



Cybercrime and data privacy in India: Legal challenges and regulatory framework

Aarav Sharma

Department of Law, University of Delhi, New Delhi, India

Abstract

India's rapid digitalisation has been accompanied by a steep rise in cybercrime and growing exposure of personal data, while the legal response remains divided between an ageing criminal-law framework and a newly operationalised data protection statute. This paper examines how the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023 jointly address offences against digital systems and the protection of personal information. Drawing on scholarly and professional literature published mainly between 2023 and 2026, it reviews the constitutional basis of privacy, the structure of cybercrime regulation, and the design of the new data protection regime. The evidence indicates that recorded cybercrime has expanded considerably, whereas convictions, investigative capacity, and cross-border cooperation have not kept pace. The data protection framework is a notable advance, yet commentators criticise its wide state exemptions, the absence of a separate category for sensitive data, and its limited response to algorithmic harms. Because its core duties take effect only in 2027, its real-world effectiveness cannot yet be measured. The paper concludes that coordinated reform, stronger institutional capacity, and independent oversight are needed to reconcile security and privacy objectives.

Keywords: Cybercrime, data privacy, Information Technology Act, Digital Personal Data Protection Act, India, regulatory framework

Introduction

India is now among the most digitally connected societies in the world. Digital payments, online public services, social media, and cloud-based commerce have moved large volumes of personal information into the hands of both state agencies and private firms. This expansion has created economic opportunity, but it has also widened the surface available to fraudsters, hackers, and other offenders, and it has made personal data a valuable and frequently targeted resource. Commentators link the growth of digital governance, fintech, cloud services, and artificial intelligence to heightened risks of identity theft, surveillance, data breaches, and misuse of information (Kalyan & Singh, n.d.).

For two decades the principal legal response was the Information Technology Act, 2000^[8] (IT Act), supplemented by the Indian Penal Code and, since 2024, the Bharatiya Nyaya Sanhita, 2023^[3] (BNS). Privacy, by contrast, had no dedicated statute until Parliament enacted the Digital Personal Data Protection Act, 2023^[4] (DPDP Act), which was operationalised through the DPDP Rules, 2025^[2]. Cybercrime control and data protection are therefore regulated by different instruments, administered by different bodies, and driven by different policy priorities. This paper asks three questions. What legal and regulatory structures currently govern cybercrime and data privacy in India? What does recent literature reveal about how well these structures work? And what obstacles stand in the way of effective implementation? The argument developed here is that India has built the formal architecture of a modern regime but still faces substantial gaps in enforcement capacity, legislative precision, and accountability of the state itself.

Review Approach

This study is a narrative, doctrinal review rather than a systematic review or meta-analysis. In October 2026^[12],

targeted keyword searches were carried out on publicly accessible journal pages, university repositories, a preprint server, and professional legal commentary. Search terms combined phrases such as cybercrime in India, Information Technology Act enforcement, Digital Personal Data Protection Act, and DPDP Rules. Priority was given to material from 2023 to 2026^[4, 12], and foundational statutes and Supreme Court decisions were added where the argument required them.

Sources were retained when they offered an analysis of the legal framework, empirical indicators of cybercrime, or an evaluation of the data protection regime. Law-firm briefings and press reports were used only to confirm dates, timelines, and statutory mechanics, not to support evaluative claims. Several recent articles are pre-publication or lack full bibliographic details, and the review is limited to what could be accessed openly. All findings are paraphrased, and readers should verify each source before relying on it.

Regulatory Framework and Major Approaches

1. Constitutional foundations of privacy

The modern Indian approach to privacy rests on the Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)^[9], which recognised privacy as a fundamental right protected under Article 21 of the Constitution. Scholars describe the DPDP Act as a statutory expression of that judgment, an attempt to reconcile individual autonomy with the state's interest in governance and with commercial demand for data (Nath, n.d.). The Court's earlier ruling in Shreya Singhal v. Union of India (2015)^[14], which struck down Section 66A of the IT Act for vagueness, remains a reference point for how speech-related cyber offences must be drafted.

2. Cybercrime regulation: the IT Act and the BNS

The IT Act, strengthened by the 2008 amendment, remains the core instrument. It penalises unauthorised access to

computer systems, identity theft, cheating by personation using computer resources, and the transmission of obscene material, and it supports the work of the Computer Emergency Response Team (CERT-In), which issues security advisories and receives incident reports. Overlapping offences such as cheating, extortion, and forgery are prosecuted under the BNS, so a single online fraud may engage provisions from both statutes. Naren and Gupta (2026)^[12], writing on the Act's twenty-fifth year, credit India with being an early legislator on digital offences in the Global South but point to vague definitions, low conviction rates, and the lack of tailored provisions for AI-enabled crime.

3. The DPDP Act and Rules

The DPDP Act introduces a consent-centred model built around data principals (individuals) and data fiduciaries (entities that decide how data is processed). It protects data in digital form, or data digitised from other formats, which is narrower than the European Union's General Data Protection Regulation (Hogan Lovells, 2025)^[2]. Analysts note that it treats all personal data alike and has no separate sensitive-data category (Naithani, 2024; Nath, n.d.). The Act also creates the Data Protection Board of India and allows penalties of up to INR 250 crore per breach (Deccan Herald, 2025)^[5].

The Rules were notified in November 2025^[2] and are being phased in over roughly eighteen months. They set out the content of notices, the registration of consent managers, verifiable parental consent for children's data, breach reporting duties, data erasure timelines, and conditions for cross-border transfers (AZB & Partners, 2025)^[2]. Until the phased rollout is complete, the older rules under Section 43A of the IT Act continue to apply (Hogan Lovells, 2025).

Evidence on Effectiveness

The available evidence is stronger on the scale of cybercrime than on the performance of the law. A recent survey of cybercrime in India over the past decade reports that registered cases under the IT Act rose from 9,622 in 2014 to 77,858 in the first eight months of 2024, while arrests increased from 5,752 to 36,235 over the same period ("A Comprehensive Survey," 2025). These figures show growing detection and reporting, but they also illustrate that rising arrests do not automatically translate into successful prosecutions. Naren and Gupta (2026)^[12] specifically identify low conviction rates as a structural weakness.

Evidence on the data protection regime is necessarily prospective. Because the substantive duties of the DPDP Act begin to apply only in 2027, no study can yet measure compliance levels, penalty outcomes, or the experience of data principals. What exists instead is doctrinal evaluation. Naithani (2024) compares the Act with the EU framework and the proposed American Privacy Rights Act and concludes that some provisions, particularly those on exemptions, consent, and erasure, require careful interpretation if individuals are to gain real control over their data. A 2026 critique in the *Global Privacy Law Review* argues that broad exemptions, thin transparency and accountability measures, and the omission of core processing principles weaken the protection offered ("Data, Control, and Power," 2026).

Taken together, the literature supports a cautious reading: India has expanded both its legal tools and its institutions,

but there is little reliable evidence yet that either has reduced harm or improved outcomes for victims.

Barriers and Challenges to Implementation

Several recurring obstacles emerge from the literature. The first is legislative clarity. Ambiguous or outdated terms in the IT Act complicate interpretation, and the statute struggles to address crypto-assets and AI-driven offences (Naren & Gupta, 2026)^[12]. The overlap between the IT Act and the BNS further raises the risk of inconsistent charging decisions.

The second is capacity. Cybercrime investigations demand technical skills, forensic tools, and fast access to platform data, yet commentators describe law enforcement capacity as still developing and uneven across states. Digital evidence rules and the cross-border nature of many offences add delay, since requests for foreign data often depend on slow mutual legal assistance procedures. Naren and Gupta (2026)^[12] therefore place India's framework alongside the Budapest Convention and the new United Nations cybercrime treaty, suggesting that closer harmonisation with multilateral instruments could ease evidence sharing and joint investigation.

The third challenge concerns state power. Critics argue that the DPDP Act allows the government to exempt notified agencies from its obligations on grounds such as security and public order, with limited independent oversight, and that the Data Protection Board is constituted by the executive, which may compromise its independence ("Data, Control, and Power," 2026; Nath, n.d.). Reviewers also note the lack of heightened protection for sensitive data and the limited treatment of automated decision-making and profiling.

Finally, there are practical transition issues. Organisations must redesign consent notices, security safeguards, and breach-response systems within a fixed window, and smaller firms may find this costly. Public awareness among data principals is also low, which limits the practical use of rights such as access, correction, and erasure (Kalyan & Singh, n.d.).

Discussion and Implications

The reviewed literature suggests that India's difficulty lies less in the absence of law than in the fit between law, institutions, and technology. The IT Act was drafted for a different internet, and its patchwork of amendments sits alongside new criminal provisions and a new privacy statute. A coherent reform strategy would clarify definitions, align overlapping offences, and introduce provisions that address AI-enabled fraud and deepfake abuse, as Naren and Gupta (2026)^[12] propose.

For data protection, the central policy question is whether the state will be held to standards comparable to those imposed on private actors. Narrowing exemptions, requiring proportionality and independent review when they are invoked, and strengthening the autonomy of the Data Protection Board would go some way towards this. Reintroducing a sensitive-data category and regulating automated decision-making, as suggested by Nath (n.d.), would also close notable gaps.

Operationally, investment in digital forensics, specialised training for police and judges, and faster international cooperation would improve conviction prospects. Firms should treat the eighteen-month phase-in as a period to build

genuine security and consent practices, not merely paperwork. Future research should assess enforcement outcomes once the Board begins issuing decisions, and should use empirical data on conviction rates and victim experience rather than relying only on doctrinal analysis. Policymakers should also communicate the new rights in plain language, since a regime that individuals cannot understand or invoke will deliver little protection, however carefully it is drafted.

Conclusion

India has moved from a single, general-purpose cyber statute to a layered framework that combines criminal law, sectoral regulation, and a comprehensive data protection law. This is a meaningful step, and the DPDP Rules give the new regime an operational timetable. Yet the literature consistently points to unresolved concerns: vague offence definitions, low conviction rates, uneven investigative capacity, broad exemptions for the state, and limited attention to AI-driven risks.

Whether the framework protects people in practice will depend on how it is implemented after 2027. Clear drafting, independent enforcement, and sustained institutional investment will determine if India can secure its digital economy while keeping privacy a genuine right and not just a statutory promise.

References

1. A comprehensive survey of cybercrimes in India over the last decade. arXiv,2025. <https://arxiv.org/pdf/2505.23770>
2. AZB & Partners. Digital Personal Data Protection Rules, 2025 notified, enforcement timelines announced. AZB & Partners,2025. <https://www.azbpartners.com/pub/update-indias-digital-personal-data-protection-framework-comes-into-effect/>
3. Bharatiya Nyaya Sanhita, 2023 (India).
4. Data, control, and power, decoding India's Digital Personal Data Protection Act, 2023. Global Privacy Law Review,2026:6(4). <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/6.4/GPLR2026002>
5. Deccan Herald. Centre notifies DPDP Rules, implementation planned in phases spread over 12–18 months. Deccan Herald,2025. <https://www.deccanherald.com/amp/story/india%2Fcentre-notifies-dpdp-rules-implementation-planned-in-phases-spread-over-12-18-months-3798465>
6. Digital Personal Data Protection Act, 2023 (No. 22 of 2023) (India).
7. Hogan Lovells. India's Digital Personal Data Protection Act 2023 brought into force. Hogan Lovells,2025. <https://www.hoganlovells.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force->
8. Information Technology Act, 2000 (No. 21 of 2000) (India).
9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
10. Kalyan S, Singh RD. Digital personal data protection in India, a critical analysis of Digital Personal Data Protection Act, 2023 in age of artificial intelligence and digital governance. Indian Journal of Law and Legal Research,n.d. <https://www.ijllr.com/post/digital-personal-data-protection-in-india-a-critical-analysis-of-digital-personal-data-protection-a>
11. Naithani P. Analysis of India's Digital Personal Data Protection Act, 2023. International Journal of Law and Management,2024. <https://doi.org/10.1108/IJLMA-05-2024-0174>
12. Naren N, Gupta K. Rethinking India's cybercrime law, from Information Technology Act to emerging threats in a global context. International Review of Law, Computers & Technology,2026.
13. Nath S. An analysis of the Digital Personal Data Protection Act 2023. Christ University Law Journal,n.d.:15(1):93–120. <https://doi.org/10.12728/culj.28.5>
14. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).