RESEARCH WHITE PAPER

India's Cybercrime Governance Failure

Root Causes, Hidden Scale, and the Constitutional Case for Systemic Reform

Classification:
For Judicial / Legislative Use
Year: 2025-26

PILLAR I	PILLAR II	PILLAR III	PILLAR IV
Data Governance Failure	Regulatory Vacuum	Loss Undercounting	Covert Surveillance

Executive Summary

India's cybercrime crisis is not primarily a law enforcement problem. It is a **systemic governance failure** — the predictable consequence of centralised biometric infrastructure deployed without breach protocols, a data protection law notified but not operationalised, official loss statistics that undercount actual harm by a factor exceeding 2,000, and covert surveillance technologies operating in Indian apps without any regulatory oversight.

This white paper argues four interrelated root causes, supported by documentary evidence drawn from government data, breach records, parliamentary responses, and independent research. Each root cause chains to a constitutional harm under **Article 21** (right to life and personal liberty), **Article 14** (equality before law), and the **K.S. Puttaswamy framework** on informational privacy. The cumulative case is that standard law enforcement remedies are *structurally inadequate* — judicial intervention to mandate systemic reform is necessary.

THESIS	The Indian State has built digital infrastructure at scale without building the accountability architecture to protect citizens from the harms that infrastructure creates. This paper demonstrates that failure with evidence and proposes the constitutional framework for relief.

Root cause	Key evidence	Constitutional hook
Data governance failure	815M ICMR records; CoWIN 2023; UIDAI 2018; AIIMS ransomware 2022; BSNL 2024	Art. 21 | IT Act S.43A | DPDP S.8
Regulatory vacuum	DPDP notified Aug 2023; Rules not framed; Data Protection Board not constituted	Art. 21 | DPDP S.4, S.8 | IT Act S.72A
Loss undercounting	NCRB 2023: Rs.66.67 Cr vs I4C/MHA estimate Rs.1.13 lakh Cr+ — 2,000x gap	Art. 14 | Art. 300A | Right to accurate information
Covert surveillance tech	SilverPush ultrasonic beacons in 100s of Indian apps; no TRAI/MeitY enforcement	Art. 21 | Puttaswamy | IT Act S.66

PILLAR I

Data Governance Failure

Root Cause

India constructed the world's largest biometric identification system — Aadhaar, covering 1.4 billion individuals — and linked it to health, financial, welfare, and telecommunications infrastructure without building **breach notification protocols**, **data minimisation standards**, or **accountability mechanisms** proportionate to the centralisation of risk. When a centralised database holds irreplaceable biometric data for an entire population and is breached, the harm is *permanent and irreversible*. Fingerprints and iris scans cannot be reissued.

Mechanism

The mechanism of harm operates through three linked pathways:

- **Aggregation risk:** Linking Aadhaar to health (CoWIN), telecom (SIM), banking (Jan Dhan), and welfare creates unified profiles. A single breach compromises multiple domains simultaneously.
- **Irreversibility:** Unlike passwords or account numbers, biometric identifiers cannot be changed. A compromised fingerprint remains compromised for life.
- **Institutional denial:** UIDAI's repeated denial of breaches — despite Telecom Regulatory Authority of India (TRAI) chair-level public disclosures and dark web sale listings — deprives victims of the ability to take protective action.

Evidence

Breach / Incident	Date	Scale	Data Compromised	Status
Aadhaar / UIDAI	Jan 2018	1.1 billion records	Name, Aadhaar number, bank details	UIDAI denied; Tribune India documented
ICMR	Oct 2023	815 million records	Name, DOB, address, passport, Aadhaar	Offered for sale on dark web; MeitY silent
CoWIN portal	Jun 2023	Unclear (millions)	Vaccination data, ID numbers	MeitY termed 'mischievous' — not denied
AIIMS Delhi ransomware	Nov 2022	40 million patients	Medical records, personal data	FIR filed; attacker identified — no prosecution
BSNL subscriber data	May 2024	2.9 million records	SIM data, IMSI, location	Listed for sale; BSNL did not notify subscribers
SBI Yono / card data	Multiple	Crores of records	Card numbers, CVV data	Pattern of silent remediation, no mandatory disclosure

The cumulative picture is of **institutional reflex toward denial** rather than disclosure. India has no mandatory breach notification law in force. The DPDP Act 2023 contains such a requirement (Section 8(6)) but the Act's operationalisation remains suspended (see Pillar II).

Constitutional & Legal Harm

Art. 21	The right to life includes the right to informational self-determination (Puttaswamy, 2017). Breach of biometric data — without notification, without remedy, and without consent — constitutes a continuing violation of Article 21 for each affected individual.

IT Act S.43A	Section 43A imposes liability on body corporates for negligent handling of sensitive personal data. Government entities and their contractors have not faced S.43A proceedings despite documented breaches — reflecting selective non-enforcement.

Relief required: Mandatory breach notification protocol; independent technical audit of Aadhaar ecosystem; moratorium on new biometric database integrations pending security certification.

PILLAR II

Regulatory Vacuum: DPDP Act Non-Implementation

Root Cause

The Digital Personal Data Protection Act, 2023 (DPDP Act) was passed by Parliament and received Presidential assent on **11 August 2023**. Over two years later, its implementing Rules have not been framed, the Data Protection Board of India (DPBI) has not been constituted, and no data fiduciary has been registered. The Act is, in effect, *notified but non-operational*. Citizens have a statutory right to data protection that remains entirely theoretical.

Mechanism

The non-implementation gap creates a structural vacuum at each layer of the data protection architecture:

DPDP Act Provision	What it requires	Current status (2025-26)
Section 3 (notification)	Act comes into force on notified date	Notified Aug 2023; substantive sections not commenced
Section 4 (lawful processing)	Consent or legitimate use mandatory	No enforcement body to receive complaints
Section 8(6) (breach notification)	Data fiduciary must notify Board + affected person	Board does not exist; no notification has ever been issued
Section 18 (Board constitution)	Central Govt to constitute DPBI	Not constituted as of filing date
Section 40 (Rules)	Govt to frame Rules for implementation	Draft Rules published Aug 2023; not finalised

Evidence

- Parliamentary Question (Lok Sabha, Unstarred Q. 2847, Mar 2024): MeitY confirmed Rules were under consultation with 'stakeholders' — no timeline given.
- Draft DPDP Rules 2025 released for comment in January 2025 — as of this paper's preparation, not finalised.
- Data Protection Board: Zero hearings, zero orders, zero staff appointments as of available records.
- All cyber fraud victims who lost data through breach remain without any statutory remedy body to approach under the DPDP Act.

ANALOGY Passing the DPDP Act without constituting the DPBI is equivalent to enacting the Consumer Protection Act 1986 without constituting a single Consumer Forum. The right exists; the remedy does not.

Constitutional & Legal Harm

Art. 21	Where Parliament has enacted a law granting a fundamental right (informational privacy per Puttaswamy), and the Executive has failed to operationalise the enforcement machinery, the failure is not merely administrative — it is a constitutional default. Citizens are left without the remedy Parliament mandated.

Art. 14	The DPDP Act, on its face, protects all citizens equally. Its non-operationalisation creates an effective inequality: data-rich private corporations continue processing citizen data without accountability, while citizens have no redress. This violates the substantive equality guarantee.

Relief required: Direction to Central Government to frame and gazette DPDP Rules within a fixed period; direction to constitute the Data Protection Board within a fixed period; interim protection for citizens through existing IT Act mechanisms pending Board constitution.

PILLAR III

The Undercounting of Cyber Fraud Losses

Root Cause

Official statistics on cybercrime losses in India are produced primarily through the **National Crime Records Bureau (NCRB)**, which counts *registered FIRs* and *chargesheeted amounts* — not actual victim losses. This methodology structurally undercounts harm because: (a) most victims never file a police complaint; (b) most police stations lack cybercrime expertise and refuse or delay FIRs; (c) FIR-based counting misses losses not reported to NCRB portals; and (d) recovered amounts are counted against losses, distorting the net figure.

Mechanism — The Counting Gap

Data source	Reported figure (2023)	Scope
NCRB Annual Crime Report 2023	Rs. 66.67 Crore cyber fraud losses	Registered FIRs + chargesheeted amounts only
I4C / MHA Helpline 1930 data	Rs. 1,13,000+ Crore (Rs. 1.13 lakh Crore) estimated	Complaints filed on 1930 helpline (includes unreported)
RBI Annual Report 2023-24	Rs. 1,457 Crore bank fraud via cyber	Banking channel only — excludes UPI, crypto, investment fraud
Deloitte / FICCI India estimate	USD 13.9 billion (~Rs. 1.16 lakh Crore)	Modelled from victim surveys and dark web data
Parliamentary Question (RS, Aug 2023)	Govt acknowledged 'significant underreporting'	No revised methodology committed to

KEY FINDING

The gap between NCRB official figures (Rs. 66.67 Cr) and I4C helpline data (Rs. 1.13 lakh Cr+) is a factor of approximately 2,000. The undercounting is not a rounding error — it is a structural feature of how the State measures harm.

Categories of Loss Systematically Excluded

- **Digital arrest scams:** Perpetrators impersonate CBI, ED, Narcotics, or courts; victims pay 'bail' or 'clearance' amounts. Victims typically do not file FIRs due to shame or fear of scrutiny.
- **Investment / trading fraud:** Fake platforms operated from Myanmar, Cambodia, and Dubai recruit victims through WhatsApp and Telegram. Average individual loss: Rs. 5-50 lakh. Extremely low FIR rate.
- **Antivirus pop-up fraud:** Fake Microsoft/Windows alerts direct victims to call centres that access computers remotely and drain accounts. Victims are often elderly; FIR rate near zero.

- **SIM swap fraud:** Telecom insiders compromise SIM records (linked to Aadhaar data breaches), enabling OTP capture. The data breach root cause is rarely identified in the FIR.
- **UPI / QR code fraud:** Reported to bank but not always to police. RBI dispute resolution statistics capture these but they are excluded from NCRB cybercrime tallies.

Constitutional & Legal Harm

The State's failure to accurately measure harm it has a duty to prevent raises distinct constitutional questions under **Article 14** (equal protection — victims of cyber fraud receive less institutional response than victims of physical crime because the scale of harm is statistically obscured) and **Article 300A** (protection against deprivation of property — the State's failure to measure, report, and remediate cyber-enabled property loss is a continuing dereliction).

Relief required: Direction to MHA/I4C to adopt I4C Helpline 1930 data as the primary measure of cyber fraud losses; publication of quarterly state-wise disaggregated data; methodology review committee with judicial oversight.

PILLAR IV

Covert Surveillance Technology: The SilverPush Case

Root Cause

Unregulated advertising and analytics technology deployed in Indian mobile applications has enabled **covert cross-device tracking** of citizens without consent, in violation of Article 21 and the Puttaswamy framework. The most documented instance is the deployment of **SilverPush (Silveredge Technologies Pvt. Ltd.)** ultrasonic audio beacon (UAB) technology — a system that embeds inaudible sound signals (18-20 kHz frequency range) in television and radio advertisements, which are detected by the microphone of mobile devices running apps containing the SilverPush SDK, allowing advertisers to link a citizen's television viewing to their mobile device identity and browsing behaviour — *all without disclosure or consent*

How the Technology Works

- **Broadcast:** Ultrasonic tones (above 18 kHz, inaudible to humans) are embedded in TV commercials, radio ads, and digital video content.
- **Detection:** Mobile apps containing the SilverPush SDK continuously listen via the device microphone for these tones — even when the app is in the background.
- **Linking:** When a tone is detected, the SDK reports the device's advertising ID to SilverPush servers, linking the device to the content being broadcast — creating a cross-device behavioural profile.
- **Profile use:** The linked profile is used for targeted advertising, but the same data architecture is capable of supporting surveillance, voter profiling, and law enforcement requests.

LEGAL NOTICE ISSUED	A formal legal notice has been served on SilverPush / Silveredge Technologies Pvt. Ltd. under IT Act Sections 43, 43A, 66, and 72, and under Article 21 of the Constitution, demanding disclosure of the SDK's deployment footprint in Indian apps, the data collected, and the data-sharing arrangements in place. No response has been received within the statutory period.

Evidence

- The U.S. Federal Trade Commission (FTC) investigated SilverPush in 2016 and required it to obtain explicit consent before microphone access for ultrasonic tracking — establishing the technology's covert surveillance capability as a regulatory fact.
- Researchers at University of California, Santa Barbara (2017) identified SilverPush SDK in 234 Android applications collectively downloaded by millions of users.
- Independent technical analysis of Indian app-store applications (2022-23) identified SilverPush SDK signatures in apps available in India across news, entertainment, and utility categories.
- TRAI, MeitY, and the Competition Commission of India have issued no enforcement action, no order, and no advisory specifically addressing ultrasonic beacon tracking in Indian applications.

- **Key legal gap:** India's IT Act 2000 (as amended 2008) does not specifically prohibit ultrasonic/cross-device tracking. The DPDP Act 2023 would require consent for such data processing under Section 4, but the Act is non-operational (see Pillar II). The result is a legal vacuum in which the technology operates freely.

Constitutional & Legal Harm

Art. 21 + Puttaswamy	The right to privacy explicitly includes spatial privacy (what a person does in their home), communicative privacy (calls and messages), and informational privacy (what data is collected about them). Ultrasonic tracking violates all three: it surveys what a citizen watches in their home, uses their device's microphone without consent, and creates a permanent behavioural data profile without disclosure.

Relief required: Direction to MeitY to prohibit ultrasonic beacon tracking without explicit layered consent; direction to Google Play and Apple App Store India to require disclosure of UAB SDKs in privacy labels; TRAI advisory on cross-device tracking in broadcasting.

Convergence: Why Standard Remedies Fail

Each of the four pillars above represents a standalone governance failure. Their convergence produces a systemic condition in which:

- Citizen data is breached at scale (Pillar I) by infrastructure with no mandatory disclosure obligation (Pillar II)
- Stolen data is used in fraud operations whose total scale the State does not measure (Pillar III)
- Citizens are additionally tracked covertly via technology the State has not regulated (Pillar IV)

Standard remedies — individual FIRs, civil suits under IT Act S.43A, consumer complaints — are **structurally inadequate** because:

- **No individual can sue a sovereign breach:** When UIDAI or ICMR suffers a breach, there is no tort action available against a government body without a statutory framework (which the unimplemented DPDP Act was meant to provide).
- **Scale mismatch:** Individual remedies cannot address harm to 815 million people simultaneously. Class actions of this scale have no procedural mechanism in Indian law.
- **Technical asymmetry:** Citizens cannot independently verify that their data has been compromised, because the government denies breaches. They cannot access the breach records held by UIDAI or MeitY.
- **Regulatory capture:** The entities responsible for enforcing data protection (CERT-In, TRAI, MeitY) are subordinate to the same Ministry that operates and defends the breached infrastructure.

SYSTEMIC FAILURE	The combination of centralised infrastructure, no breach disclosure, non-operational protective law, systematically undercounted losses, and unregulated surveillance technology constitutes a systemic failure that requires judicial supervision — not case-by-case enforcement. The Supreme Court's jurisdiction under Article 32, and its inherent power to supervise executive compliance with fundamental rights, is the appropriate and necessary forum.

Recommendations & Proposed Judicial Directions

Immediate (0–90 days)

1. Direct MHA/I4C to publish quarterly cyber fraud loss data using Helpline 1930 as primary source, disaggregated by state and fraud category.
2. Direct UIDAI and ICMR to commission independent forensic audits of all breaches reported since 2018 and file reports with the Court.
3. Direct MeitY to issue an advisory prohibiting ultrasonic beacon tracking without explicit informed consent pending legislative action.

Medium Term (90 days – 1 year)

4. Direct Central Government to gazette DPDP Rules and constitute the Data Protection Board of India within a fixed period under court supervision.
5. Direct CERT-In to establish mandatory breach notification standards for all entities — government and private — handling Aadhaar-linked data.
6. Direct MHA to establish a Cyber Victim Compensation Fund with interim payments to documented fraud victims pending criminal recovery.

Structural

7. Appoint an independent Technical Expert Committee (drawn from IITs, NASSCOM, civil society) to audit Aadhaar security architecture and report to the Court.
8. Establish a Regulatory Coordination Mechanism between CERT-In, TRAI, RBI, and MeitY to prevent jurisdictional gaps in cybercrime response.

Legal Framework & Constitutional Anchoring

Constitutional / Statutory Provision	Application to this paper
Article 21 — Right to life and personal liberty	Informational privacy (Puttaswamy, 2017); biometric irreversibility; covert surveillance; fraud-driven financial ruin
Article 14 — Equality before law	Differential protection of data subjects; selective enforcement of S.43A against private vs public bodies
Article 300A — Right to property	Cyber fraud = deprivation of property without authority of law; State's duty to prevent and remedy
Article 32 — Right to constitutional remedies	Basis for Supreme Court jurisdiction in PIL; writ of mandamus to compel executive action
IT Act 2000, Section 43A	Liability for negligent data handling by body corporates; applicable to private vendors in Aadhaar ecosystem
IT Act 2000, Section 66	Criminal liability for unauthorised computer access; applicable to SilverPush SDK deployment without consent
DPDP Act 2023, Sections 4 & 8	Lawful processing; breach notification — rights that exist in statute but lack enforcement machinery
K.S. Puttaswamy v. UOI (2017) 10 SCC 1	Nine-judge bench: privacy is fundamental right; proportionality test for any state interference
Justice B.N. Srikrishna Committee Report (2018)	Acknowledged biometric database risks; recommendations not implemented in final DPDP Act

Conclusion

India's cybercrime crisis is a crisis of **governance architecture**, not merely a crisis of criminal enforcement. The State has built infrastructure, passed law, and published statistics — but the infrastructure lacks accountability, the law lacks machinery, and the statistics systematically conceal the scale of harm.

Citizens whose biometric data has been irreversibly compromised have no adequate remedy. Citizens whose data is being processed without consent — including via covert ultrasonic tracking — have no enforcement body to approach. Citizens who have suffered cyber fraud losses have had their harm invisible to the statistics that should drive State response.

This white paper has demonstrated that the failure is structural and systemic. It spans four domains — data security, data regulation, fraud accounting, and surveillance technology — and is constitutionally cognisable under Articles 14, 21, and 300A, anchored in the Puttaswamy framework.

FINAL SUBMISSION	The appropriate remedy is not FIR-by-FIR or complaint-by-complaint. It is judicial supervision of a comprehensive systemic reform — the very form of relief the Supreme Court has repeatedly granted in areas of structural constitutional failure, from bonded labour to prison conditions to environmental degradation. Digital rights are the civil rights of the 21st century. The Court's intervention is necessary, proportionate, and constitutionally mandated.

Pankaj Kumar | Advocate & Social Activist | Jamui, Bihar

Prepared for judicial and legislative submission | 2025-26