). Without targeted public-education campaigns, multilingual just-in-time notices, and clear opt-out signage at every checkpoint, Digi Yatra risks institutionalising a regime of de facto biometric compulsion under the guise of voluntary participation.

9.2 Security vulnerabilities in tech infrastructure

The integrity of Digi Yatra’s “edge-centric” architecture is premised on two assumptions: that the passenger’s mobile device securely stores the primary biometric template and that airport-side edge servers are sufficiently hardened to resist compromise for the 24-hour retention window. However, independent audits find many problems at every level. The Software Freedom Law Centre (2023) did a forensic review of the Android app and found that session tokens and the encrypted facial embedding were stored in the app's shared-preferences directory. This directory is automatically backed up by Google Drive unless users turn off cloud sync. This design flaw not only goes against the program's claim of local-only storage, but it

also makes it possible to send things across borders without being checked by either Digi Yatra Foundation or Indian export controls. On the network side, GMR Airports hired people to do penetration tests that found misconfigured TLS implementations that didn't use certificate pinning. This made the system vulnerable to man-in-the-middle attacks on airport Wi-Fi, which IBM's X-Force Threat Index (2024) already rated as "high risk."

Edge servers add more ways for attackers to get in. Digi Yatra uses a demilitarised subnet, but the RTSP protocol is still used to send live camera streams. This protocol still supports legacy digest authentication, which is open to relay attacks (CERT-In, 2022). If an enemy gets this stream, they can use facial images to make fake embeddings that pass liveness checks later on. These technical gaps get worse because of supply-chain risks. For example, the NEC Neo Face Library is sent out as a binary blob with hidden update channels, making it hard to quickly patch when new CVEs are found (NIST, 2023). The Digital Personal Data Protection Act 2023 doesn't require companies to report vulnerabilities, and breaches are only reported after "significant harm" (§8). Because of this, airports may put off patches to avoid problems at work, which means that exposure windows are longer. These vulnerabilities undermine key statutory obligations to implement “reasonable security safeguards” (DPDP Act, §8) and erode proportionality under the Puttaswamy doctrine, which assumes robust data-security baselines before privacy trade-offs can be justified. A credible remediation strategy must therefore include end-to-end encryption with mutual certificate pinning, mandatory mobile-app security reviews under CERT-In’s vulnerability guidelines, signed-update mechanisms for biometric libraries, and independent red-team exercises whose results are published for public scrutiny. Without such measures, Digi Yatra’s promise of seamless, privacy-preserving travel rests on brittle technical foundations prone to exploitation.

10. Recommendations

The analysis of Digi Yatra's legal and technical architecture reveals significant gaps between aspirational privacy-by-design principles and operational reality. To align the system with constitutional proportionality standards and international best practices, six interconnected reforms are essential.

10.1 Strengthening Consent Architecture in Digi Yatra

Digi Yatra's current consent model suffers from three defects: bundling of multiple purposes, convenience coercion, and inadequate awareness. The Digital Personal Data Protection Act's

requirement for "freely given, specific, informed" consent (§6) demands granular unbundling. Airport operators should implement just-in-time consent interfaces that separately seek permission for (a) identity verification, (b) queue analytics, and (c) commercial profiling, with clear opt-out mechanisms for each purpose (Richards & Hartzog, 2021). To address convenience coercion, manual check-in lanes must offer functionally equivalent throughput, not merely token availability. This requires staffing parity and prominent signage in local languages emphasising voluntary participation. Building on GDPR Article 7's withdrawal standard, passengers should be able to revoke consent mid-journey via the mobile app, triggering immediate deletion of cached templates. Finally, consent forms must meet plain-language accessibility standards—targeting a Flesch-Kincaid grade-8 reading level—with mandatory comprehension checks before enrolment completion (Chatterjee & Sengupta, 2022).

10.2 Role of Ministry of Civil Aviation in Issuing Sector-Specific Privacy Rules

India's fragmented regulatory landscape necessitates sectoral leadership from the Ministry of Civil Aviation (MoCA). Drawing authority from the Aircraft Act 1934 and the DPDP Act's rule-making provisions (§39), MoCA should issue comprehensive "Biometric Aviation Privacy Rules" addressing four lacunae. First, clear controller-processor demarcation: Digi Yatra Foundation should be designated as joint controller for architectural decisions, while individual airport operators assume controller status for on-site processing, mirroring GDPR Article 26's joint-controller framework. Second, mandatory Data Processing Agreements with standardised breach-notification chains, audit rights, and liability caps. Third, statutory prohibition on secondary use without fresh consent, closing the function-creep loopholes created by DPDP's national-security exemptions (§17). Fourth, interoperability mandates requiring biometric credentials to be portable across airports and vendors, preventing lock-in effects that entrench monopolistic data practices (Mahapatra, 2024).

10.3 Operationalisation of the DPDP Board

The Data Protection Board's continued non-existence, nearly a year after the Act's passage, undermines the entire regulatory edifice. Immediate priorities include appointing a chairperson and members with demonstrated expertise in biometrics and constitutional law, ensuring budgetary independence through parliamentary allocation rather than executive discretion, and establishing regional offices in Mumbai, Bangalore, and Chennai to oversee high-traffic airports. The Board's mandate should be expanded beyond adjudication to include proactive

audit authority, modelled on EU Data Protection Authorities' investigative powers under GDPR Article 58. Specific to Digi Yatra, the Board should conduct annual compliance assessments of deletion logs, consent processes, and security controls, with public reporting requirements. To prevent capture, Board members should be subject to cooling-off periods prohibiting post-tenure employment with biometric vendors or airport operators (Rao, 2023).

10.4 Public Audits and Third-Party Assessments of Digi Yatra

Self-attestation of security and privacy controls breeds complacency and erodes public trust. MoCA should mandate annual third-party audits by CERT-In-empanelled agencies, covering both technical security (penetration testing, code review, infrastructure hardening) and privacy compliance (consent mechanisms, data flows, retention schedules). Audit reports should be published in redacted form, balancing security considerations with transparency imperatives. Additionally, algorithmic audits should evaluate facial-recognition accuracy across demographic groups, detecting and correcting bias that could result in discriminatory false-match rates. The European Union Agency for Cybersecurity's biometric evaluation framework provides a methodological template adaptable to Indian conditions (ENISA, 2022). Costs should be borne by airport operators as a licence condition, creating financial incentives for robust initial design rather than post-deployment remediation.

10.5 Transparent Privacy Policy and User Access Controls

Digi Yatra's current privacy disclosures are buried in lengthy terms-of-service documents that fail the DPDP Act's transparency obligations (§5). A redesigned approach should feature layered notices: a one-page summary at enrolment highlighting key risks and rights, supplemented by detailed technical documentation for interested users. Real-time dashboards should allow passengers to view their processing history, including timestamps of facial matches, airport locations, and any third-party access. Building on California's CPRA model, users should be able to request deletion of specific processing events while retaining others, enhancing granular control. QR-code mechanisms should enable instant access to privacy settings without requiring app downloads, reducing barriers for occasional travellers (Solove & Hartzog, 2020).

10.6 Mandatory Privacy Impact Assessments (PIAs) for Biometric Systems

High-risk processing under DPDP requires formal risk assessment once "significant data fiduciary" criteria are notified. MoCA should anticipate this by mandating PIAs for all airport biometric deployments exceeding 50,000 annual passengers. PIAs should evaluate necessity, proportionality, and alternatives—following the Justice K.S. Puttaswamy framework—with public consultation periods for civil-society input. Key assessment criteria should include demographic bias testing, breach-impact modelling, and function-creep scenarios. The UK Information Commissioner's Office provides a methodological precedent through its biometric processing code, emphasising stakeholder engagement and mitigation planning (ICO, 2022). PIAs should be updated whenever technical architecture changes or new use-cases are proposed, ensuring ongoing proportionality review.

These recommendations collectively address the accountability vacuum, consent deficits, and technical vulnerabilities that currently undermine Digi Yatra's privacy claims. Implementation will require sustained political commitment, adequate budgetary allocation for the DPDP Board, and industry acceptance of higher compliance costs. Yet the alternative—a gradual drift toward pervasive biometric surveillance—poses far graver threats to constitutional democracy and individual autonomy. India has the opportunity to demonstrate that technological convenience and robust privacy protection are compatible; realising that vision demands urgent, comprehensive reform of the existing governance framework.

11. Conclusion

India's Digi Yatra initiative highlights the tension between technological convenience and constitutional privacy rights in democratic societies. Despite India's sophisticated legal architecture, significant implementation gaps compromise the system's privacy integrity. The Digital Personal Data Protection Act 2023, the Aadhaar framework, and the constitutional proportionality doctrine established in Justice K.S. Puttaswamy v. Union of India are compared to European Union and United States frameworks. The continued non-operationalisation of India's Data Protection Board represents a critical institutional vacuum.

Technical analysis reveals that Digi Yatra's "privacy-by-design" claims rest on fragile foundations, with controller-processor ambiguities, security vulnerabilities, and bundling, coercion, and awareness deficits. These deficiencies violate the DPDP Act's fiduciary obligations and the proportionality standard mandated by constitutional jurisprudence.

To address these issues, India must operationalize the Data Protection Board with adequate resources and independence, mandate sector-specific privacy rules for aviation biometrics, and institute mandatory privacy impact assessments for high-risk processing. The Ministry of Civil Aviation should lead this harmonisation effort, drawing on international best practices while respecting India's federal structure and constitutional values.

.

12. References

- Airports Authority of India. (2023). Digi Yatra operational metrics report Q1 FY 2023–24. AAI Publications.
- Asia-Pacific Economic Cooperation. (2015). APEC privacy framework (2nd ed.). APEC Secretariat.
- Bach, D., & Newman, A. (2014). Self-regulatory trajectories in the shadow of public power: Resolving digital dilemmas in Europe and the United States. *Governance*, 27(4), 635–652.
- Bani, A. (2021). Biometric innovations and privacy in Singapore's Changi Airport. International Aviation Law Review, 34(2), 88–109.
- CERT-In. (2022). *Directions under Section 70-B of the Information Technology Act, 2000*. Ministry of Electronics and IT.
- CERT-In. (2022). *Directions under sub-section (6) of section 70-B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. Ministry of Electronics and IT.
- Chander, A. (2022). India's new data-protection bill: Progress or regress? *Computer Law Review International*, 23(1), 1–9.
- Changi Airport Group. (2021). Seamless and contactless travel at Changi: Technology factsheet.
- Chatterjee, R., & Sengupta, S. (2022). Navigating privacy challenges: Biometric authentication at Indian airports. Journal of Law & Technology, 45, 112–150.
- Commission Nationale de l'Informatique et des Libertés. (2022). *Deliberation No. SAN-2022-019 concerning Clearview AI*. CNIL.
- Customs and Border Protection. (2023). Biometric Entry-Exit Program: FY 2023 report to Congress. U.S. Department of Homeland Security.

- De Hert, P., & Szekely, I. (2019). The right to privacy and the right to personal data protection: Interactions and tensions. *Fordham International Law Journal, 47*(2), 1–35.
- de Montjoye, Y.-A., Gambs, S., Blondel, V., Canright, G., de Cordes, N., Deletaille, S., … Smoreda, Z. (2018). On the privacy-conscientious use of mobile phone data. Scientific Data, 5, 180286.
- Digi Yatra Foundation. (2023). *Passenger awareness survey report Q2–2023*. https://www.digiyatra.gov.in
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- Electronic Frontier Foundation. (2022). TSA's facial recognition expansion: Civil liberties implications. https://eff.org
- European Data Protection Board. (2022). *Annual report 2021*. EDPB.
- European Data Protection Board. (2022). *Guidelines 07/2022 on controller–processor distinctions*. EDPB.
- European Data Protection Supervisor. (2019). Facial recognition in EU aviation security: 2019 report. https://edps.europa.eu
- European Parliament & Council. (2016). Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.
- European Union Agency for Cybersecurity. (2022). *Biometric recognition and privacy enhancement*. ENISA.
- Fraport. (2022). Biometrics@Gate: Pilot results and expansion plans. Fraport AG.
- Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology.
- GMR Airports. (2022). *Biometric boarding impact assessment report*. GMR Group.
- IBM Security. (2024). X-Force threat intelligence index 2024. IBM Corporation.
- Information Commissioner's Office. (2022). *Guidance on biometric recognition technology*. ICO.
- Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
- International Air Transport Association. (2023). Biometric identification in air travel: Global report 2023. IATA Publications.

- International Civil Aviation Organization. (2022). Annex 9—Facilitation (15th ed.). ICAO.
- International Organization for Standardization. (2018). ISO/IEC 19795-1:2018—Biometric performance testing and reporting. ISO.
- Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
- Lyon, D. (2020). *Surveillance society: Monitoring everyday life* (2nd ed.). Polity Press.
- Mahapatra, S. (2024). Analysing India's Digital Personal Data Protection Act, 2023: Scope and challenges. *Indian Journal of Law & Policy, 15*, 210–238.
- Ministry of Civil Aviation. (2018). *Policy document on Digi Yatra*. Government of India.
- Ministry of Civil Aviation. (2022). Press release: Launch of Digi Yatra for contactless passenger processing. Government of India.
- Ministry of Civil Aviation. (2024). Directive No. AV-15011/2/2024-DG: Conditions for Digi Yatra expansion. Government of India.
- NEC Corporation. (2021). NeoFace accuracy evaluation report v5.2. NEC Biometrics Division.
- NIST. (2023). CVE-2023-45107: Vulnerability in NEC NeoFace SDK. National Vulnerability Database. https://nvd.nist.gov
- Personal Data Protection Commission. (2022). Advisory guidelines on biometric data under the Personal Data Protection Act. PDPC Singapore.
- Press Information Bureau. (2023). Digi Yatra now operational at 13 airports; roadmap for 20 more. Government of India.
- Rao, N. (2023). Distributed accountability under India’s DPDP Act: Lessons from GDPR enforcement. *Data Policy*, 5, e28
- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
- Richards, N., & Hartzog, W. (2021). The pathologies of digital consent. Washington University Law Review, 98(4), 1007-1050.
- Software Freedom Law Centre. (2023). Security audit of Digi Yatra Android application (v 1.4). SFLC-IN.
- Solove, D. J., & Hartzog, W. (2020). *Breached! Why data security law fails and how to improve it*. Oxford University Press.

- Transportation Security Administration. (2023). CAT-2 deployment update: Enhancing identity verification. U.S. Department of Homeland Security.
- U.S. Customs and Border Protection. (2023). Biometric entry–exit program: Fiscal year 2023 report to Congress. Department of Homeland Security.
- UIDAI. (2021). Aadhaar QR code specification version 2.0. Unique Identification Authority of India.
- United States Federal Trade Commission. (2023). *Ring LLC—Complaint and decision & order*. FTC.
- Voigt, P., & Von dem Bussche, A. (2021). The EU General Data Protection Regulation (GDPR): A practical guide (2nd ed.). Springer.