REGULATING THE DIGITAL LEVIATHAN: LEGAL CHALLENGES AND REFORM PATHWAYS IN INDIA'S AI, DATA, AND CYBERSECURITY LANDSCAPE

Avinash Verma, National University of Study and Research in Law, Ranchi
Divyansh Singh, National University of Study and Research in Law, Ranchi

ABSTRACT

India's digital revolution has brought incredible opportunities, but it has also created significant legal challenges that our current laws struggle to address. This paper explores how India is trying to regulate emerging technologies like artificial intelligence, protect personal data, and combat cybercrime, while comparing our approach to international standards.

The government's digital initiatives such as Aadhaar and Jan Dhan Yojana have transformed how Indians interact with technology, yet our legal framework remains fragmented and often outdated. The Digital Personal Data Protection Act of 2023 and the Information Technology Act of 2000, while important steps, still leave major gaps in regulation and enforcement. When compared to robust international frameworks like Europe's GDPR and AI Act, India's approach appears less comprehensive and more reactive.

This research examines three critical areas: data privacy protection, AI governance, and cybersecurity law. Through this analysis, it becomes clear that India's regulatory landscape suffers from overlapping authorities, inconsistent enforcement, and a lack of coordination between different government bodies. The paper argues that India needs a more unified, rights-based approach to digital governance that protects individual freedoms while encouraging innovation.

The study concludes that meaningful reform requires creating new institutional frameworks, such as a Digital Law Commission, and fostering better cooperation between regulators, courts, and civil society. Only through such comprehensive changes can India effectively balance technological progress with constitutional rights and national security in our digital age.

Keywords: Digital Governance, Artificial Intelligence, Data Protection, Cybersecurity, Regulatory Reform

Introduction

India's journey toward a digital economy has profoundly reshaped the country, weaving economic ambitions with social and political goals to change how people, businesses, and institutions operate[1]. The government has spearheaded this effort with key initiatives like **Aadhaar** and the **Jan Dhan Yojana**, which demonstrate its use of technology as a tool for improving governance, public service delivery, and overall innovation[2]. This transition, however, is about more than just adopting new technology; it also underscores the ongoing challenge of bridging the gap between the promise of inclusivity and the realities of unequal access to infrastructure and digital literacy[3]. Furthermore, as India's digital public infrastructure grows, it has created tensions between state and private entities over issues like surveillance, regulatory oversight, and accountability, which demand greater ethical and legal scrutiny [4].

The integration of **artificial intelligence (AI)** and **big data** has made this landscape even more intricate. AI-powered systems are increasingly used in various sectors, from healthcare and banking to agriculture and law enforcement[5]. While this presents immense potential for innovation, it also raises significant concerns. Opaque decision-making processes, the risk of inherent bias, and threats to traditional employment patterns continue to test the resilience of India's regulatory frameworks [6]. In addition, the rapid expansion of data-driven platforms and the constant "datafication" of daily life have exposed individuals to greater risks of privacy breaches and security vulnerabilities. These risks are worsened by the unrestricted flow of data across borders, often making effective jurisdictional oversight difficult[7]. Recent incidents of large scale cyberattack on government databases and critical infrastructures have further reinforced the understanding that cyberspace is no longer merely a technological issue but also

[1] S. Inampudi, *Barriers to Implementation of Digital Transformation in the Indian Health Sector: A Systematic Review*, 11 Humanities & Soc. Scis. Comm. (2024), https://www.nature.com/articles/s41599-024-03081-7.
[2] M. Totty, *Addressing Its Lack of an ID System, India Registers 1.2 Billion in a Decade*, UCLA Anderson Rev. (Mar. 13, 2022), https://irjems.org/irjems-v2i3p170.html
[3] S. Kraus, *Digital Transformation: An Overview of the Current State*, 11 SAGE Open 3 (2021), https://journals.sagepub.com/doi/10.1177/21582440211047576.
[4] S. Inampudi, *supra* note 1.
[5] *Accelerating Digital Transformation Through Digital Leadership: Strategies for Innovation, Sustainability, and Organisational Performance Enhancement*, 11 BISMA (2025), https://journal.unesa.ac.id/index.php/bisma/article/view/38859.
[6] *Why We Need Data Protection Laws for AI in India*, Defacto L.J. (May 11, 2025), https://defactolawjournal.org/papers/why-we-need-data-protection-laws-for-ai-in-india/.
[7] *Id.*

a pressing matter of national security and protection of individual rights.[8].

Despite the introduction of legal measures such as the Information Technology Act of 2000, the Digital Personal Data Protection Act of 2023 and a range of regulatory directives across sectors, India's legislative and policy framework still remains fragmented, reactive, and often unable to keep up with the sheer pace of technological advances[9]. Legislative responses frequently lag behind industry practices and the pace of technological change, making it difficult to ensure robust governance[10]. Recent literature review highlights problems such as overlapping mandates, siloed interventions, and inconsistent enforcement all of which create space for exploitation, whether by malicious actors or by unchecked algorithmic systems[11]. The absence of comprehensive, AI-specific legislation also leaves unresolved key concerns related to transparency, accountability, and mechanisms for redress[12].

At the same time, while India is drawing lessons from comparative international frameworks, these efforts cannot be wholesale imports given the country's unique democratic, constitutional, and socio-cultural context. Borrowing without adaptation risks undermining constitutional protections, cultural pluralism, and the distinctive nature of digital life in India[13]. The central challenge lies not in adoption alone but in actual reform: creating a legal order that is strong enough to address digital harms while remaining innovative and flexible[14]. Regulatory responses must therefore balance openness with oversight, innovation with rights protection, and decentralized digital growth with mechanisms for accountability[15].

This paper argues that an administrative revolution in digital governance is necessary in India. However, the incremental steps taken to date - as important as they are, not enough for the developed world at a time of exponential artificial intelligence development, datafication, and increasing cyber threats. It will not change by incremental steps but rather the construction of something built into the legal order of an actor that is sensitive both to the promise and to the threat of the digital leviathan, and that is equally committed to legal principles designed to

[8] *A Constitutional Analysis of India's Response to Cyber Threats*, IJCRT (2024), https://ijcrt.org/papers/IJCRT2408768.pdf.
[9] *Global AI Governance Law and Policy: India*, IAPP (July 14, 2024), https://iapp.org/resources/article/global-ai-governance-india/.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*

assist it[16].

Data Privacy and Protection: Between Consent and Surveillance

The context of data privacy in India can be described as one of uneasy tension: between, on the one hand, constitutional guarantee of autonomy and dignity granted by the Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India; and on the otherhand a data regulation regime rife with loopholes for enforcement, regulatory uncertainty, state and commercial surveillances[17]. This section critically examines the development of Indian privacy jurisprudence post Puttuswamy, criticises the Digital Personal Data Protection Act, 2023 (DPDP), highlights the remaining regulation and enforcement vacuum and draws comparative observations in relation to the European Union's General Data Protection Regulation (GDPR)[18].

The *Puttaswamy* judgment in 2017 marks a watershed in Indian constitutional law, repositioning privacy as a fundamental right subsumed under Article 21 and linked to the values of autonomy, dignity, and informational self-determination[19]. The Court articulated privacy as multidimensional encompassing not just informational but also decisional and bodily privacy while establishing the now-canonical three-prong test: legality, legitimate state aim, and proportionality[20]. As subsequent rulings and legislative initiatives have shown, however, this robust constitutional pronouncement has struggled to find full realization in statutory and regulatory practice.

While *Puttaswamy* heralded a tectonic shift in Indian rights discourse, the gap between constitutional promise and practical enforcement has repeatedly been laid bare. In an age of algorithmic governance, high-profile leakages of Aadhaar database and continued requests for bulk collection of data for public distribution highlight the vulnerability of privacy to sophisticated surveillance infrastructure including CCTV, facial recognition, while the courts continued to pit privacy against welfare and national security. The DPDP Act, 2023 is India's

[16] *India's Advance on AI Regulation*, Carnegie Endowment for Int'l Peace (Nov. 20, 2024), https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en.
[17] K. Dubey & J. Singh, *The Right to Privacy in India: Evolution and Developments*, 7 IJFMR 1 (2025).
[18] *Analysis of the Digital Personal Data Protection Act - India*, TNP Consultants (Nov. 19, 2024), https://www.tnpconsultants.com/en/analysis-digital-personal-data-protection-act-indias-new-personal-data-protection-law/.
[19] Dubey & Singh, *supra* note 17.
[20] *Privacy as a Fundamental Right: Impact and Implementation After Puttaswamy*, IJLLR (Aug. 23, 2025), https://www.ijllr.com/post/privacy-as-a-fundamental-right-impact-and-implementation-after-puttaswamy.

first major attempt to codify the law for personal data protection and substitutes outdated provisions of Information Technology Act, 2007. Formulated after years of debate and in the wake of a phenomenon of increased datafication, the law draws extensively from international templates (more specifically, the European GDPR) in incorporating principles of purpose limitation, consent, data minimization, and security. On paper, the Act confers rights to access, correction, erasure, and grievance redressal, while retaining broad exceptions for state actors and "legitimate uses"[21].

However, a closer analysis reveals shortcomings that go beyond mere implementation delays. The Act's design significantly privileges governmental and business interests over individual autonomy exempting a wide swath of activities, including government processing on grounds of national security, disaster management, and other vaguely defined "legitimate uses"[22]. Consent is formally entrenched, but the Act allows personal data to be processed even without explicit consent in numerous scenarios, diluting the salience of informed, substantive choice[23]. Equally problematic is the Act's approach to cross-border data transfers: it adopts a default posture of permissiveness, relying on future government notifications to restrict flows, in sharp contrast with the GDPR's strict adequacy requirements[24].

Perhaps the greatest analytical concern, however, is the DPDP's enforcement architecture. The establishment of a Data Protection Board lacks the regulatory teeth and independence granted to European supervisory authorities; it possesses no explicit powers to issue binding guidelines or "soft law" and remains vulnerable to executive influence[25]. Duties imposed on data fiduciaries (controllers) are often diluted by pragmatic carve-outs for small entities, and obligations for data processors remain context-dependent and unclear[26]. The result, as argued in critical literature, is a law that is broad and imprecise, perpetually deferred to further rules and marked by weak enforceability[27].

Gaps in Enforcement, Cross-Border Data Flows, and State Surveillance

Despite the DPDP's formal recognition of data protection values, enforcement remains the

[21] TNP Consultants, *supra* note 18.
[22] TNP Consultants, *supra* note 18.
[23] TNP Consultants, *supra* note 18.
[24] TNP Consultants, *supra* note 18.
[25] TNP Consultants, *supra* note 18.
[26] TNP Consultants, *supra* note 18.
[27] TNP Consultants, *supra* note 18.

Achilles' heel of India's data regime. The architecture for redress and oversight is fragmented and lacks both technical capacity and institutional independence[28]. The Data Protection Board's mandate is hamstrung by absence of rule-making powers, meaning vital questions around standards for security, breach notification, or consent management are left unsettled[29]. Additionally, India's permission-based regime for cross-border data flows, combined with limited oversight, exposes personal data to global vectors of exploitation especially as sectoral regulators in banking and telecom continue to impose their own idiosyncratic rules[30].

The state's own role as a data collector and surveillant also raises acute concerns. While *Puttaswamy* mandates that privacy be balanced against legitimate state aims, expansive exemptions for security, public order, and "welfare" in the DPDP render the "proportionality" principle ineffectual in many instances[31]. Government access to telecommunications metadata, mass deployment of biometric systems, and the use of facial recognition panels in law enforcement all persist under inadequate oversight mechanisms; the state is, in effect, both protector and principal violator of privacy rights[32]. The Pegasus spyware controversy and recurring judicial challenges to surveillance laws highlight how foundational constitutional values continue to clash with executive convenience[33].

Comparative Insights: GDPR vs Indian Framework

A comparative lens exposes both the ambition and limitations of India's legislative turn. The GDPR, as gold standard, is rooted in robust rights-based approaches, strict accountability for controllers, extraterritorial application, and strong redress and enforcement through independent supervisory bodies[34]. The regulation mandates data processing based on clear lawful grounds, informed consent, and comprehensive protections for "special categories of data"[35]. It severely restricts cross-border flows to jurisdictions lacking "adequate" protections, strengthening individual agency and limiting government overreach[36].

[28] Dubey & Singh, *supra* note 17.
[29] TNP Consultants, *supra* note 18.
[30] TNP Consultants, *supra* note 18.
[31] Dubey & Singh, *supra* note 17.
[32] Dubey & Singh, *supra* note 17.
[33] Dubey & Singh, *supra* note 17.
[34] *Comparing GDPR and DPDPA: Data Protection Laws in EU and India*, SecurePrivacy (June 13, 2024), https://secureprivacy.ai/blog/comparing-gdpr-dpdpa-data-protection-laws-eu-india.
[35] *Id.*
[36] *Id.*

Against this, the DPDP appears more permissive and pragmatic, but at the cost of legal certainty and effective rights protection. Notable divergences include:

Scope and Exemptions: The DPDP covers digital (not analog) personal data, and provides sweeping exemptions for state and "legitimate uses," severely curtailing the real autonomy of data principals[37].

Consent and Rights: While DPDP models consent on GDPR lines, the proliferation of exceptions undermines the right to say no. Unlike the GDPR, which prescribes clear notice, withdrawal rights, and automated-decision safeguards, the DPDP omits any right not to be subject to solely automated decisions[38].

Enforcement and Sanctions: The GDPR's penalties up to 4% of global turnover are matched by the DPDP's fine regime, but the independence and resourcing of the Indian Data Protection Board remains suspect[39].

Cross-Border Data Flows: Where the GDPR requires adequacy findings, the DPDP waffles transfers are permitted unless explicitly restricted by the Indian government, increasing legal and practical uncertainty[40].

This comparative analysis signals that while India draws technical inspiration from global models, the adaptation is hobbled by political economy concerns and state-centric imperatives. The resulting framework is simultaneously overbroad, fragmented, and under-enforced a "patchwork" that privileges organizational convenience over transformative privacy safeguards.

The central challenge for India is neither technological nor merely legal: it is ultimately normative and institutional. As digital infrastructures deepen and state-corporate data linkages proliferate, the stakes of privacy especially for marginalized and rural population become existential. The persistence of asymmetries in awareness, access, and redress means that the promise of *Puttaswamy* risks becoming not transformative reality, but constitutional rhetoric,

[37] TNP Consultants, *supra* note 18.
[38] TNP Consultants, *supra* note 18.
[39] SecurePrivacy, *supra* note 34.
[40] TNP Consultants, *supra* note 18.

unless matched by structural reforms.

It is therefore imperative that India embrace a genuinely rights-based, cohesive data governance model: one that centers individual autonomy, mandates transparency and accountability, resists exceptionalist carve-outs, and empowers an independent, well-resourced regulatory agency. Absent such reform, the digital leviathan will continue to outpace the fragmented, reactive legal regime meant to contain it[41].

Regulating Artificial Intelligence: Law Lagging Behind Code

India's encounter with artificial intelligence is marked by a paradox: even as AI-driven systems reshape governance, policing, and finance with unprecedented scale and ambition, the country's legal and regulatory frameworks remain inherently reactive and piecemeal[42]. This section scrutinizes how the law lags behind code, interrogating real-world use cases, the lacunae of AI-specific regulation, the ethical complexities of rapid deployment, and competing models of governance, ultimately weighing the imperative of sectoral versus unified reforms.

AI in Governance, Policing, and Finance: Opportunity and Risk

Across the public and private sector, AI's adoption is both transformative and fraught. Indian governments deploy predictive analytics in traffic management, resource allocation for smart cities, automated legal research, and AI-assisted surveillance in crime prevention[43]. In law enforcement, facial recognition, predictive policing, and crime-mapping tools have proliferated, promising efficiency but risking profiling and overreach[44]. In finance, AI is used for credit scoring, fraud detection, risk assessment, and robo-advisory services, expanding access and accelerating decision cycles yet also amplifying concerns about discrimination, exclusion of marginalized borrowers, and the opacity of algorithmic decisions[45].

Empirical studies highlight that Indian fintech and banking have integrated biometric

[41] Dubey & Singh, *supra* note 17.
[42] *Legal Challenges of Artificial Intelligence in India's Cyber Law Framework*, 11 IJFMR 31347 (2024).
[43] Indian Institute of Public Administration, *AI in Governance: Risks and Challenges* (2025), https://www.iipa.org.in/GyanKOSH/posts/ai-in-governance-risks-and-challenges.
[44] PIB, *Integrating AI in India's Judiciary and Law Enforcement* (2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/feb/doc2025225508901.pdf.
[45] DSK Guha, B. Savage-Mansaray & N. Samanta, *The Present and Future of AI Usage in the Banking and Financial Decision-Making Processes within the Developing Indian Economy*, 2022 IJLT, https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1149&context=ijlt.

authentication, automated lending approvals, and AI-powered customer support, while government-backed initiatives use machine learning for welfare targeting and regulatory oversight[46]. However, public sector experiments with automated facial recognition led to wrongful arrests and social media monitoring in policing contexts, provoking legal and ethical concerns about due process, privacy, and the difficulty of challenging algorithmic authority[47]. Notably, the pace of technological embedding has not been matched by mechanisms for transparency or systemic accountability, often leaving affected parties without redress[48].

The Legal Vacuum: AI-Specific Legislation Still Elusive

Despite the visible proliferation of "AI in the wild," India's statutory architecture remains archaic. There is currently no legislation that specifically targets AI systems, their risks, or their unique regulatory needs[49]. The Information Technology Act 2000, drafted decades before the AI revolution, does not define or address autonomous decision-making, algorithmic accountability, or the legal status of non-human actors[50]. Liability frameworks civil, criminal, or contractual presume human intent and foreseeability, leaving open major questions: Who is responsible for harm when AI acts independently? How does the law address emergent and unforeseeable outcomes?[51]

The few AI-focused policy statements such as NITI Aayog's National Strategy for Artificial Intelligence and various sector-specific advisories lack binding legal force or detailed enforcement mechanisms[52]. While the Ministry of Electronics and Information Technology (MeitY) has issued guidance on transparency, fairness, and bias mitigation, these recommendations are voluntary and fragmented, frequently overridden by sectoral discretion or withdrawn after industry pushback[53]. As such, AI deployments in critical infrastructures or sensitive functions remain regulated, if at all, under general laws ill-suited to address their

[46] *Balancing Innovation and Investor Protection: A Study of Accessibility, Accountability, and Responsible Investing in Digital Era of India*, 7 IJFMR 48701 (2025).
[47] Indian Institute of Public Administration, *supra* note 43.
[48] *The Role of Artificial Intelligence in Driving ROI through Synergized HR, Marketing, and Financial Decision-Making*, 7 IJSSS 153 (2025).
[49] Lawful Legal, *The Legal Challenges of Artificial Intelligence in India* (2025), https://lawfullegal.in/the-legal-challenges-of-artificial-intelligence-in-india/.
[50] *Rethinking Legal Status and Responsibility for AI in India*, 7 IJLSSS 109 (2025).
[51] *Id.*
[52] Lawful Legal, *supra* note 49.
[53] Law Asia, *Call for Focused Approach to AI Regulation in India* (2025), https://law.asia/india-ai-regulation-focus-unified-approach/.

scale, complexity, or societal implications[54].

Ethical Dilemmas: Bias, Accountability, and Transparency

The rapid ascent of AI intensifies longstanding ethical and constitutional dilemmas that India's piecemeal governance has failed to meaningfully resolve. Bias in AI-driven decisions especially in policing, finance, and public benefits has led to automated reproductions of caste, gender, or religious inequities, sometimes even exacerbating patterns of structural discrimination[55]. Case studies repeatedly show how training data reflecting historical bias can result in systemic exclusion, wrongful denial of benefits, or algorithmic prejudice in hiring and lending decisions[56].

Accountability is further compromised by the "black box" nature of many AI systems: neither citizens nor regulators can easily trace how, why, or on what basis a given decision was made[57]. The Hyderabad facial recognition misidentification incident and misdiagnoses by health-sector AI systems illustrate how contested the lines of responsibility become when a mistake occurs[58]. Developers tend to deflect to users, public agencies invoke systemic complexity, and contracted AI vendors often remain shielded by ambiguous contractual terms[59].

Transparency and explainability central to the legitimacy of any AI regime remain aspirational under current Indian practice. There are no statutory requirements for algorithmic audits, clear notice, or user challenge rights, leaving fundamental principles of natural justice under protective[60].

Global Models: Lessons from the EU AI Act and OECD Principles

The normative and technical challenge of AI governance has prompted diverse international experimentation. The European Union's AI Act offers a risk-based framework: high-risk AI systems must meet stringent transparency, human oversight, and audit requirements, while

[54] *Id.*
[55] *Algorithmic Bias and Discrimination: Legal Accountability of AI Systems*, 7 IJIRMPS 232659 (2025).
[56] *Id.*
[57] Indian Institute of Public Administration, *supra* note 43.
[58] Indian Institute of Public Administration, *supra* note 43.
[59] IJIRMPS, *supra* note 55.
[60] Lawful Legal, *supra* note 49.

banned categories (such as social scoring) are clearly defined[61]. The Act mandates independent assessments, ongoing data governance, and substantial penalties for non-compliance, underscoring the EU's rights-driven regulatory philosophy[62].

In contrast, the OECD's AI Principles adopt a softer, principle-based approach: emphasizing inclusiveness, transparency, accountability, safety, and the rule of law, with governments and industry asked to align on voluntary standards and cross-border cooperation[63]. These standards foreground human rights and non-discrimination while promoting innovation and adaptability, yet ultimately rely on existing legal architectures for enforceability[64].

While both models address fairness, accountability, and transparency, their modes of operation diverge. The EU emphasizes binding obligations and regulatory supervision; the OECD stresses international harmonization, flexibility, and the layering of new norms atop established law[65].

Sectoral Versus Unified Regulation: The Indian Dilemma

The pressing question for India is whether to continue fragmenting AI regulation across disparate sectors (banking, telecom, healthcare, law enforcement), each with its own rules and enforcement cultures, or to formulate a unified, sovereign statute that centralizes oversight and creates consistent standards[66]. The current landscape is typified by sector-specific advisories from regulators like the RBI, SEBI, and TRAI, resulting in regulatory gaps, forum shopping, and business uncertainty[67].

Recent government reports and expert consultations increasingly argue for a unified or "whole-of-government" approach, recognizing that fragmented regulation risks both stifling innovation and overlooking systemic vulnerabilities[68]. A singular Digital India Act or AI Act could consolidate disparate authorities, set minimum standards for risk assessment, require

[61] OECD and EU, *OECD and EU Standards for Trustworthy AI* (2019), https://youaccel.com/lesson/oecd-and-eu-standards-for-trustworthy-ai/premium.
[62] OECD and EU, *supra* note 61.
[63] OECD and EU, *supra* note 61.
[64] OECD and EU, *supra* note 61.
[65] OECD and EU, *supra* note 61.
[66] Law Asia, *supra* note 53.
[67] *Id.*
[68] AZB Partners, *Update on MeitY's Report on AI Governance Guidelines* (2025), https://www.azbpartners.com/bank/update-on-meitys-report-on-ai-governance-guidelines-development/.

algorithmic audits, mandate data and impact transparency, and provide uniform avenues for redress[69]. However, concerns persist: uniform law may lead to regulatory inertia, overbreadth, and inadequately address sectoral nuances[70].

The dynamic consensus emerging is in favor of a hybrid regulatory framework sector-specific guidelines underpinned by a general AI law that foregrounds constitutional values, establishes a central AI authority, and ensures adaptability as technology evolves[71].

Cybercrime and National Security: Law vs Digital Anarchy

The exponential growth of India's digital ecosystem, while catalyzing economic and social resilience, has also opened avenues for complex cyberattacks, ransomware proliferation, and digital fraud challenges that expose critical vulnerabilities in the nation's legal and security infrastructure[72]. This section of the paper interrogates cybercrime's rise, assesses the strengths and gaps in the Information Technology (IT) Act, examines the operational realities of CERT-In, NCIIPC, and law enforcement, and explores urgent reform priorities for jurisdiction, evidence, and comprehensive codification.

The Surge of Cyberattacks, Ransomware, and Digital Fraud

Over the last decade, India has experienced an unprecedented surge in cybercrime incidents including ransomware attacks crippling hospitals, digital banking fraud, identity theft, data breaches, and phishing campaigns targeting individuals and critical infrastructure[73]. The rapid proliferation of digital onboarding, the penetration of e-governance platforms, and the shift to cashless payments have created lucrative targets for cybercriminals: according to recent national surveys, cybercrime in India has grown at double-digit rates, with attacks such as ransomware and social engineering dramatically increasing in frequency and financial impact[74]. The cybersecurity response is complicated further by organized crime networks, cross-border actors, and the emergence of sophisticated tactics like deepfakes and zero-day exploits[75].

[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] H. Choudhary & T. Agarwal, *Cyber Law in India: Evolution & Current Limitations* (2025), IJRPR144.
[73] *A Comprehensive Survey of Cybercrimes in India Over the Last Decade* (2024), IJSRA119.
[74] *A Study on Cyber Frauds Post Digitalization in India* (2024), IJRASET148.
[75] *Securing India in the Cyber Era* (2022), Strategic Analysis122.

Despite efforts to raise cyber awareness and promote best practices, vulnerabilities persist through outdated software, poor cyber hygiene, and lack of incident reporting factors exacerbated by rapid digitalization and uneven regulatory compliance[76]. The resulting "digital anarchy" is not merely the product of technical deficiencies, but also of regulatory inertia, resource constraints, and fragmented legal authority[77].

IT Act Provisions: Strengths and Persistent Limitations

India's primary statutory response the Information Technology Act, 2000 (as amended) provides the core legal framework for offenses such as unauthorized computer access, hacking, data theft, cyberterrorism, digital fraud, and publication of obscene material[78]. Sections 65–67 and 66D address a range of cybercrimes, while Section 70B establishes CERT-In as the national incident response authority[79].

However, critical limitations undermine the IT Act's effectiveness in the contemporary threat landscape. The Act was conceived before the explosion of ransomware, social media abuse, cloud computing, and internationalized cyberthreats, rendering many provisions outmoded or ambiguous[80]. Notably:

> The IT Act's definition of cyber offenses is narrow, often failing to capture new iterations of fraud, extortion, and digital harassment[81].
>
> Investigation and prosecution are hampered by procedural lacunae especially regarding rapid evidence preservation, digital forensics standards, and coordinated multi-agency action[82].
>
> Critical issues of data protection, victim compensation, coopting international law enforcement, and corporate obligations are largely unaddressed or only weakly codified[83].

[76] Gupta & Mehta, *An Analytical Study on Challenges and Gaps in India's Cyber Security Framework* (2020), CLJ141.
[77] *Id.*
[78] Sattrix, *Cyber Law in India: A Comprehensive Guide To Key Regulations* (2025)152
[79] *CERT-In: India's Cybersecurity Response Framework Explained* (2024), IndiaLaw150.
[80] Choudhary & Agarwal, *supra* note 72.
[81] Choudhary & Agarwal, *supra* note 72.
[82] Choudhary & Agarwal, *supra* note 72.
[83] Choudhary & Agarwal, *supra* note 72.

Judicial and academic analysis point to the growing gap between the Act's legislative intent and evolving cyber realities, advocating for stronger data protection, clearer jurisdictional norms, and more specialized enforcement mechanisms[84].

Institutional Roles: CERT-In, NCIIPC, and Law Enforcement

India's cyber defense infrastructure is multi-layered but often diffuse. The Computer Emergency Response Team of India (CERT-In), constituted under Section 70B of the IT Act, is central to incident management, threat notification, and national cyber risk mitigation[85]. CERT-In coordinates with the National Critical Information Infrastructure Protection Centre (NCIIPC), which focuses on safeguarding "critical information infrastructure," and works closely with law enforcement, state agencies, and sectoral Computer Security Incident Response Teams (CSIRTs)[86].

CERT-In's rapid advisories and mandatory breach reporting within six hours of detection signify progress. Yet, as recent analyses reveal, the effectiveness of CERT-In and NCIIPC is circumscribed by:

Overlaps and unclear mandates dividing responsibility across sectoral lines[87].

Limited resources for digital forensics, real-time coordination, and capacity building outside metropolitan centers[88].

Law enforcement's lack of technical training, outdated investigative tools, and limited cyber-literacy, which delays response times and hampers prosecution[89].

The upshot is a patchwork response to major incidents: while CERT-In may swiftly alert entities or issue advisories, actual investigation and disruption of criminal networks rely on police and the judiciary, often with variable competence and outcomes[90].

[84] Choudhary & Agarwal, *supra* note 72.
[85] IndiaLaw, CERT-In, *supra* note 79.
[86] *Mapping India's Cybersecurity Administration in 2025* (2025), Carnegie Endowment145.
[87] *Id.*
[88] Choudhary & Agarwal, *supra* note 72.
[89] Choudhary & Agarwal, *supra* note 72.
[90] IndiaLaw, CERT-In, *supra* note 79.

Challenges: Attribution, Jurisdiction, and Evidence Collection

Cybercrime's transnational and anonymized nature presents formidable hurdles for attribution, jurisdiction, and evidence gathering. While Section 75 of the IT Act expands Indian jurisdiction to crimes with a "substantial connection" to domestic systems, practitioners and courts routinely confront obstacles:

> Attribution of attacks is complicated by proxy servers, anonymizing technologies, and the ease of obfuscating origins[91].
>
> Multiple jurisdictional claims from local to international create forum shopping risks procedural delays[92].
>
> Evidence collection is hobbled by inadequate digital forensics infrastructure, inconsistent preservation protocols, and limited law enforcement coordination with private service providers[93].

Indian courts may invoke the "effects doctrine" to assert jurisdiction for cybercrimes impacting domestic victims, but practical enforcement remains difficult when suspects and data reside abroad, and when mutual legal assistance treaties are slow to operationalize[94].

Toward a Comprehensive Cybercrime Code?

These challenges have led to growing scholarly and policy consensus that piecemeal amendment of the IT Act is no longer sufficient; instead, India must pursue a comprehensive cybercrime code[95]. Such a code would clarify definitions, incorporate global best practices on procedures, provide harmonized standards for digital evidence, address overlapping regulatory authorities, and reflect the real-time and borderless nature of digital harm[96].

A modern code should:

> Expand definitions to encompass emerging crimes like ransomware, deepfakes, IoT-

[91] The Law Institute, *General Jurisdiction Principles for Cyber Crimes* (2025)146.
[92] *Id.*
[93] Choudhary & Agarwal, *supra* note 72.
[94] The Law Institute, *supra* note 91.
[95] Choudhary & Agarwal, *supra* note 72.
[96] Choudhary & Agarwal, *supra* note 72.

based attacks, and AI-generated fraud[97].

Impose robust and graduated obligations on both public and private entities for reporting, response, and transparency[98].

Create specialized cybercrime units, properly trained in forensics and cross-border collaboration[99].

Establish victim-friendly mechanisms, including compensation funds and accessible grievance redress[100].

Absent such reform, the disconnect between India's vibrant digital economy and its fragmented legal framework will only widen, threatening both national security and individual rights in the face of digital anarchy[101].

Regulatory Reform and Institutional Architecture

The rapid digital transformation in India, characterized by complex technological innovations and a widening governance scope, has revealed significant **fragmentation across ministries and regulatory bodies**. Ministries such as the Ministry of Electronics and Information Technology (MeitY), the Reserve Bank of India (RBI), and the Telecom Regulatory Authority of India (TRAI) operate with overlapping and sometimes conflicting mandates in regulating areas like data protection, digital payments, telecommunications, and emerging technologies[102]. This section analyses the challenges stemming from such fragmentation, evaluates proposals for unified governance structures such as a Digital Law Commission or AI Ethics Board, explores the judiciary's evolving role in digital rights protection, and examines the significance and obstacles of public-private partnerships and stakeholder engagement in regulatory reform.

Fragmentation Across Ministries and Regulators

India's digital governance landscape is marked by siloed regulatory regimes operating under

[97] Choudhary & Agarwal, *supra* note 72.
[98] Carnegie Endowment, *supra* note 86.
[99] Carnegie Endowment, *supra* note 86.
[100] Choudhary & Agarwal, *supra* note 72.
[101] Gupta & Mehta, *supra* note 76.
[102] *Fragmentation and Overlap in India's Digital Regulatory Framework*, 2025 IJFMR 2917.

distinct ministries MeitY overseeing IT and digital policy, RBI governing digital payments and financial technology, and TRAI regulating the telecom sector. While specialization enables domain specific expertise, at the same time it is creating jurisdictional overlaps, policy incoherence, and regulatory arbitrage[103]. For instance, issues surrounding data localization, cross-border data flow, and AI deployment witness inconsistent stances, with RBI's caution on financial data security at odds with MeitY's liberal approach towards innovation and data sharing[104].

Such fragmentation undermines the harmonization of standards and complicates enforcement, leaving businesses unclear about compliance and citizens vulnerable to regulatory gaps[105]. The disconnected oversight often slows decision-making in addressing rapidly evolving digital risks while diluting accountability when overlapping authorities pass responsibility[106]. This complexity is evident in cross-sectoral challenges such as AI ethics, cybersecurity breaches, and consumer protection in digital markets, where the limits of coordination are exposed[107].

Proposal for a Unified Digital Law Commission or AI Ethics Board

Recognizing these fissures, several academic and policy commentators have proposed the creation of a **unified institutional framework** a Digital Law Commission or a dedicated AI Ethics Board that would centralize and rationalize governance across digital domains[108]. Such a body would ideally consolidate legislation, draft comprehensive frameworks, arbitrate overlapping regulatory conflicts, and oversee ethical standards in digital technology deployment[109].

A Digital Law Commission could function as a high-powered, multi-stakeholder agency integrating expertise from technologists, ethicists, legal scholars, and civil society to ensure cohesive policy coherence, timely law reform, and technology-sensitive governance[110]. Similarly, an AI Ethics Board could serve as an independent regulator with the mandate to enforce transparency, algorithmic fairness, and accountability, including issuing binding ethical

[103] *Id*
[104] *Balancing Innovation and Investor Protection: A Study of Accessibility, Accountability, and Responsible Investing in Digital Era of India*, 7 IJFMR 48701 (2025).
[105] IJFMR, *supra* note 102.
[106] *Id.*
[107] *Legal Challenges of Artificial Intelligence in India's Cyber Law Framework*, *supra* note 42.
[108] AZB Partners, *supra* note 68.
[109] *Id.*
[110] *Id.*

guidelines for AI systems used by both government and private sectors[111].

Critically, the design of such bodies should balance independence shielding them from political pressures and industry capture with mechanisms for democratic participation and accountability[112]. There is also a risk that centralization curtails innovation agility or stifles sectoral nuances, underscoring the need for adaptable governance models that can evolve alongside technology[113]. Effective institutional reform thus requires a nuanced approach rather than blunt centralization.

Role of the Judiciary in Digital Rights Protection

Parallel to regulatory institutions, the **judiciary in India has assumed a pivotal role** in shaping digital rights protection, often stepping in to fill legislative vacuum or enforcement inertia[114]. Landmark judgments like *K.S. Puttaswamy* have elevated privacy to a fundamental right, obliging courts to interpret digital governance in ways that safeguard individual dignity and autonomy[115].

Courts have increasingly engaged with issues related to surveillance, data protection, freedom of expression online, and the right to access digital services, thereby acting as critical arbiters where regulatory gaps persist[116]. Judicial activism has sometimes pressured executive agencies to reveal criteria for algorithmic decision-making or challenged the constitutionality of mass data collection initiatives[117].

However, judicial intervention also faces limits technical complexity, slow procedural mechanisms, and the reactive nature of litigation restrict its transformative potential[118]. There is a growing consensus that courts should supplement, not substitute, robust institutional frameworks that proactively regulate digital ecosystems[119].

[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] Dubey & Singh, *supra* note 17.
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.*

Public-Private Partnerships and Stakeholder Consultations

Recognizing the multifaceted challenges of regulating digital technologies, Indian policymakers increasingly emphasize **collaborative governance models** involving public-private partnerships (PPPs) and broad stakeholder consultations[120]. The technology sector's fast pace, globalized supply chains, and technical specialization necessitate dialogue between government, industry leaders, academia, and civil society[121].

Such consultative processes aim to build legitimacy, align incentives, and leverage expertise, as seen in the formulation of the Digital Personal Data Protection Rules or MeitY's AI governance guidelines[122]. PPPs can also foster capacity building, such as joint cybersecurity exercises, digital literacy campaigns, and innovation hubs supporting ethical AI development[123].

Nonetheless, power asymmetries between state actors and large technology firms risk undermining democratic accountability and public interest safeguards[124]. Without transparency in consultation processes or balanced stakeholder representation, regulatory capture and co-optation remain acute threats[125].

Broader Implications and the Way Forward

India's digital governance landscape confronts the dual imperative of **harmonization and pluralism**—creating unified, stable legal frameworks while accommodating diverse sectoral needs and rapid technological advances[126]. Institutional reform must clarify mandates, enhance coordination, and empower bodies with technical expertise and enforcement capabilities[127].

The proposal for a Digital Law Commission or AI Ethics Board, while promising in concept, must integrate mechanisms for adaptive, participatory governance, balancing independence with inclusiveness[128]. Judicial oversight will continue to play an indispensable role in

[120] *Digital Personal Data Protection Rules, 2025* (MeitY draft) (2025).
[121] AZB Partners, *supra* note 68.
[122] *DPDP Act and Consultation Mechanisms* (TNP Consultants, 2025).
[123] AZB Partners, *supra* note 68.
[124] *Id.*
[125] *Id.*
[126] IJFMR, *supra* note 102.
[127] *Id.*
[128] AZB Partners, *supra* note 68.

safeguarding constitutional values amid digital transformation[129]. Moreover, fostering respectful and transparent public-private dialogues is vital to ensure regulatory legitimacy and innovation-friendly policy[130].

Ultimately, India's challenge is to architect institutions capable of **regulating the digital leviathan** complex, dynamic, and socio-politically embedded while upholding the constitutional vision of liberty, equality, and justice in the digital age[131].

Conclusion: Towards a Rights-Based, Innovation-Friendly Legal Ecosystem

This paper has foregrounded the manifold challenges India faces in regulating its rapidly evolving digital landscape. From intergovernmental gaps and siloed governance (regulations sector by sector) to a legal vacuum around emerging technologies such as AI, the problems are systemic and not stand-alone. Although Puttaswamy affirmed the right to privacy for the first time as a constitutional right in India, this right is not equal and it remains prone to government surveillance and patchy enforcement. Conversely, when it comes to artificial intelligence, the law has been slower to catch up with rapid technological change. Ethical issues such as bias in algorithms, lack of transparency, and questions of accountability are already visible, but the statutes meant to govern them remain underdeveloped. At the same time, the sharp rise in cybercrime exposes the weaknesses of outdated legislation and the difficulty of coordinating across fragmented institutions, which often delays timely investigations. In this situation, the most constructive step forward lies in reforming existing frameworks and streamlining regulatory bodies so that the protection of constitutional rights does not come at the cost of stifling innovation. The challenge for India's legal system is to hold together three objectives that are often in tension promoting technological progress, safeguarding national security, and upholding individual rights. Striking this balance requires clear and principled regulatory measures that are guided by foresight rather than short-term reactions. One promising approach is to design flexible, forward-looking mechanisms such as regulatory sandboxes, which enable new technologies to be tested in a controlled environment while ensuring oversight. These tools, paired with inclusive governance that brings together state institutions, industry, and civil

[129] Dubey & Singh, *supra* note 17.
[130] AZB Partners, *supra* note 68.
[131] IJFMR, *supra* note 102.

society, can better prepare India for the digital risks that lie ahead[132].

The path forward must begin with **a rights-based approach** that anchors digital regulation firmly in constitutional guarantees: privacy, freedom of expression, due process and equality before the law. This foundation requires reforms that clearly define institutional roles, bring together fragmented regulators under a unified body such as a Digital Law Commission or an AI Ethics Board, and establish independent oversight with the authority to ensure fairness and transparency across different sectors[133]. Judicial bodies have an important role in responding to rapid technological change by interpreting rights in an adaptive manner; however, the courts alone cannot replace the need for strong legislation and well-functioning regulatory institutions[134].

It is equally important to embrace a mindset that supports innovation while encouraging responsible experimentation and open dialogue. Collaboration through public–private partnerships, along with wide-ranging stakeholder consultations, helps ensure that regulation gains legitimacy and remains rooted in practical realities, while also guarding against excessive influence from industry interests[135]. Flexibility through anticipatory, evidence-based regulation can accelerate beneficial technological diffusion while staying vigilant against emerging risks[136].

Ultimately, India's digital governance challenge is one of foresight and integration: developing **legal architectures capable of governing complex, dynamic technologies in a pluralistic democracy**. This requires investment in technical capacity, coherent policy design, transparent yet agile regulatory frameworks, and participatory governance mechanisms that systematically incorporate social values alongside economic imperatives[137].

Only by embracing these approaches the simultaneous pursuit of constitutional rights, innovation facilitation, and anticipatory regulation can India hope to tame the digital leviathan it has unleashed. The future of its democracy, economy, and citizens' fundamental freedoms

[132] OECD, *Framework for Anticipatory Governance of Emerging Technologies* (2024), https://www.oecd.org/en/publications/framework-for-anticipatory-governance-of-emerging-technologies_0248ead5-en.html.
[133] *Legal Challenges of Artificial Intelligence in India's Cyber Law Framework*, *supra* note 42.
[134] K. Dubey & J. Singh, *The Right to Privacy in India: Evolution and Developments*, 7 IJFMR 42002 (2025).
[135] AZB Partners, *supra* note 68.
[136] OECD, *supra* note 132.
[137] *Fragmentation and Overlap in India's Digital Regulatory Framework*, *supra* note 102

depend on legal reforms that are as forward-thinking as the technologies they aim to regulate[138].

[138] IJFMR, *supra* note 102.