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

VOLUME 5 AND ISSUE 10 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

FINTECH AND DATA PRIVACY: INDIA'S LEGAL LAG

AUTHOR - ARYAN NANDA, STUDENT AT AGNEL SCHOOL OF LAW

BEST CITATION - ARYAN NANDA, FINTECH AND DATA PRIVACY: INDIA'S LEGAL LAG, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (10) OF 2025, PG. 522-525, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

India's financial sector is rapidly evolving through technologies like AI, block chain, and real-time payments. However, existing laws such as the IT Act, 2000 and the DPDP Act, 2023 are not fully equipped to address the challenges these innovations bring. The IT Act remains outdated for current digital systems, while the DPDP Act, though a step toward data protection, raises concerns about government overreach, unclear cross-border data rules, and heavy compliance burdens on startups.

The lack of clear AI regulations in FinTech leads to issues around accountability, algorithmic bias, and misuse of personal data. This paper highlights these gaps and suggests reforms including independent oversight for data exemptions, simplified rules for small FinTechs, and a dedicated legal framework for AI in finance. Strengthening these areas is crucial to ensure user protection while supporting innovation in India's growing digital economy.

Current state of technological laws in India

IT ACT 2000

[630][THE INFORMATION TECHNOLOGY ACT, 2000 ACT NO. 21 OF 2000 [9th June, 2000.] An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as —electronic commerce , which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The following are the main objectives of the Information Technology Act of 2000 that you should know:

- The legislation aims to facilitate the implementation of efficient electronic service delivery mechanisms for public services and establish frameworks for secure digital transactions across business entities and citizens.
- Furthermore, it endeavors to create a robust cybersecurity framework by implementing penalties for various forms of cybercrime, including unauthorized system access, data breaches, digital identity theft, and cyber harassment.
- The Act mandates the development and enforcement of comprehensive regulatory frameworks to govern electronic communications, digital behavior patterns, and commercial channels in the virtual space.
- Additionally, it seeks to stimulate the expansion of India's Information Technology and IT-enabled Services sector while fostering an ecosystem conducive to technological innovation and entrepreneurial development.]

630 https://cleartax.in/s/it-act-2000

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

VOLUME 5 AND ISSUE 10 OF 2025

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

Published by

Institute of Legal Education

https://iledu.in

The Digital Personal Data Protection (DPDP) Act, 2023.

What does this law state?

[631][THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023) [11th August, 2023.] An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.]

A Simpler explanation

The Digital Personal Data Protection Act is India's effort to safeguard people's personal information in the digital space. It strikes a balance between protecting an individual's right to privacy and allowing businesses and organizations to use data when genuinely needed. Under this law, people are given greater control over their own personal data, they can ask to see it, correct any mistakes, have it deleted, and even take action if their data is misused or leaked.

Limitations / Challenges

[632][Challenges in the Implementation of the Digital Personal Data Protection (DPDP) Act, 2023 and its Impact on the Financial Sector

A major issue emerges from **Section 18** of the Act, which permits government agencies to bypass data protection requirements citing national security and public order. Though designed to facilitate investigations, this broad exemption lacks proper oversight mechanisms. This could potentially compromise privacy rights and erodes confidence in the system, particularly affecting **banking and financial services** institutions where customer data security is paramount.

For financial institutions especially **startups and fintech companies**, **Section 8** of the Act presents challenges. It requires obtaining clear informed and explicit user consent before data collection. While this promotes user rights smaller firms may struggle with the cost of legal compliance data audits and hiring **Data Protection Officers (DPOs)**. Given the rapid digitization of financial services these compliance burdens could hamper innovation and exclude smaller business competition.

Section 16's **data transfer regulations** create significant hurdles for international financial organizations. The lack of clear guidelines regarding international data flows gives the government broad discretionary powers, leading to uncertainty. This ambiguity not only affects **cloud computing in finance** but could also limit international investments in India's expanding fintech industry.]

[633][Inadequacy of the IT Act, 2000 in Regulating Emerging Financial Technologies

The **Information Technology Act of 2000** marked India's initial regulatory framework for digital commerce and governance. Despite updates, this legislation reflects an earlier digital age and struggles to address contemporary technological advancements in **machine learning**, **distributed ledger systems**, and **instant payment networks**. As computerized systems increasingly handle credit evaluation, security monitoring, and customer service in finance, the lack of regulations regarding system transparency, fairness testing, and result interpretation exposes users to unclear and potentially unfair automated judgments.

Regarding **distributed ledger systems**, the IT Act provides insufficient guidance on emerging innovations like **automated agreements** and decentralized software. While Section 10-A acknowledges electronic agreements, those based on distributed ledgers—particularly using encryption instead of certified electronic signatures—lack clear legal recognition in India.

631 https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

632 https://ijlsss.com/navigating-indias-digital-personal-data-protection-act-critical-implications-and-emerging-challenges/

633 https://www.researchgate.net/publication/390195375_Blockchain_and_AI_in_Digital_Contracts_A_Legal_Review_of_Smart_Contract_Enforcement

This creates uncertainty in enforcement, particularly regarding international transactions and decentralized financial services. The law also lacks clear direction on legal jurisdiction, verification processes, and information security within these networks.

The emergence of **instant payment platforms** such as UPI, electronic money services, and the Central Bank Digital Currency (CBDC) further highlights the Act's limitations. These systems operate with immediate, continuous transaction processes not considered in the Act's original structure. Consequently, user protection measures, information exchange protocols, and system compatibility requirements remain insufficient.]

Legal Gaps in AI-Driven Fintech

[634][A key concern in India's current legal landscape is the absence of a clear, specialized law to regulate the use of Artificial Intelligence in the financial sector. Although laws like the Digital Personal Data Protection Act, 2023, and the Companies Act, 2013, exist, they do not effectively cover the complexities that AI technology introduces into Fintech operations. These systems often referred to as "black boxes," operate through complex algorithms that are not easily understood or traceable. This lack of clarity becomes particularly problematic when AI is used in sensitive areas like credit assessment or financial advice. There have already been cases where individuals were denied loans based on income levels or other demographic factors, with no reasonable explanation provided—raising red flags about potential bias and unequal treatment.

Furthermore, the reliance of AI systems on large volumes of personal data brings serious concerns about privacy. Many FinTech platforms collect and process user data without obtaining clear or informed consent, thereby undermining the core principles of the DPDP Act. Some companies have even faced backlash for accessing private phone data and call records without user approval. Additionally, the rules governing the international flow of such data remain vague, making compliance difficult for businesses with cross-border operations. On the cyber security front, AI-driven platforms are becoming increasingly attractive targets for cyber criminals. Advanced hacking techniques are now capable of exploiting weaknesses in these systems, and the outdated IT Act, 2000, provides little guidance or protection against such threats. One widely reported case involved a major payment gateway being breached through AI-enabled tactics, exposing flaws in the system's fraud detection setup.

Accountability also remains a grey area. As AI becomes more autonomous in decision-making, it becomes harder to identify who should be held responsible when things go wrong—the technology developers, the financial firms deploying them, or the vendors supplying the systems. This lack of legal clarity has already resulted in lawsuits from customers who suffered financial harm due to incorrect recommendations from AI tools. Startups in the FinTech space, though highly innovative, are burdened by the costs and confusion of trying to comply with unclear or outdated laws. Questions about who owns AI-generated content—like proprietary algorithms or financial models—further complicate matters, often stalling product development or market entry.]

Legal Reforms to Strengthen FinTech and Data Protection [Personal Opinion]

To address the overbroad exemptions in Section 18 of the DPDP Act, a review mechanism should be introduced where any bypass of data protection norms must be subject to judicial or independent oversight. This can restore user trust, especially in the financial sector, by ensuring such powers aren't misused.

The consent-heavy structure under Section 8 should be made proportional to the size and risk exposure of the company. Startups and small fintechs should be allowed simplified compliance procedures, with optional regulatory sandbox participation to test

634 https://www.ijfmr.com/papers/2025/1/37447.pdf

products under guided supervision without full legal burden.

For Section 16's ambiguity around cross-border data flow, the government should define a transparent framework with clear benchmarks for "trusted" countries. Standard contractual clauses and bilateral data-sharing protocols can make cross-border operations smoother and legally secure.

Since the IT Act, 2000 is outdated; there is an urgent need for a sector-specific legal framework to cover AI-based financial technologies. This should include rules for algorithmic accountability, transparency in automated decisions, and mandatory explanation of AI-based rejections or approvals in financial services.

Privacy norms must be strictly enforced through mandatory user consent audits and periodic cybersecurity testing. Platforms using personal data, especially in sensitive services like credit scoring, should be held liable for breaches or unauthorized data use.

To solve the accountability gap in AI deployment, a legal liability structure must be created. This should assign responsibility based on the function—developer, deployer, or data provider—and ensure consumers have clear legal recourse when harmed by AI-driven tools.

Finally, courts should encourage the drafting of a unified FinTech and AI regulation code that integrates privacy, cybersecurity, algorithmic fairness, and intellectual property to ensure India's financial innovation grows without compromising user rights.

As India advances toward a digitally-driven financial ecosystem, it becomes crucial to align legal frameworks with the pace of innovation. While the IT Act, 2000 and the DPDP Act, 2023 offer foundational support, they fall short in addressing the complexities of AI, data privacy, and emerging FinTech models. Without clear rules on accountability, data governance, and algorithmic transparency, both users and service providers face uncertainty. To ensure inclusive growth, regulatory clarity, and user protection, India must adopt a forward-looking, sector-specific legal framework that supports innovation without compromising individual rights or systemic integrity.