Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

THE CONSTITUTIONAL AND STATUTORY DIALECTIC: NAVIGATING THE INTERSECTION OF PERSONAL PRIVACY AND NATIONAL CYBERSECURITY IN INDIA

[1]Dr. Deepmala Shrivastava and [2]Sanjay Pandey
[1]Associate Professor,Department of Law, TRC Law College, Barabanki
[2]LLM (Final Semester),TRC Law College, Barabanki

The rapid evolution of the Indian digital landscape over the last quarter-century has necessitated an equally rapid, though often contentious, evolution of its legal and regulatory frameworks. As India positions itself as a global leader in digital innovation and data management, the fundamental conflict between the individual's right to privacy and the state's duty to ensure national security has become the defining jurisprudential challenge of the contemporary era. This conflict is not merely a matter of statutory interpretation but is a deep-seated philosophical and operational struggle that pits the architecture of the modern internet—centered on end-to-end encryption and anonymity—against the sovereign requirements of a nation-state seeking to regulate cyberspace to prevent cyber-terrorism, financial fraud, and social instability.

India's journey from a nascent internet user base of 20 million in the year 2000 to a digital powerhouse with over 100 crore connections by 2025 represents a transformation of scale that few jurisdictions have matched. This transformation has been built upon a robust "Digital Public Infrastructure" (DPI), encompassing systems like the Unified Payments Interface (UPI), which processed over 21 billion transactions in a single month by late 2025, and the Aadhaar biometric database, the largest of its kind globally. However, the same infrastructure that has driven financial inclusion and administrative efficiency has also expanded the "attack surface" for both state and non-state actors. Between 2019 and 2023, cyber-attacks on the Indian government increased by 138 percent, while the surge in cybersecurity incidents reached over 20 lakh cases in 2024 alone. In this environment, the state's move toward "digital authoritarianism"—characterized by mass surveillance and the dismantling of encryption—stands in direct tension with the 2017 landmark judicial recognition of privacy as a fundamental right.

The Jurisprudential Foundation: From Restriction to Recognition

The modern understanding of privacy in India was finalized by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), but the path to this recognition was long and characterized by significant judicial resistance. For decades, the Indian state operated under a restrictive view of personal liberty. Early decisions in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962) held that the Indian Constitution did not explicitly guarantee a right to privacy. In M.P. Sharma, the court reasoned that in the absence of a provision similar to the Fourth Amendment of the US Constitution, a right to privacy could not be read into the protection against self-incrimination. Similarly, while the Kharak Singh judgment invalidated night-time "domiciliary visits" by police as a violation of ordered liberty, it explicitly stated that privacy was not a guaranteed right.

The 2017 Puttaswamy judgment marked a "watershed" moment, unanimously overruling these precedents and locating the right to privacy as an intrinsic component of Article 21 (the right to life and personal liberty) and Part III of the Constitution. The court's analysis was expansive, defining privacy not merely as the "right to be left alone" but as an overarching framework covering physical, informational, and decisional autonomy. Crucially, the court acknowledged that in an age of information, the collection and analysis of data about an individual grant the state and corporations power over that person, creating a "chilling effect" on fundamental freedoms if not strictly regulated.

To balance this new fundamental right against the state's legitimate interests, the nine-judge bench introduced a "triple-fold test" or "proportionality test," which has since become the benchmark for evaluating any state action that intrudes upon privacy.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

The Triple-Fold Test for State Intrusion Requirement

1. Detailed Criteria
2. Purpose and Application
3. Legality

The existence of a clear, valid law, Ensures state action is not based on arbitrary executive discretion or private contracts.

Need / Legitimate Aim A pressing social need or state interest
Valid aims include national security, preventing crime, public order, and the delivery of welfare benefits.

Proportionality A rational nexus between means and ends
The state must use the "least restrictive alternative" to achieve its objective, ensuring the impact on rights is minimized.

The application of this test has revealed deep inconsistencies in how courts handle state surveillance. For example, in the second Puttaswamy case (2018), which examined the Aadhaar Act, the court upheld the mandatory linking of Aadhaar with PAN numbers as proportional to prevent tax evasion but struck down Section 57, which allowed private companies to request Aadhaar for authentication, because a private contract does not constitute a "law" under the legality prong. This highlighted the court's intent to shift from a "culture of authority" to a "culture of justification," where the state must prove that every intrusion is strictly necessary.

The Statutory Evolution: The Information Technology Act and Beyond

For over twenty years, the primary instrument for digital governance was the Information Technology Act, 2000. Originally drafted to provide a legal basis for e-commerce and electronic signatures, the Act was ill-equipped for the complexities of modern data privacy. Its 2008 amendments significantly expanded state power through Section 69, which empowers the government to intercept, monitor, or decrypt any information through any computer resource. Unlike the Telegraph Act of 1885, which limited interception to the network of service providers, Section 69 allows agencies to bypass intermediaries and reach directly into a subscriber's personal computer, making it a far more intrusive mechanism for state surveillance.

This security-first model reached its zenith with the notification of the Information Technology **(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Rule 4(2)** introduced the "traceability" requirement, mandating that significant social media intermediaries—those with over 50 lakh users—enable the identification of the "first originator" of any message upon legal order. The government justified this as a necessary tool to combat "viral misinformation" and communal violence that has led to loss of life in incidents like mob lynchings. However, platforms like WhatsApp, utilizing end-to-end encryption (E2EE), filed immediate legal challenges in the Delhi and Kerala High Courts, arguing that traceability would require them to break the very encryption that protects the privacy of 50 crore Indian users.

The introduction of the Digital Personal Data Protection (DPDP) Act, 2023, was intended to modernize this regime by providing a standalone framework for personal data protection. Influenced by global standards like the GDPR, the DPDP Act introduces rights for "Data Principals" and obligations for "Data Fiduciaries," emphasizing consent as the core principle for lawful processing. Yet, the Act has been sharply critiqued for its "hollow heart"—specifically the repeal of Section 43A of the IT Act, which removed the right of data breach victims to seek individual compensation.

Transition from the IT Act to the DPDP Act Framework Feature

1. IT Act (2000/2008)
2. SPDI Rules (2011)
3. DPDP Act (2023)

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Scope of Data

- Only "Sensitive Personal Data" (SPDI) like passwords and health records.
- All digital personal data, regardless of its sensitivity.
- Applicability Primarily "body corporates".
- All persons and entities, including government agencies.
- Remedial Focus Compensatory: Victims could sue for damages.
- Penal-centric: Fines go to the state, not the victim.
- State Oversight Adjudicating Officers with broad discretion.
- Independent Data Protection Board (DPB) of India.
- Consent Opt-out for general data; written for sensitive.
- Explicit, free, informed, and withdrawable opt-in.

The state's preparations for operationalizing the DPDP Act in 2025 and 2026 show a focus on rapid enforcement. Phase I, effective from November 13, 2025, established the Data Protection Board, while full compliance for businesses is mandated by mid-May 2027. Despite these advancements, the state's broad exemptions under Section 17 of the DPDP Act allow it to bypass consent and transparency mandates for "national security" and "public order," terms that critics argue are alarmingly vague and lack the procedural safeguards required by the Puttaswamy judgment.

Technical Standoff: Traceability vs. End-to-End Encryption

The conflict over Rule 4(2) of the 2021 Rules represents the primary technical and legal flashpoint between the right to privacy and national security. End-to-end encryption is built on the principle that only communicating users can read the content, as messages are encrypted on the sender's device and decrypted only on the recipient's device. For platforms like WhatsApp, E2EE is not just a feature but a fundamental architecture that prevents anyone—including the service provider and the government—from accessing content.

The Indian government's stance is that traceability is possible without breaking encryption if platforms adopt alternative technologies. They emphasize that they are not asking for message content, only for the identification of the "first originator" of problematic information. However, technical experts and privacy advocates argue that to trace even a single message, a platform must maintain a massive database of "fingerprints" or hashes of every message sent, which effectively ends the promise of private, untracked communication.

Critical Evaluation of Proposed Traceability Mechanisms Method

1. Proposed Mechanism Security and Privacy Implications
2. The Kamakoti Proposal
3. Intermediaries hold originator info in escrow, linked to forwarded messages.

Requires fundamental changes to E2EE technology, creating a centralized target for hackers.

Hashing Libraries
Servers store alphanumeric hashes of all messages to match them.

Rest on the faulty assumption that identical content has identical hashes; can be reverse-engineered.

Metadata Tracking
Relying on unencrypted data trails and sender identity keys.

Undermines anonymity for whistleblowers and journalistic sources, leading to self-censorship.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Client-Side Scanning
Software on the device scans content before it is encrypted.

Turns every smartphone into a potential surveillance terminal, destroying the "zone of privacy".

The legal battle in the Delhi High Court has seen WhatsApp's counsel state that being forced to break encryption would lead to the platform withdrawing from the Indian market entirely. This "exit threat" underscores the stakes for digital sovereignty. As one analyst noted, the government may think they have won a key to the data, but if a foreign corporation like Meta holds the "master key" to the private conversations of 500 million Indians, the state is trading long-term digital sovereignty for a short-term safety feature. The global context is provided by the 2024 ECHR ruling in Podchasov v. Russia, which found that decryption orders that compromise the security of all users are "inherently disproportionate," regardless of the procedural safeguards implemented to restrict actual government access.

The Surveillance Apparatus: Mass Interception and Profile Aggregation
While high-profile encryption debates dominate the media, the Indian state has institutionalized an expansive surveillance ecosystem through systems that often bypass traditional warrant requirements. Projects like the Central Monitoring System (CMS), NETRA, and NATGRID allow for a level of data aggregation that transforms vital public spaces into "privacy-violating zones".

Central Monitoring System (CMS): This tool empowers the government to directly monitor communications across mobile and internet platforms without requiring service provider authorization, facilitating unprecedented access to personal data.

Network Traffic Analysis (NETRA): Developed by the DRDO, NETRA monitors internet traffic to flag suspicious keywords in social media posts, emails, and VoIP calls.

National Intelligence Grid (NATGRID): Established after the 2008 Mumbai attacks, NATGRID aggregates data from telecommunications, immigration, and financial records to create 360-degree profiles of individuals, often without adequate independent oversight.

The 2021 Pegasus spyware revelations served as a "wake-up call" regarding the vulnerability of this framework to misuse. Pegasus, a sophisticated malware, was allegedly used to target activists, journalists, and political opponents, allowing government agencies to monitor every file, contact list, and location on an infected phone. The Supreme Court's intervention in the Pegasus case and its demand for a probe by an independent committee highlighted the court's view that such acts are akin to "peeking through the veil of keepability itself".

The erosion of anonymity is further institutionalized through the 2022 and 2024 directions issued by CERT-In. These mandates require a wide range of entities—including data centers, cloud service providers, and VPN providers—to maintain detailed logs and subscriber information for a minimum of five years.

CERT-In Cybersecurity Compliance Requirements (2022-2026)

Obligation	Threshold / Detail	Rationale and Privacy Concern
Breach Reporting	Within 6 hours of discovery or notice.	Strictest globally (GDPR is 72 hours); forces "report first, verify later" mentality.
Log Retention	180 days within Indian jurisdiction.	High storage costs and increased risk of data breaches from centralized log stores.
KYC/Registration	Names, IPs, email, contact info for 5 years.	

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Eliminates "no-log" policies of VPNs; creates a permanent paper trail for law enforcement.
NTP Synchronization Must sync to NPL/NIC time servers.
Essential for forensic integrity but increases attack surface and centralized monitoring.
Annual Audits Mandatory 3rd-party audits for all enterprises.
Moves beyond "checkbox" compliance to operational maturity and infrastructure hardening.

The impact on the VPN industry was immediate. Providers that marketed themselves on a "strict no-log policy" found themselves in a position where they either had to alter their technical architecture—thereby compromising their core value proposition—or exit the Indian market. Major firms like NordVPN and PureVPN chose the latter, leading to concerns that law-abiding citizens would lose access to privacy-enhancing technologies while sophisticated criminals simply migrated to non-regulated, foreign platforms.

AI, Deepfakes, and the 2026 Regulatory Pivot

The emergence of generative AI has introduced a new layer of complexity to the privacy-security debate. In early 2026, the Indian government moved from reactive content moderation to proactive algorithmic governance through amendments to the IT Rules. These rules provide the first legal recognition of "Synthetically Generated Information" (SGI)—any media created or modified by algorithms to appear authentic.

The 2026 amendments impose some of the most aggressive takedown timelines in the world, requiring platforms to remove deepfake pornography within two hours and other unlawful content within three hours of a government notice. To retain their "safe harbor" protection under Section 79 of the IT Act, platforms must now use automated AI filters to block the upload of illegal content. Critics argue that these timelines are impossible for smaller intermediaries to meet, potentially cementing the monopoly of tech giants like Meta and X, who are the only entities with the resources to maintain the necessary 24/7 legal and technical infrastructure.

Risks and Uncertainties in the 2026 AI Governance Framework
Challenge Area
Mechanism / Provision
Potential Adverse Outcome
Algorithmic Bias
Proactive filtering for "misinformation".
Automated tools often fail to distinguish satire or political parody, leading to over-censorship.
Asymmetric Liability Safe harbor is lost for failure to remove, but no penalty for wrong removal.
Systemic incentive to "delete first, verify later," eroding procedural safeguards.
Source Provenance Mandatory watermarking and provenance metadata.
Permanent digital fingerprints make anonymous whistleblowing impossible; traceable to the AI tool used.
Agentic AI AI tools executing actions autonomously.
Breaks traditional assumptions of human-controlled decision-making and accountability.

The 2026 AI Impact Summit in New Delhi highlighted that India is wagering its long-term advantage on "**integration capacity**" rather than frontier technological leadership. The unveiling of three major indigenous "Sovereign AI" models signals a decisive shift toward building a national AI stack that uses local data and Indian languages, thereby reducing dependence on global tools that might be vulnerable to foreign intelligence or geopolitical leverage. However, this " techno-legal approach" often allows the state to act as both regulator and participant, creating a conflict of interest where security measures might be used to suppress legitimate political dissent under the banner of combating deepfakes.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

The Transparency Paradox: Diluting the Right to Information

One of the most profound and controversial impacts of the new privacy regime is the amendment to the Right to Information (RTI) Act, 2005. Historically, Section 8(1)(j) of the RTI Act provided a narrow exemption for personal information, but it was qualified by two critical safeguards: the "public activity" test and the "public interest override". If disclosure was necessary to advance public interest, or if the information could not be denied to Parliament, it had to be shared with the citizen.

Section 44(3) of the DPDP Act has effectively removed these safeguards, substituting a categorical and absolute bar on the disclosure of any "personal information". Transparency activists argue that this "weaponizes" privacy, allowing public officials to hide records of their assets, qualifications, and performance of duties. In March 2026, the Supreme Court issued a notice in a petition filed by journalist Geeta Seshu and the Software Freedom Law Center, challenging these provisions as an attempt to "shield the state from scrutiny". The Chief Justice noted the urgency of defining "public data" versus "personal data" in an era where data has become the "true wealth of the day".

The removal of journalistic carve-outs from the DPDP Rules 2025 further exacerbates this chilling effect. Journalists investigating public corruption are now treated as "data processors" who may be required to obtain consent from the very individuals they are investigating, potentially alerting suspects and making investigative reporting impossible. The DIGIPUB News India Foundation and the Editors Guild of India have warned that this regulatory framework endangers source confidentiality and facilitates disproportionate state overreach into editorial independence.

Global Convergence and the Future of Digital Security

India's struggle to balance privacy and security is mirrored in several other major jurisdictions, though India's timelines are notably more aggressive. The United States' recently implemented "Bulk Data Transfer Rule" and the UK's "Investigatory Powers Act" (often called a "snooper's charter") both reflect a growing national security overlay on cybersecurity regulation. However, international frameworks like the OECD's Recommendations on Digital Security Risk Management and the UN Security Council's high-level AI debates suggest a growing consensus that security and privacy should not be treated as a "zero-sum" game.

In 2026, the convergence of AI, privacy concerns, and cross-border regulatory requirements is set to redefine corporate data strategies. Leading organizations are moving toward "Privacy-Enhancing Technologies" (PETs) like differential privacy and homomorphic encryption, which allow them to derive value from data without revealing raw sensitive information.

Comparison of International Cybersecurity and Privacy Frameworks (2025-2026)

Jurisdiction Key Legislation / Rule Reporting Window Primary Focus
India
DPDP Act 2023 / CERT-In Directions.
6 Hours (Mandatory).
Sovereignty, Traceability, and Consent.
European Union NIS2 Directive / AI Act.
24 - 72 Hours (Tiered).
Risk-based, Harm-centric, and Transparent.
United States CIRCIA / Bulk Data Transfer Rule.
72 Hours (Critical Infra).
Geopolitical Risk and National Security.
China PIPL / Synthetic Media Rules.
Immediate (Significant incidents).
Sovereignty and Platform Traceability.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(2), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

The 2026 outlook suggests that while India has secured Tier 1 status in the ITU Global Cybersecurity Index, its "organizational measures" remain an area for potential growth. The recent amendment to the Allocation of Business (AoB) Rules, which task the National Security Council Secretariat (NSCS) with overall coordination for cybersecurity, is a significant move toward reducing institutional silos. However, the real challenge lies in whether India can bridge the gap between its ambitious technological goals and its constitutional obligations to protect the individual.

Conclusion: Toward a Rights-Respecting Digital Sovereignty

The conflict between the fundamental right to privacy and the mandates of national cybersecurity laws in India has entered a phase of intense structural transformation. The Puttaswamy judgment provided the normative architecture for a "Constitution 3.0" that places the individual at the center of the constitutional scheme. However, the operational reality—characterized by mass surveillance systems like CMS and NATGRID, the compression of content takedown timelines, the dismantling of RTI safeguards, and the legal stalemate over end-to-end encryption—indicates a persistent state bias toward executive convenience and opacity.

For India to maintain public trust in its rapidly expanding digital ecosystem, it must shift from a model of "surveillance by default" to "privacy by design". This requires several critical reforms: the reintroduction of the public interest override in the RTI Act; the establishment of independent, judicial oversight for intelligence agencies; and the adoption of technical standards for traceability that do not compromise the integrity of encryption for the entire population. The success of India's digital public infrastructure was built on clarity and trust; its future will depend on whether its cybersecurity laws are perceived as a shield for its citizens or as a sword for the state. As the digital frontier continues to redefine the boundaries of sovereignty, India’s ability to "iron out the creases" between safety and liberty will set a precedent for the global South and the wider democratic world.

Reference:

1. Justice K.S. Puttaswamy (Retd) v. Union of India (2017): The foundational "Privacy Judgment" which declared privacy a fundamental right under Article 21. It established the "Triple Test" for any state intrusion: legality, legitimate state interest (including national security), and proportionality.
2. Article 19(1)(a) & 19(2): These deal with freedom of speech and the "reasonable restrictions" the state can impose for sovereignty and security. Recent Supreme Court reviews have scrutinized whether new data laws overstep these boundaries.
3. Digital Personal Data Protection (DPDP) Act, 2023
4. Information Technology Act, 2000 (and 2021 Rules)
5. Telecommunications Act, 2023
6. DPDP Rules, 2025
7. National Cyber Coordination Centre (NCCC) & CERT-In Guidelines
8. Privacy vs. National Security: Balancing Surveillance and Data Protection in India (2026)
9. Analysis of Institutional Independence