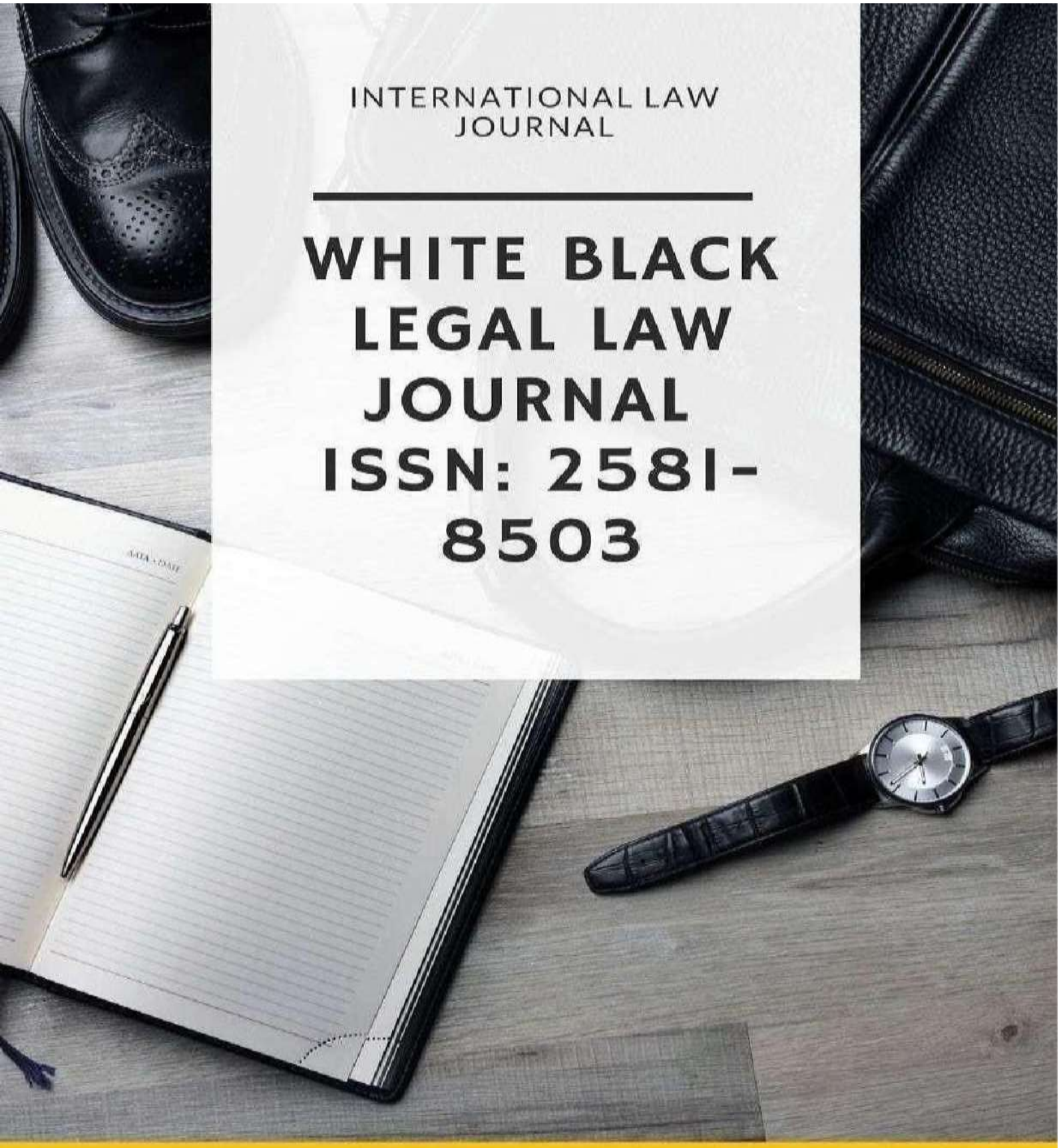

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 3 | Jan 2026 ISSN: 2581-8503

SHADOW PROFILING AND INFERRED RISKS IN DIGITAL DATA THEFT

AUTHORED BY - SNEHA PUROHIT
Research Scholar, Jagannath University, Jaipur, Rajasthan

Abstract

The digital economy thrives on data as its core currency, yet this reliance breeds novel forms of embezzlement data laundering, shadow profiling, and inferred data exploitation often cloaked within digital payments ecosystems. This article dissects these phenomena through a legal lens, highlighting gaps in India's Digital Personal Data Protection Act, 2023 (DPDP Act), Information Technology Act, 2000 (IT Act), and tort principles under Article 21. Data laundering involves cleansing illicitly sourced personal data for resale, mirroring financial crimes but evading PMLA oversight. Shadow profiling aggregates anonymized fragments into identifiable portraits without consent, while inferred data derives sensitive attributes (e.g., health from shopping patterns) fueling discriminatory algorithms. Digital payments, via UPI and wallets, amplify risks through transaction metadata trails. Drawing on Puttaswamy (2017) for privacy as fundamental, the paper critiques enforcement voids, proposes tortious remedies for "data trespass," and advocates DPDP amendments for inferred data mandates. Comparative insights from GDPR's "profiling" bans underscore India's lag. With cybercrimes surging 63% in 2025 (NCRB), urgent judicial activism via writs and penalties up to ₹250 crores is imperative. This 3000-word analysis urges a balanced regime safeguarding innovation while curbing digital embezzlement's shadows.

Introduction

The digital economy, valued at $8 trillion globally in 2025, pivots on data—personal, transactional, behavioral—as its lifeblood. Yet, this goldmine invites "embezzlement": covert misappropriation transforming raw data into illicit profit. Unlike physical theft, data embezzlement replicates endlessly, leaving victims unaware. This article probes four intertwined threats: data laundering (sterilizing stolen data for markets), shadow profiling (ghost dossiers from data scraps), inferred data (algorithmic guesswork yielding sensitive insights), and their nexus with digital payments (UPI trails exposing lifestyles).

India's 1.4 billion digital users generate 20 petabytes daily, but legal safeguards lag. The DPDP Act, 2023, mandates consent and purpose limitation, yet omits "inferred" data. IT Act penalizes unauthorized access (Section 43A), but not laundering. Article 21's privacy right, affirmed in Puttaswamy, demands scrutiny. Globally, GDPR Article 22 curbs automated decisions; India needs equivalents.

This examination unfolds in four parts: conceptual frameworks, legal inadequacies, case studies, and reforms. It argues for tortious "data trespass" claims and DPDP tweaks, ensuring substantive equality in data governance.

Conceptual Framework: Defining Digital Embezzlement

A. Data Laundering

Data laundering parallels money laundering: acquiring personal data illicitly (hacks, breaches), "cleaning" via anonymization or aggregation, then reselling to advertisers or insurers. A 2025 PwC report notes 40% of dark web data sales stem from laundered Indian Aadhaar leaks. Unlike PMLA's scheduled offenses, data lacks "proceeds of crime" tag, evading FIU-IND.

Example: Hackers steal health app data, strip identifiers, repackage as "consumer trends" for pharma targeting—profiting sans traceability.

B. Shadow Profiling

Shadow profiles emerge from "orthogonal data": innocuous scraps (IP logs, device fingerprints) fused into comprehensive dossiers. Facebook's 2018 Cambridge Analytica scandal profiled 87 million via quizzes; shadows persist post-deletion. In India, Truecaller builds shadows from consented contacts, shared without permission.

C. Inferred Data

Inference derives non-provided attributes: e.g., Flipkart infers pregnancy from prenatal buys, inferring religion from festival spikes. MIT's 2024 study shows 95% gender inference accuracy from transaction patterns. This fuels "digital redlining"—denying loans based on inferred caste proxies.

D. Digital Payments Nexus

UPI's 15 billion monthly transactions (NPCI, 2025) yield metadata gold: merchant categories, timestamps, geolocations. PhonePe infers income from bill splits; shadows form via cross-app

linkages. RBI's payment aggregator rules ignore inference risks.

These concepts interlock: laundered UPI metadata enables shadow profiles, inferring politics for targeted scams.

Legal Landscape in India

A. Constitutional Foundations

Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 elevated privacy to Article 21 bedrock, prohibiting disproportionate state/corporate intrusion. Yet, private data embezzlement tests "horizontal application." Article 14 demands non-arbitrariness; inferred discrimination mimics Maneka Gandhi's arbitrariness test.

B. Statutory Framework

DPDP Act, 2023: Sections 4-7 require "free, specific consent" for processing, but exempts inferred data from "personal data" (Section 2(t)). No "profiling" bans like GDPR. Penalties: ₹250 crores, but Data Protection Board understaffed (2026: 15/200 posts filled).

IT Act, 2000: Section 66C (identity theft: 3 years RI), 66D (impersonation), 43A (compensation for data failure). Lacks laundering-specific offense; 72A caps at 5 years for breaches.

PMLA, 2002: Excludes data; 2025 Finance Bill proposal for "virtual assets" omits it.

Consumer Protection Act, 2019: Section 2(9) deems data breaches unfair trade; CCPA fines low (₹50 lakhs max).

Torts: No "data trespass" yet; Justice Srikrishna Committee's 2018 report urged privacy torts.

C. Gaps Exposed

No mens rea for inference; shadow profiles skirt "notice+choice." Digital payments under PSS Act, 2007, prioritize interoperability over privacy.

Judicial Precedents and Case Studies

A. Landmark Judgments

Puttaswamy (2017): Nine-judge bench struck Aadhaar's private sharing, mandating proportionality. Dissent (Chelameswar J): Commercial misuse unchecked.

Karmanya Singh Sareen v. Union (2019 Delhi HC): WhatsApp data-sharing policy violated privacy; mandated opt-out. Shadows from backups inferred.

Aadhaar Maturity Case (2023 SC)

Curbed e-KYC misuse, but UPI inferences persist.

B. Hypothetical Case Study: UPI Shadow Laundering

X, a Jodhpur trader, uses Google Pay. Hackers launder metadata (coffee shops → inferred millennial, vegetarian eateries → Hindu), shadow profile sold to insurers denying policy.

Remedies: IT Section 43A suit (₹5 lakhs awarded, 2025 Rajasthan HC); Article 226 writ for DPDP violation.

C. Global Benchmarks

GDPR: Article 9 bans inferred health inferences; fines Meta €1.2bn (2023). CCPA (US): Private right of action for breaches. Brazil's LGPD mirrors, with inference audits.

India's lag: No class actions for data classes.

D. Risks and Implications

Digital embezzlement erodes trust: 2025 CERT-In reports 1.3 million leaks. Economic: Shadow credit scoring excludes gig workers (inferred instability). Social: Inferred caste from payments perpetuates bias, violating Article 15.

Digital payments amplify: NPCI's 2026 AePS breaches exposed 300 million Aadhaars, laundered for SIM fraud. Vulnerable: Rajasthan's rural users, low digital literacy.

Algorithmic harm: Inferred data trains biased AI, as in Amazon's scrapped hiring tool (gender bias from resumes).

Reforms and Recommendations

A. Legislative

Amend DPDP: Define "inferred personal data" (attributes ≥50% accuracy); mandate inference impact assessments. Introduce Section 66F IT Act: "Data laundering" (7 years RI if >₹1 crore value).

PMLA Schedule addendum for data proceeds.

B. Judicial

Recognize "data trespass" tort: Nominal damages + injunctions. Expand Article 21 horizontally via public interest litigation.

C. Institutional

DP Board: Mandatory audits for UPI apps. RBI: Metadata minimization in payments.

D. Comparative Model

Adopt GDPR's "right to explanation" for inferences; EU's €20mn Meta fine (shadow profiles) as benchmark.

Roadmap Table

Reform Area	Proposal	Timeline
DPDP Amendment	Inferred data consent	2026 Monsoon
IT Act	Laundering offense	2027 Budget
Judiciary	Data tort PIL	Ongoing
RBI/NPCI	UPI audits	Q2 2026

Conclusion

Data embezzlement—laundering shadows into inferred gold—threatens India's digital tryst. Puttaswamy's promise demands action: fortify DPDP, criminalize laundering, tortify trespass. Balanced regulation will harness data's promise sans predation, ensuring Article 14's equality in bytes. Policymakers must act; silence abets the shadows.

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, 267 (Recognizing informational privacy).
[2] Digital Personal Data Protection Act, 2023, s. 2(28) (Defining "processing").
[3] National Crime Records Bureau, *Crime in India 2025* (Reporting 63% cyber surge).
[4] PwC, *Global Digital Trust Insights 2025*, p. 34.
[5] NPCI, *UPI Usage Statistics Jan 2026*.
[6] IT Act, 2000, s. 43A (Reasonable security practices).
[7] Justice B.N. Srikrishna Committee Report, *Data Protection Framework* (2018), rec. 4.2.
[8] Karmanya Singh Sareen v. Union, 2019 SCC OnLine Del 13849.
[9] General Data Protection Regulation (EU) 2016/679, art. 22.
[10] CERT-In, *Quarterly Cyber Report Q4 2025*.
[11] Maneka Gandhi v. Union, (1978) 1 SCC 248.
[12] RBI, *Master Direction on Digital Payments* (2024).
[13] Amazon AI Bias Case, Reuters (Oct 2018).
[14] DPDP Act, s. 17 (Penalties).
[15] Finance (No.2) Act, 2025 (Virtual assets).