International Journal of Modern Engineering and Management | IJMEM
ISSN No: 3048-8230
Volume 3 Issue 3 March- 2026

Critical Analysis of the Information Technology Act 2000, Its Amendments, and the Emerging Digital Personal Data Protection Act 2023 in the Context of Global Regulatory Benchmarks

Malathi Sundaram Iyer[1], Krishnaswamy Venugopalan[2], Shirin Fatima Ansari[3], Rohit Desai Shettigar[4]

[1,2]*Department of Law, Vivekananda College of Law, Bengaluru, Karnataka, India*

[3,4]*Department of Criminology and Forensic Science, Karnatak University Dharwad (PG Department), Dharwad, Karnataka, India*

Abstract

The rapid digitization of India's economy and society has generated a correspondingly rapid proliferation of cybercrime—encompassing financial fraud, data breaches, online harassment, ransomware, and state-sponsored intrusions—that has severely strained legal frameworks designed for the early 2000s digital environment. India's primary legal framework, the Information Technology Act 2000 (ITA 2000) and its 2008 Amendment, was enacted before smartphones, social media, cloud computing, and cryptocurrency existed at meaningful scale, and has been subjected to sustained scholarly criticism for definitional inadequacies, evidentiary challenges, and constitutional tensions with fundamental rights guarantees. This article conducts a comprehensive doctrinal and comparative analysis of India's cybercrime legal framework from the ITA 2000 through the Digital Personal Data Protection Act 2023 (DPDPA 2023), the IT Rules 2021, and relevant Supreme Court jurisprudence, evaluating India's framework against the Budapest Convention, GDPR, and CFAA benchmarks. While DPDPA 2023 represents a significant advance in data protection governance, the article identifies important limitations including absence of data portability rights, weak accountability for government data processing, and concerns about enforcement body independence, and proposes five legislative and institutional reform priorities.

Keywords: *cybercrime legislation, Information Technology Act 2000, Digital Personal Data Protection Act 2023, GDPR, Budapest Convention, data protection, India, cyber law reform, intermediary liability, privacy rights, data fiduciary, cybersecurity governance*

1. Introduction

The digitization of India has been among the most spectacular socioeconomic transformations of the twenty-first century. From approximately 22 million internet users in 2000, India's internet population surpassed 900 million in 2024. Mobile payment transactions through UPI exceeded 13.89 billion in December 2024 with aggregate monthly value surpassing INR 23 trillion. This extraordinary transformation has created immense value alongside an expanded attack surface for cybercriminal exploitation. India's National Cybercrime Reporting Portal received over 1.56 million complaints in 2023, a 113% increase over 2021, with the Union Home Ministry's I4C estimating losses of approximately INR 1.8 trillion to cybercrimes in 2023.

Against this backdrop, the adequacy of India's legal framework for cybercrime prevention, investigation, prosecution, and victim redressal has become a matter of urgent public policy concern. The ITA 2000 struggles analytically and practically with the vastly more complex threat landscape of 2024: AI-generated deepfake fraud, cryptocurrency ransomware, platform-mediated incitement to violence, state-sponsored advanced persistent threats (APTs), and the systematic exploitation of AI tools for cybercrime at industrial scale.

2. The ITA 2000: Foundations and Critical Limitations

2.1 Evolution of India's Cyber Law Framework

Figure 1 presents the evolutionary timeline of India's cybercrime legislation from ITA 2000 through DPDPA 2023, with key provisions and identified gaps at each stage. The ITA 2000 was enacted primarily to give legal recognition to electronic transactions and digital signatures rather than comprehensively regulating cybercrimes. Chapter IX (Ss. 43–47) and Chapter XI (Ss. 65–78) constitute the principal cybercrime provisions. Section 66A—subsequently struck down in Shreya Singhal v. Union of India (2015)—was found unconstitutionally vague. The 2008 Amendment added identity theft (S.66C), impersonation (S.66D), privacy violation (S.66E), cyber terrorism (S.66F), and government interception powers (S.69).

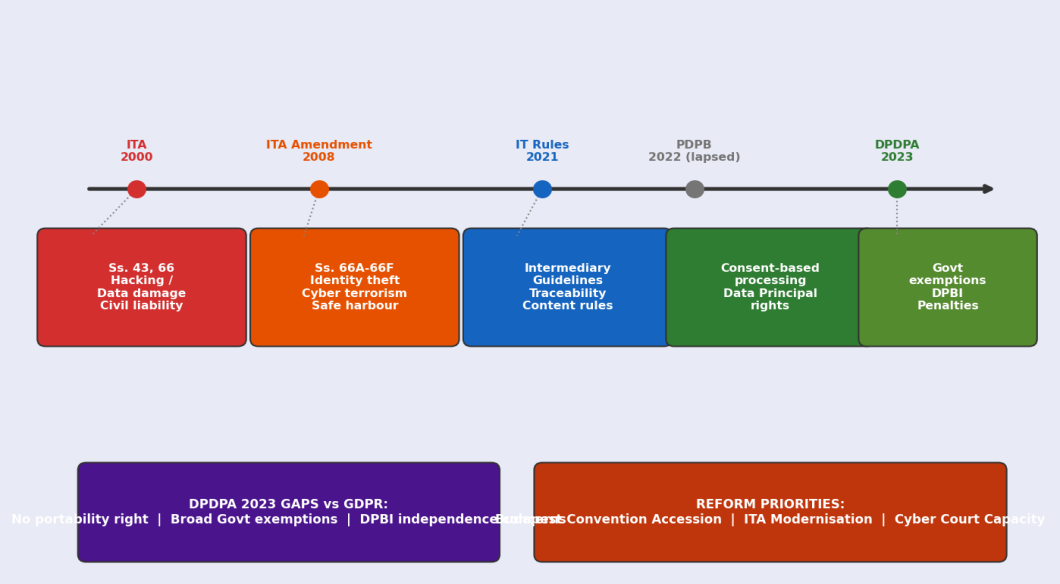

Fig. 1. Evolution of India's Cybercrime and Data Protection Legislative Framework: ITA 2000 to DPDPA 2023 with Key Provisions and Identified Gaps

2.2 Systemic Limitations in the Contemporary Context

Beyond definitional inadequacy, the ITA 2000/2008 framework suffers from: (1) jurisdictional fragmentation—Section 75's extraterritorial extension is insufficiently operationalized through MLAT mechanisms, creating practical barriers to evidence gathering in internationally-sourced cybercrimes that constitute the majority of high-impact attacks; and (2) enforcement capacity deficits—the number of trained cyber forensic investigators per 100,000 internet users in India is estimated at approximately 0.8, compared to 4.2 in the UK and 6.1 in the USA (DSCI, 2022), creating a structural gap that legislative reform alone cannot bridge.

3. The DPDPA 2023: Advances and Gaps

3.1 Key Provisions and Comparative Evaluation Against GDPR

The DPDPA 2023 establishes India's first comprehensive personal data protection framework with consent-based processing, data principal rights (access, correction, erasure, grievance), and Data Protection Board enforcement with penalties up to INR 500 crore. Figure 2 presents India's cybercrime complaint statistics and a radar chart comparison of DPDPA 2023 versus GDPR across six key regulatory dimensions.

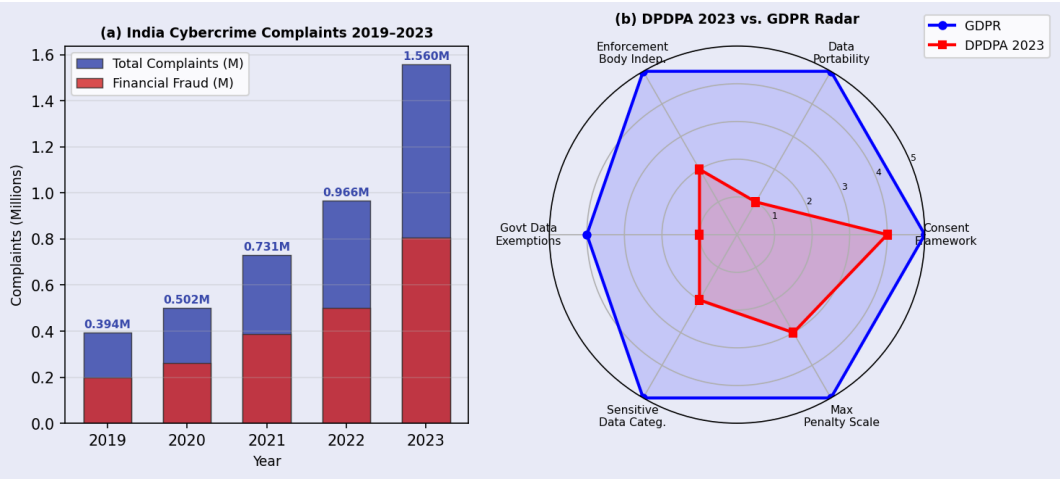

Fig. 2. (a) India Cybercrime Complaint Volume 2019–2023; (b) Regulatory Capability Radar: DPDPA 2023 vs. GDPR Across Six Governance Dimensions

Table 1: Comparative Analysis of Key Provisions: DPDPA 2023 vs. GDPR

Dimension	DPDPA 2023 (India)	GDPR (EU)
Consent Framework	Explicit, revocable consent required	Freely given, specific, informed, explicit consent
Data Subject Rights	Access, correction, erasure, grievance	Access, rectification, erasure, portability, objection
Right to Data Portability	Not included	Article 20 – Fully recognized
Government Data Exemptions	Broad sovereign/security exemptions (S.17)	Limited, narrowly construed, subject to judicial review
Enforcement Body	Data Protection Board (govt-constituted)	Independent Data Protection Authorities (DPAs)
Maximum Penalty	INR 250–500 crore (~EUR 27–55M)	EUR 20M or 4% global annual turnover
Cross-Border Transfer	Government whitelist mechanism	Adequacy decisions + SCCs + BCRs
Sensitive Data Categories	Not separately enumerated	Special categories explicitly protected

SCCs: Standard Contractual Clauses; BCRs: Binding Corporate Rules; S.17: Section 17 DPDPA 2023.

4. The IT Rules 2021 and Intermediary Liability

The IT Rules 2021 introduce a tiered intermediary classification with progressively stringent compliance obligations for significant social media intermediaries (over 5 million users). The originator traceability requirement—widely criticized as technically mandating the weakening of end-to-end encryption—remains the most contested provision, challenged before multiple High Courts on constitutional grounds. The Madras High Court raised delegated legislative competence concerns, while the Bombay High Court stayed specific provisions pending hearing.

5. Proposed Reforms and Conclusion

The article proposes five reform priorities: (1) comprehensive ITA modernisation incorporating cloud computing, AI, cryptocurrency, and IoT definitional frameworks; (2) DPBI restructuring as a truly independent statutory body insulated from executive control; (3) introduction of data portability rights and enhanced sensitive data category protections; (4) Budapest Convention accession for international cybercrime cooperation; and (5) dedicated cyber forensic investigation capacity building at state police level through university-police partnership training programmes.

India's cybercrime and data protection legal framework has undergone significant evolution culminating in the DPDPA 2023—a milestone establishing consent-based data protection as a statutory right. However, persistent gaps in data portability, government data processing accountability, enforcement independence, and technical cybercrime definitions leave Indian digital citizens with less robust protection than their EU counterparts. The proposed reforms represent a constitutionally grounded agenda to substantially narrow these gaps as India's digital transformation accelerates.

References

[1] Budapest Convention on Cybercrime. (2001). European Treaty Series No. 185. Council of Europe.

[2] Data Security Council of India (DSCI). (2022). India Cyber Threat Report 2022.

[3] European Parliament. (2016). General Data Protection Regulation (GDPR) 2016/679.

[4] Government of India. (2000). Information Technology Act, 2000 (Act No. 21 of 2000).

[5] Government of India. (2008). Information Technology (Amendment) Act 2008.

[6] Government of India. (2021). IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[7] Government of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

[8] K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017). (9) SCC 1.

[9] Nappinai, N. S. (2010). Cyber Crime Law in India. Journal of International Commercial Law and Technology, 5(1), 22–33.

[10] Shreya Singhal v. Union of India. (2015). AIR 2015 SC 1523.

[11] Solove, D. J. (2013). Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880–1903.

[12] Wacks, R. (2015). Privacy: A Very Short Introduction (2nd ed.). Oxford University Press.