INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 4 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 4 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-4-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY IN INDIA: LEGAL CHALLENGES IN THE DIGITAL AGE

AUTHOR – RANJANA* & DR. RANA PARVEEN**

* RESEARCH SCHOLAR, SCHOOL OF LAW AND JURISPRUDENCE, SHRI VENKATESHWARA UNIVERSITY, GAJRAULA, AMROHA

***RESEARCH SUPERVISOR, SCHOOL OF LAW AND JURISPRUDENCE, SHRI VENKATESHWARA UNIVERSITY, GAJRAULA, AMROHA*

BEST CITATION – RANJANA & DR. RANA PARVEEN, DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND CYBER SECURITY IN INDIA: LEGAL CHALLENGES IN THE DIGITAL AGE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 06-16, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The rapid digitization of the Indian economy has transformed the socio-legal fabric of the nation, necessitating a sophisticated legal architecture to govern the triad of data protection, artificial intelligence, and cybersecurity. This report provides a comprehensive analysis of the Digital Personal Data Protection Act (DPDPA), 2023, and its intersection with the existing Information Technology (IT) Act, 2000, and emerging Artificial Intelligence (AI) regulations. It situates these legislative developments within the constitutional framework established by the landmark *Justice K.S. Puttaswamy v. Union of India* verdict, which elevated privacy to a fundamental right. The analysis critically evaluates the shift from a security-centric IT regime to a developmental, consent-based privacy framework, highlighting the friction between individual autonomy and state surveillance. Furthermore, the report explores the "responsibility gap" in AI liability, the procedural conflicts between cybersecurity reporting directives and privacy breach notifications, and the potential erosion of transparency through amendments to the Right to Information (RTI) Act. By synthesizing primary legal sources, global comparative paradigms, and philosophical insights from Indian Knowledge Systems alongside literary critiques of the surveillance state, this study offers a nuanced perspective on the challenges of preserving human dignity in an increasingly automated and data-driven republic.

Keywords: *Digital Personal Data Protection Act (DPDPA) 2023; Artificial Intelligence Regulation; Cybersecurity; Right to Privacy; Justice K.S. Puttaswamy; Information Technology Act 2000; Data Protection Board of India; Algorithmic Bias; Surveillance State; Data Sovereignty*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

.

The Digital Renaissance and the Regulatory Imperative: A Narrative Prologue

The evolution of India's digital landscape resembles the "butterfly approach" once alluded to by the national poet Rabindranath Tagore, who noted that "The butterfly counts not months but moments, and has time enough".("10 Thoughts on Law and Justice in India," n.d.) In the relentless moments of the twenty-first century, India has undergone a metamorphosis from a primary site of information technology outsourcing to a digital sovereign defined by vast data repositories and a burgeoning artificial intelligence ecosystem. However, this transition has been marked by an "obsession with time" and a corresponding urgency to establish a regulatory framework that can keep pace with technological acceleration. The initial legislative response, the Information Technology (IT) Act of 2000, was born of a simpler era, focused primarily on facilitating electronic commerce and penalizing computer-related dishonesty. As the digital age matured, it became clear that this "patchwork" of rules, including the 2011 Sensitive Personal Data or Information (SPDI) Rules, was structurally unfit to address the complexities of a data-intensive society.

The fundamental legal challenge of our time is to reconcile the "right of the individual to protect their personal data" with the "need to process such personal data for lawful purposes". This duality is not merely a matter of administrative law but a philosophical inquiry into the nature of the modern state. In the context of India, this inquiry is deeply rooted in the concept of *Dharma*—the righteous duty that sustains the social and cosmic order.(Sahoo, 2024) In the digital realm, *Dharma* manifests as the ethical obligation of "Data Fiduciaries" to protect the "Data Principals" whose lives are increasingly represented by digital traces.(THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, n.d.) Yet, as technology advances, the specter of the "mechanical state" described by Tagore looms—a state that "will never heed the voice of truth and goodness" but continues in its "ring-dance of moral corruption," linking machine unto machine while trampling the "sweet flowers of simple faith". (*Nationalism Quotes by Rabindranath Tagore*, n.d.) It is against this backdrop of constitutional promise and technological peril that the current legal landscape must be assessed.

The Constitutional Bedrock: Puttaswamy and the Birth of Informational Privacy

The current trajectory of Indian data protection law is inextricably linked to the landmark decision in *Justice Puttaswamy case* (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017). This case serves as the "cornerstone" of privacy jurisprudence in India, where a nine-judge bench of the Supreme Court unanimously reaffirmed that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution. The court recognized that privacy is an "attribute of human dignity" and an "intrinsic aspect of dignity, autonomy and liberty".

The Doctrinal Toolkit of Proportionality

The *Puttaswamy* judgment was transformative because it moved beyond the narrow conception of privacy as a right against physical intrusion, expanding it to include "decisions, choices, information and freedom". The court articulated a "doctrinal toolkit" for assessing any state interference with this right. For any law or state action to validly infringe upon privacy, it must satisfy a rigorous three-fold test:

1. **Legality**: There must be a specific law that authorizes the intrusion.
2. **Legitimacy**: The state must demonstrate a "legitimate state aim," such as national security, public order, or the prevention of crime.
3. **Proportionality**: There must be a rational nexus between the state's objective and the means adopted, ensuring that the intrusion is the least restrictive measure possible.

This test was specifically applied to the Aadhaar scheme, where the Court upheld the constitutionality of the biometric database but imposed significant restrictions to prevent its "mandatory" use in contexts that were not linked to welfare benefits.[16] The judgment also dismissed the "elitist construct" argument—the claim that the poor would trade privacy for bread—asserting instead that privacy is a right of all individuals regardless of their socio-economic status.

Implications for the Digital State

The concurring opinions in *Puttaswamy* highlighted the specific dangers of the digital age. Justice Kaul emphasized the need for a data protection regime to regulate the "interception of data by the State" and protect "informational privacy". Justice Chandrachud noted that privacy includes a "negative right against State interference" and a "positive right to be protected by the State".[13] This positive obligation directly necessitated the drafting of the Digital Personal Data Protection Act, as the court recognized that the collection of information creates a "power over" the individual, which can have a "chilling effect" on the expression of dissent and the exercise of fundamental freedoms.

The Digital Personal Data Protection Act, 2023: A Detailed Legal Anatomy

Enacted on August 11, 2023, the Digital Personal Data Protection Act (DPDPA) represents India's first comprehensive attempt to legislate on data privacy.[4] It establishes a "development-oriented" paradigm that seeks to balance individual rights with the "sovereign necessity of data utilisation for economic growth".(*Data Protection in India: Overview*, n.d.)

Scope and Applicability

The DPDPA applies to the processing of "digital personal data" within India, whether collected online or digitised from offline sources.[6] Notably, the Act has an extraterritorial reach, applying to processing outside India if it is related to the offering of goods or services to individuals within India.[4] However, unlike the GDPR, the DPDPA specifically excludes non-digital records from its scope, creating a potential lacuna for data stored in physical formats that are never digitized.

Feature	**Digital Personal Data Protection Act (DPDPA) 2023**	**EU General Data Protection Regulation (GDPR)**
Primary Basis	Explicit Consent or "Certain Legitimate Uses"	Consent, Contractual Necessity, Legitimate Interests, etc.
Data Classification	Uniform (No "Sensitive" category)	Tiered (Heightened protection for Sensitive data)

Right to Portability	Not granted	Explicitly granted
Right to Object	Diluted/Not explicitly granted	Explicitly granted
Regulator	Data Protection Board of India (DPB)	Independent Data Protection Authorities (DPAs)

The Architecture of Consent

The Act pivots on the "Consent" of the Data Principal as the primary lawful basis for processing. Consent must be "free, specific, informed, unconditional and unambiguous". Before seeking consent, a Data Fiduciary must provide a notice detailing the data to be collected and the purpose of processing. The Act also introduces the concept of "Consent Managers"—entities registered with the Board that allow individuals to "give, manage, review and withdraw" their consent through a single, interoperable platform.

However, the Act also defines "Certain Legitimate Uses" where consent is not required, such as the "voluntary sharing" of data, medical emergencies, employment purposes, and the "provision of benefit or service by the government". Critically, Section 7 of the Act allows the State to process personal data for any "permit, license, benefit or service" if the data was provided for *another* purpose, effectively removing the principle of "purpose limitation" for government processing.(*The Digital Personal Data Protection Bill, 2023*, n.d.)

Obligations of Data Fiduciaries and Processors

The Act distinguishes between a "Data Fiduciary"—the entity that determines the purpose and means of processing—and a "Data Processor," who processes data on behalf of the fiduciary. Significant obligations are placed on fiduciaries, including:

- **Security Safeguards**: Implementing reasonable measures to prevent data breaches.
- **Accuracy and Completeness**: Ensuring that personal data is accurate and complete when used to make decisions.
- **Data Retention**: Deleting data once the purpose for its collection has been fulfilled, unless retention is required by law.
- **Significant Data Fiduciaries (SDFs)**: The government may designate certain fiduciaries as "Significant" based on the volume and sensitivity of data processed and the potential risk to "electoral democracy" or "security of the State".[4] SDFs must appoint a Data Protection Officer (DPO) and conduct periodic data protection impact assessments and audits.

The Cybersecurity Crucible: CERT-In, the IT Act, and the Friction of Dual Compliance

Cybersecurity in India is primarily governed by the Information Technology Act, 2000, and the directions issued by the Indian Computer Emergency Response Team (CERT-In).[3] The emergence of the DPDPA creates a complex environment where single events trigger multiple, overlapping regulatory obligations.

The 6-Hour Rule vs. the 72-Hour Window

The most significant point of friction lies in breach notification timelines. Under the 2022 CERT-In Directions, entities are required to report cybersecurity incidents within a strict 6-hour window of detection. These directions

apply broadly to service providers, intermediaries, data centers, and corporate bodies. In contrast, the DPDPA requires fiduciaries to notify the Board and affected individuals of a personal data breach "promptly," with draft rules suggesting a more pragmatic 72-hour window.(G, 2025)

Metric	CERT-In Reporting (Security-Centric)	DPDPA Reporting (Privacy-Centric)
Trigger	"Cybersecurity incident" (Broad list) [26]	"Personal data breach"
Recipient	CERT-In	Data Protection Board + Affected Individuals
Timeline	Within 6 hours of awareness	Within 72 hours (Draft Rules)
Focus	Technical logs, IP addresses, forensic reports	Nature of breach, likely harm, remedial steps

This "dual-breach notification" duty means that in a ransomware attack, a hospital or a fintech firm must simultaneously preserve logs for forensic analysis by CERT-In while crafting user-centric notifications for the Data Protection Board. Non-compliance with CERT-In can lead to criminal liability, while failure to notify the DPB carries civil penalties of up to ₹200 crore.

The Right to Erasure vs. Data Retention

A second area of conflict concerns the "Right to Erasure" granted to Data Principals under the DPDPA. While the DPDPA mandates that data be deleted once its purpose is served, CERT-In directions impose broad "data retention requirements" for cybersecurity resilience and the investigation of crimes. Organizations must navigate these "seemingly contradictory regimes," balancing the individual's right to be forgotten against the state's requirement for a permanent digital trail.(G, 2025)

The Artificial Intelligence Frontier: Algorithmic Bias and the Responsibility Gap

As AI systems transition from productivity tools to "emotionally influential systems," Indian law remains "unprepared to confront the implications of harm caused by autonomous or algorithm-driven acts".(*Algorithmic Harm and Generative AI*, n.d.) Currently, India lacks a standalone AI statute, relying instead on a "patchwork" of existing statutes and policy documents.

The MeitY AI Advisory 2024: A Regulatory Oscillation

In March 2024, the Ministry of Electronics and Information Technology (MeitY) issued a controversial advisory for AI platforms and intermediaries. Originally, it mandated that "under-testing or unreliable" AI models obtain "explicit permission" from the government before being deployed to users in India—a move that critics argued would *"kill startups"*

unable to afford government liaison and rigorous testing. Following a revised advisory on March 15, 2024, the "permission" requirement was rescinded and replaced with a *"labelling"* mandate. Intermediaries are now directed to label "undertrial/unreliable" models to inform users of the "possible inherent fallibility or unreliability of the output generated".("Navigating AI Regulation in India," n.d.)

Algorithmic Bias and Constitutional Safeguards

The use of AI in high-stakes sectors like hiring, lending, healthcare, and policing raises significant concerns regarding "algorithmic bias". Bias can originate at the "data collection phase" (historical societal prejudices), the "algorithm design" (cognitive pitfalls of developers), or through "feedback loops" where AI learns from biased user interactions. In India, these biases threaten the constitutional values of "liberty, equality, and justice".

- **Article 14**: Guarantees equality before the law; biased algorithms in recruitment or credit scoring may violate this right if they operate on "opaque criteria".
- **Article 15 & 16**: Prohibit discrimination based on race, religion, or sex; AI systems that replicate historical discrimination in employment or public access attract direct constitutional scrutiny.
- **Article 21**: Protects life and personal liberty, including the right to "fair treatment" by automated decision-making systems.

The Liability Challenge: Tort and Criminal Law Gaps

Assigning responsibility for AI-induced harm remains a complex legal hurdle. The "Black Box Problem" means that developers are not currently required to disclose the internal logic of their models, making it difficult for courts to determine "standard of care" or "causation".[31]

1. **Tort Law**: Traditional negligence requires a "foreseeable" harm. However, advanced AI that adapts independently via machine learning may produce outcomes that a developer could not reasonably anticipate.
2. **Product Liability**: The Consumer Protection Act 2019 provides remedies for "defective products," but it is unclear if software—especially software that evolves post-deployment—qualifies as a "product" under strict liability.
3. **Criminal Liability**: The Indian Penal Code (IPC) and the new Bharatiya Nyaya Sanhita (BNS) base liability on *mens rea* (guilty mind). Since AI lacks consciousness, and harm often arises from "distributed responsibility" across developers, data providers, and deployers, holding a specific human actor criminally liable is "highly problematic".

The Surveillance State and Literary Dystopias: Orwell, Kafka, and the Panopticon

The expansion of digital governance in India has reinvigorated debates about the "Surveillance State." Primary among the concerns is Section 69 of the Information Technology Act, which grants the government "disproportionate and unchecked power" to intercept and monitor digital communications for investigating even "the pettiest of crimes".

The Orwellian Shadow and Section 69

George Orwell's *1984* envisioned a world of "constant surveillance" through "telescreens" that serve as both monitoring devices and propaganda tools. In the Indian context, the lack of "independent inter-branch oversight" over surveillance authorization creates a scenario where the executive monitors itself. As Orwell noted, the goal of such surveillance is to create "docile, conformed bodies" to sustain control over individuals. The DPDPA 2023 arguably exacerbates this by granting blanket

exemptions to state agencies under Section 17, allowing the government to conduct large-scale data collection without the safeguards applied to private entities.(Bhandari & Lahiri, 2020)

Kafkaesque Complexity and Accountability

While Orwell provides the model for overt control, Franz Kafka's work illustrates the "menacing complexity" of systems where "accountability becomes meaningless". In a "Kafkaesque" world, the individual struggles against a force that "does not lend itself to human logic".(Bluemink, 2015) This is mirrored in the DPDPA's adjudicatory framework: the Data Protection Board is appointed by the central government, raising doubts about its "willingness to enforce the law rigorously" against the state itself. When a citizen's data is compromised by a government agency, the path to redress is often obscured by procedural barriers and the "vague language" of national security exceptions.

Panopticism and the Chilling Effect

Michel Foucault developed Jeremy Bentham's "Panopticon" into a symbol of social control where individuals "self-regulate their behaviour" because they feel they are *always* being watched. In the digital era, the collection of biometric and behavioural data creates an "internalized authority". Justice Chandrachud in *Puttaswamy* warned that this "collection of information" has a "chilling effect not only on the expression of dissent but also on the exercise of fundamental rights".[14] The "Thought Police" of our age are not merely agents at the door, but the invisible algorithms that "manufacture feelings" and become "suspiciously watchful" when individuals show signs of "inclining toward the dissident".

Reconciling Transparency and Privacy: The DPDPA vs. the RTI Act

A critical conflict arises between the DPDPA 2023 and the Right to Information (RTI) Act, 2005. Section 44(3) of the DPDPA amends Section 8(1)(j) of the RTI Act to provide a "blanket exemption" for any "information which relates to personal information".

The Erosion of Public Accountability

Previously, the RTI Act allowed the disclosure of personal information if a Public Information Officer (PIO) was satisfied that a "larger public interest justifies the disclosure". The amendment removes this discretion and the "proviso" which stated that information that cannot be denied to Parliament shall not be denied to a citizen. Critics argue that PIOs may now "deny information arbitrarily" by simply quoting the DPDPA, thereby undermining the transparency required for a healthy democracy. This shift represents a prioritization of the "secrecy of the state" over the "right to freedom of speech and expression" which inherently implies a right to information.

Procedural Barriers and Digital Inequality

Furthermore, the DPDPA's Data Protection Board operates "almost exclusively in digital form," which creates a significant barrier in a country where internet penetration was only 52.4% in early 2024. While the RTI Act mandates "reasonable assistance" to those who cannot write their requests, the DPDPA's digital-first approach risks excluding the uneducated and the digitally marginalized, further concentrating power in the hands of the "technologically savvy".

Institutional Independence: Critiquing the Data Protection Board of India

The Data Protection Board (DPB) is the central watchdog for the DPDPA, tasked with investigating breaches and imposing penalties. However, its structural design has been criticized for "executive control" that undermines its autonomy.

Appointments and Tenure

Unlike independent regulators like the Securities and Exchange Board of India (SEBI) or the GDPR's Data Protection Authorities, the DPB's members are appointed unilaterally by the central government without bipartisan or judicial oversight. The short two-year term for members, with the possibility of re-appointment, may "affect the independent functioning of the Board," as members may feel pressured to align with government interests to secure another term.(*Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards - Express Computer*, n.d.)

The Veto of the Sovereign

Section 27(3) of the Act enables the central government to "issue directions" that the DPB may "modify or suspend" its own orders based on government reference. This effectively gives the union government a "veto or override power" on the Board's decisions, violating the principle of *nemo judex in causa sua* (no one should be a judge in their own cause) since the government is a major data processor itself. Consequently, observers have warned that the DPB may become a "watchdog without teeth," reluctant to penalize state agencies for breaches in projects like Aadhaar or DigiLocker.(*Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards - Express Computer*, n.d.)

Global Comparative Regimes: GDPR, EU AI Act, and the Indian Developmental Model

India's DPDPA is often compared to the EU's GDPR, but they represent "distinct paradigms". While the GDPR establishes a "strict rights-based framework," the DPDPA prioritizes "digital innovation" and "economic growth".

Rights-Based vs. Development-Oriented

The GDPR functions as a "robust shield" for individual dignity, providing extensive rights like data portability and the right to object to automated decision-making. The DPDPA, however, functions as a "flexible umbrella" framework that facilitates "ease of business". For instance, while the GDPR imposes turnover-based penalties (up to 4% of global turnover), India adopts "fixed penalty caps" (up to ₹250 crore), offering greater regulatory predictability for multinational enterprises.

Risk-Based AI Regulation

The EU AI Act (2024) provides a "horizontal" regulatory framework that categorizes AI based on "risk levels"—unacceptable, high, and limited risk. AI systems with "unacceptable risk" (e.g., social credit scoring) are banned, while "high-risk" systems (e.g., biometrics) face strict transparency and safety standards.[45] In contrast, India's current approach, defined by the MeitY advisories, is "vaguely formed," focusing on "trust, fairness, and accountability" through non-binding guidelines rather than a tiered risk-oriented platform.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Paradigm	EU Model (GDPR/AI Act)	India Model (DPDPA/Advisories)
Philosophical Base	Privacy as a Fundamental Right	Privacy balanced with Development
Data Hierarchy	Rigid (Sensitive vs. Non-Sensitive)	Uniform (All personal data is the same)
AI Focus	Precautionary; Risk-based classification	Flexible; Democratization of access
Enforcement	Strong independent oversight	Centralized, executive-led oversight

Philosophical Foundations: Dharma, Karma, and Ethical Governance

In seeking an ethical grounding for these legal challenges, Indian jurisprudence can draw upon "Indian Knowledge Systems" (IKS). The concept of *Dharma* (duty) signifies "ethical conduct and responsibility toward others". An AI system or data protection framework designed with *Dharma* in mind would prioritize "fairness, justice, and the greater good".

Satya, Ahimsa, and Accountability

The principles of *Satya* (truth) and *Ahimsa* (non-violence) discourage "unnecessary harm and deceit" in data collection and surveillance.[7] Furthermore, the principle of *Karma*—the law of action and consequence—can inform accountability frameworks: AI systems should be designed to "track consequences and learn from outcomes," mirroring this ethical principle.[10] The goal is to move toward a "digital democracy" where technology serves the "greater good, preserves individual dignity, and promotes social cohesion," rather than merely favoring "profitability and efficiency". (Singh, 2024)

The Vision of Ramrajya and Vasudevam Kutumbkam

Vedic philosophy offers the vision of *Ramrajya* (moral governance) and *Vasudevam Kutumbkam* (the world is one family). In the digital age, these ideals suggest a framework where technology reinforces "universal connectedness" and "equal opportunities for everyone".[50] However, this "blending of insights" requires careful "contextualization," as the digital age introduces challenges—like deepfakes and mass surveillance—that ancient records could not have predicted. As Tagore warned, the "Nation" is an "abstract being" that can perform "wholesale and universal acts of fearful responsibility" with "systematic unawareness" of the individual sensibilities it crushes.

Conclusion: Navigating the Digital Straits

The transition of India into a digital-first society is a journey through "pathless sky" and "trackless water". The Digital Personal Data Protection Act, 2023, while a "robust foundation," remains an incomplete answer to the country's privacy challenges. Its success will depend on

how the Data Protection Board assertively enforces regulations against powerful entities, how responsibly the government exercises its "vague and subjective" exemption powers, and how the courts interpret the "test of proportionality" established in *Puttaswamy*.

The intersection of artificial intelligence and cybersecurity necessitates a "Digital Bill of Rights" that ensures constitutional values are respected in an era of "automated or algorithmic choices". We must avoid the "Kafkaesque" horror where the individual never knows "what is happening or when" because the system is too large to fight. Instead, the legal framework must strive to be like the "clear stream of reason" in Tagore's *Gitanjali*—a stream that has not "lost its way into the dreary desert sand of dead habit".

Ultimately, data protection in India must not be viewed as a "trade-off" between security and liberty, but as a realization of the "freedom of the soul" in a digital guise. By harmonizing the "Three-Tiered Reality" of global standards, national developmental needs, and ethical imperatives, India can ensure that technology serves humanity, rather than becoming the "fetich of nationalism" to which freedom and humanity are every day sacrificed. In this age of globalization, where the butterfly counts its moments, India has "time enough" to build a digital republic where knowledge is free, the mind is without fear, and the head is held high.

References

1. 10 Thoughts on Law and Justice in India. (n.d.). *Harvard Law School Center on the Legal Profession*. Retrieved March 16, 2026, from https://clp.law.harvard.edu/article/10-thoughts-on-law-and-justice-in-india/
2. *Algorithmic Harm and Generative AI: Tort Exposure at the Edge of Emerging Technology*. (n.d.). Retrieved March 16, 2026, from https://www.wshblaw.com/publication-algorithmic-harm-and-generative-ai-tort-exposure-at-the-edge-of-emerging-technology
3. Bhandari, V., & Lahiri, K. (2020). The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World. *3*.
4. Bluemink, M. (2015, March 9). Kafka, Orwell, Huxley: The Surveillance State in Literature. *Blue Labyrinths*. https://bluelabyrinths.com/2015/03/09/kafka-orwell-huxley-the-surveillance-state-in-literature/
5. *Data Protection in India: Overview*. (n.d.). Thomson Reuters.
6. *Enforcement Gaps in India's DPDP Act and the case for decentralized data protection boards—Express Computer*. (n.d.). Retrieved March 16, 2026, from https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140/
7. G, D. K., Vaishnavi Viswanathan,Viswanathan. (2025, October 13). *Obligations under CERT-In and DPDP – Not a zero-sum game*. Bar and Bench - Indian Legal News. https://www.barandbench.com/view-point/obligations-under-cert-in-and-dpdp-not-a-zero-sum-game
8. Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 AIR 4161 (The Supreme Court of India 2017).
9. *Nationalism Quotes by Rabindranath Tagore*. (n.d.). Retrieved March 16, 2026, from https://www.goodreads.com/work/quotes/160596-nationalism
10. Navigating AI Regulation in India:

Unpacking the MeitY Advisory on AI in a Global Context - ELP Law. (n.d.). *Economic Laws Practice*. Retrieved March 16, 2026, from https://elplaw.in/leadership/navigating-ai-regulation-in-india-unpacking-the-meity-advisory-on-ai-in-a-global-context/

11. Sahoo, J. (2024, September). *Dharma and Digital Democracy: An Indian Perspective on Participatory Governance*. Conference: International Conference on Indian Knowledge Systems: Global Perspectives and Practices.
12. Singh, N. (2024, January 23). *Navigating AI Regulation: A Comparative Analysis of EU and Indian Perspectives*. https://digi-con.org/navigating-ai-regulation-a-comparative-analysis-of-eu-and-indian-perspectives/
13. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, 22, The Parliament of India.
14. *The Digital Personal Data Protection Bill, 2023*. (n.d.). PRS Legislative Research. Retrieved March 16, 2026, from https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023