ORIGINAL RESEARCH PAPER
Volume - 14 | Issue - 09 | September - 2025 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

EMERGING TRENDS IN INFORMATION TECHNOLOGY WITH SPECIAL REFERENCE TO THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A SYNOPTIC VIEW

Law

Dr Nameeta Rana Assistant Professor (LAW), HPU Regional Centre, Dharamshala.

ABSTRACT

The fast-paced evolution of Information Technology (IT) has drastically reshaped the digital ecosystem, bringing significant changes to the ways in which data is generated, utilized, and shared. Among these developments, the safeguarding of personal data has emerged as a key issue, necessitating robust legal and technological frameworks. In response, the Government of India introduced the Digital Personal Data Protection Act, 2023 (DPDPA), a comprehensive legislation aimed at ensuring the responsible handling of personal data in the digital age. This paper presents a concise overview of the latest trends in IT-such as Artificial Intelligence (AI), Big Data, Cloud Computing, Internet of Things (IoT), Block chain, and advancements in Cyber security-and evaluates them in relation to the provisions of the DPDPA, 2023. While these technologies offer transformative potential across sectors, they also raise critical concerns around privacy, data security, and ethical usage. The Act introduces foundational principles like lawful processing, consent-based data collection, data minimization, and transparency to address these challenges. One of the key features of the DPDPA is the establishment of the Data Protection Board of India, tasked with ensuring compliance and addressing grievances. The legislation grants individuals greater control over their personal data, including rights to access, correction, and deletion, while imposing accountability measures on organizations that handle such data. This abstract highlights how the intersection of cutting-edge IT innovations and stringent data protection laws is shaping a new paradigm for digital governance in India. It emphasizes the need for a balanced approach-encouraging technological advancement while upholding privacy rights. The DPDPA, 2023, thus represents a critical step towards building a secure, ethical, and inclusive digital future where innovation and individual rights go hand in hand.

KEYWORDS

Information Technology (IT), Data, Data Security, Privacy, digital governance

INTRODUCTION

In the era of rapid digital transformation, personal data has become immensely valuable commodities, driving innovations in artificial intelligence, e-commerce, healthcare, and governance. However, this unprecedented data explosion has raised serious concerns about privacy, security, and individual autonomy. Recognizing these challenges, the Indian Parliament enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), marking a decisive step toward a comprehensive legal framework for data protection.

The DPDP Act aligns India with global data protection trends while addressing unique national priorities such as data sovereignty and raising a digital economy. By codifying rights for data principals and responsibilities for data fiduciaries, the Act aims to build trust in digital services, promote transparency, and safeguard citizens' privacy in the digital age.

The 21st century has witnessed a unique explosion in the use of digital technologies. The proliferation of smartphones, the continuous use of the internet, the rise of artificial intelligence, and the deployment of big data analytics have fundamentally transformed how masses connect, individuals businesses, and governments interact. While these advancements have boosted innovation, efficiency, and economic growth, they have also given rise to complex concerns regarding the collection, storage, processing, and transfer of personal data.

In India, this digital evolution has been rapid and far-reaching. The government's ambitious Digital India initiative, e-governance, and online platforms, and the increasing penetration of social media have made data an indispensable resource. However, the exponential increase in personal data generation has also led to growing apprehensions about data breaches, unauthorized surveillance, profiling, and the erosion of individual privacy.

But the current situation is that India lacked a comprehensive statutory framework dedicated solely to the protection of personal data. The primary legal protections were embedded in the Information Technology Act, 2000, and the accompanying rules, which proved inadequate in addressing contemporary data protection challenges. Judicial pronouncements, particularly the landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017), recognized the right to privacy as a fundamental right under Article 21 of the Constitution, thus compelling the legislature to act. Responding to this constitutional mandate and evolving global norms, the Indian Parliament enacted the **Digital Personal Data Protection Act, 2023** (hereafter, "DPDP Act"). This legislation represents a critical turning point in India's approach to digital governance. It establishes a rights-based, consent-centric framework for the processing of digital personal data and aligns India with international data protection standards, such as the General Data Protection Regulation (GDPR) of the European Union.

This article gives a synoptic yet in-depth legal analysis of the emerging trends in information technology, with special reference to the DPDP Act. It will explore the structure, principles, and provisions of the Act; assess its implications for stakeholders in the IT ecosystem; analyse its collaboration with emerging technologies; and evaluate its convergence with global data protection regimes. In doing so, the article seeks to critically examine how the DPDP Act is shaping the future of privacy, innovation, and accountability in the digital economy. By analysing these facets, the article aims to provide a deep understanding of how the DPDP Act is redefining India's digital future.

Overview Of The Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection Act, 2023** (DPDP Act) is India's first comprehensive data protection law that seeks to provide a structured legal framework for safeguarding digital personal data while facilitating lawful data processing for legitimate purposes. The Act was passed by the Indian Parliament and received Presidential assent on August 11, 2023, following several recapitulations of earlier draft bills, intense policy debates, and extensive public consultations.

The DPDP Act applies to the processing of **digital personal data** within the territory of India, where such data is collected online or collected offline and subsequently digitalized. It also applies to the processing of digital personal data outside India, if such processing is related to offering goods or services to data principals within India. Unlike the GDPR, the DPDP Act restricts its ambit to **digital data only**, excluding non-digitized personal data unless it is subsequently digitized. This clear explanation avoids overlapping with other legal domains and narrows the law's focus to the digital sphere.

The DPDP Act is built on seven foundational principles i.e. lawful use of personal data, consent-based processing, Purpose limitation, Data minimization, Data accuracy, storage limitation and accountability through compliance and grievance redress mechanisms. These principles underscore the dual aims of the DPDP Act protecting the rights of individuals and facilitating the responsible and secure processing of personal data for lawful purposes.

The journey toward comprehensive data protection legislation in India began with the 2017 Supreme Court decision in *Justice K.S. Puttaswamy v. Union of India*, which affirmed the right to privacy as a fundamental right. This landmark ruling necessitated the formulation of a statutory regime to protect personal data. In response, the Ministry of Electronics and Information Technology constituted a committee led by Justice B.N. Srikrishna, which released the draft Personal Data

Protection Bill in 2018. After several rounds of revisions, public consultations, and scrutiny by parliamentary committees, the DPDP Bill was introduced in 2023, reflecting a balance between individual privacy and the needs of innovation ease of doing business, and national security. The final legislation, while drawing from global data protection standards, is tailored to India's unique digital ecosystem and governance challenges. The DPDP Act is intended to coexist with sectoral laws such as the Information Technology Act, 2000 and industry-specific regulations (e.g., RBI guidelines for fintech, IRDAI rules for insurers). In case of conflict, the DPDP Act has an overriding effect, ensuring consistency in privacy standards across sectors.

Major IT Trends Intersect With India's DPDPA, 2023

1. Artificial Intelligence (AI)

India is rapidly adopting AI-in 2022, it ranked fifth worldwide in AI investments and GitHub contributions. Government efforts like the Centre for Machine Intelligence at IIT Bombay and AI-focused supercomputing through Digital India aim to advance areas such as health and agriculture. Under the DPDPA, AI systems must rely on explicit consent and data minimization; profiling requires transparency, and significant data fiduciaries (SDFs) must conduct Data Protection Impact Assessments (DPIAs).Privacy-by-design and ethics frameworks are essential in AI deployment.

2. Big Data & Cloud

Indian enterprises increasingly use cloud platforms and big-data analytics. The DPDPA mandates consent-based processing and restricts "legitimate interest" exemptions seen in GDPR . Complexities arise with cross-border transfers: a "block list" model is used, allowing transfers except where explicitly restricted. Draft rules are reinstating data localization for critical personal data, impacting global IT giants like Meta and Google.

3. IoT

IoT uptake in India-smart cities, wearables-is exponential but generates vast user data. Under Section 33, the Act prohibits tracking children (<18) and mandates verifiable parental consent. Manufacturers must adopt security by design, implement robust access controls, and ensure user consent and data deletion during device lifecycle end.

4. Block Chain

Indian telecom experimented with decentralized ledgers (e.g., using blockchain to curb spam messages). However, block chain's immutability conflicts with data erasure/correction rights under the DPDPA. Solutions include off-chain storage and pseudonymization to comply.

5. Cyber Security & Data Breaches

India has witnessed major data incidents and leaks-boAt, BSNL, and AIIMS breaches-affecting millions. The DPDPA mandates strict security safeguards, immediate breach notifications, and empowers the Data Protection Board (DPB) with enforcement powers.

6. Special Protections: Children & Vulnerable Groups

The Act defines children as those under 18 (higher than GDPR's under-13 threshold). For minors, parental verifiable consent is mandatory, and targeted advertising/tracking is prohibited.

7. Regulatory & Governance Structure

The Data Protection Board of India (DPB) is an adjudicatory body with civil-court powers—summoning, mediation, interim orders, and inquiries. However, experts raise concerns over government influence, broad exemptions for national security, and limited independence when compared to GDPR-style regulators,

8. Societal Awareness & SME Readiness

Despite strong legislation, public awareness remains low-most Indians and SMEs are unfamiliar with key concepts like data fiduciaries and data principals. Compliance costs-especially for SMEs-pose additional hurdles. Stakeholders urge launches of campaigns, training programs, and affordability interventions to ease the transition.

CRITICAL EVALUATION OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 IN THE INDIAN SCENARIO

a. Overbroad Government Exemptions

The central government can exempt any agency from compliance with the Act under vague grounds like national security or public order (Section 17). This dilutes the effectiveness of the Act and raises concerns of state surveillance without judicial oversight. Critics argue this could be used to bypass privacy protections for mass surveillance programs like Aadhaar, CCTNS, or NATGRID.

b. Lack of Data Localization Mandate

Unlike earlier drafts, the DPDP Act does not mandate local storage of personal data. While cross-border data flow is allowed (except to blacklisted nations), this raises cyber security and sovereignty concerns, especially in sensitive sectors like health, defence, and finance.

c. Weak Autonomy of the Data Protection Board

The Data Protection Board is appointed and controlled by the executive, raising questions about its independence. It lacks the constitutional safeguards available to independent regulators like SEBI or the Election Commission.

d. Ambiguity Around "Deemed Consent"

The concept of "deemed consent" (Section 7) allows data to be processed without explicit consent in situations like emergencies or for public interest. However, the scope of "public interest" is broadly defined and prone to misuse.

e. No Separate Category for Sensitive Personal Data

Unlike the GDPR, which imposes stricter rules for sensitive data (biometric, health, etc.), the DPDP Act does not distinguish between ordinary and sensitive personal data-potentially reducing protections for more vulnerable information.

f. Underdeveloped Grievance Redressal Process

While the Act allows users to file complaints with data fiduciaries and escalate to the Board, there is no clear time-bound, independent grievance mechanism. Also, class-action remedies are not explicitly provided.

g. Practical Challenges in Implementation SME and Start-up Compliance

Smaller businesses face significant hurdles in adopting compliance infrastructure (e.g., consent tracking, data audits, DPIAs). Without adequate government support or transition guidelines, compliance burdens could hurt digital innovation.

h. Public Awareness

India has low digital literacy and limited awareness of data rights. For the law to be effective, massive public education and training programs are essential, especially in rural and semi-urban areas.

i. Sectoral Overlap and Conflict

The Act's implementation may conflict with sector-specific regulations (e.g., RBI, TRAI, IRDAI), causing regulatory overlaps or inconsistencies that could confuse organizations.

COMPARATIVE PERSPECTIVE

A comparison between India's Digital Personal Data Protection Act, 2023 (DPDP Act) and the European Union's General Data Protection Regulation (GDPR) reveals both alignments and significant departures. One major distinction lies in government exemptions: the DPDP Act provides the Indian government with broad and largely unchecked powers to exempt any entity from the law's scope, citing reasons such as national security. In contrast, the GDPR offers narrow, specific exemptions that are subject to judicial review, ensuring a balance between public interest and individual rights. Another key difference is in the treatment of sensitive personal data. The GDPR clearly defines and provides additional safeguards for sensitive categories like biometric, health, and genetic data. The DPDP Act, however, does not explicitly differentiate between general and sensitive personal data, potentially reducing the level of protection for more vulnerable information in India.

On the matter of data localization, the DPDP Act does not mandate that personal data be stored within India's borders; it allows cross-border transfers except to countries explicitly restricted by the government. GDPR permits data transfers outside the EU but only to jurisdictions offering adequate levels of data protection, or through mechanisms like Standard Contractual Clauses (SCCs). The regulatory framework also differs significantly. Under the DPDP Act, the Data Protection Board of India is appointed and controlled by the central government,

raising concerns about its lack of independence. By contrast, the GDPR establishes independent supervisory authorities in each EU member state with strong enforcement powers. Finally, in both laws, consent remains a central requirement for data processing. However, the GDPR's consent framework is considered more detailed and stringent, incorporating the principles of unambiguous opt-in, informed consent, and the right to withdraw consent at any time. While the DPDP Act adopts similar language, its practical enforcement mechanisms and protections are still evolving.

Impact Of The DPDP Act On IT Practices

The DPDP Act introduces several obligations for data fiduciaries:

- **Cross-Border Transfers**: Transfers are permitted unless the destination is blacklisted by the government.
- **Consent Management**: Data must be processed only with free, informed, and unambiguous consent.
- **Data Breach Notification**: Fiduciaries must report breaches to the Data Protection Board and affected individuals.
- **Children's Data Protection**: Verifiable parental consent is required for processing data of minors.

These provisions compel IT companies to redesign data architectures, update privacy policies, and invest in compliance technologies. The above contents can be further elaborated i.e.

CROSS-BORDER DATA TRANSFERS UNDER THE DPDP ACT, 2023: A LEGAL ANALYSIS.

The Digital Personal Data Protection Act, 2023 (DPDP Act) introduces a pivotal framework for regulating cross-border data transfers in India. This mechanism is articulated under Section 16, which diverges from traditional models like the European Union's GDPR "adequacy list," by implementing a "negative list" approach. Instead of requiring prior approval for every destination, the Indian government may notify specific countries or territories where personal data transfers are prohibited, allowing transfers to all other jurisdictions by default. This model has been praised for its reasonableness and openness to global digital commerce, but also criticized for its current lack of clarity, as the government has yet to publish the list of restricted nations.

Importantly, the DPDP Act does not distinguish between sensitive or critical personal data for cross-border purposes, which marks a departure from earlier Indian drafts like the 2019 Personal Data Protection Bill. However, the Act preserves flexibility by enabling sectorial regulators to impose stricter localization requirements. For instance, the Reserve Bank of India's circular (2018) still mandates local storage for payment data, the IRDAI requires health insurance data to remain in India, and Department of Telecommunications (DoT) licenses enforce similar rules for telecom data. Thus, while the DPDP establishes broad permission for international transfers, organizations must navigate overlapping sector-specific mandates.

To ensure that cross-border transfers do not undermine individual privacy, fiduciaries must maintain transparency and accountability. This includes obtaining valid consent or legitimate processing grounds, updating privacy notices to inform data subjects about overseas transfers, and incorporating contractual safeguards like Standard Contractual Clauses (SCCs). Large data fiduciaries are also expected to conduct Data Protection Impact Assessments (DPIAs) prior to high-risk transfers, and maintain audit trails documenting the flow and purpose of data. These measures aim to provide equivalent protection to Indian citizens, even when data crosses borders.

Multinational corporations may benefit from Binding Corporate Rules (BCRs), which, once vetted and approved by the Data Protection Board, allow intra-group transfers across jurisdictions not on the government's restricted list. Moreover, in cases where foreign legal authorities request access to Indian personal data, the Act does not bar compliance-unless the recipient jurisdiction is prohibited or another Indian law explicitly forbids disclosure.

In conclusion, the DPDP Act's stance on cross-border data transfers reflects a delicate balance between openness and sovereignty. While the default openness supports innovation and international collaboration, the Act's evolving nature, especially the pending notification of restricted countries, necessitates constant vigilance by organizations. They must monitor regulatory updates, align contractual practices, and ensure compliance with both general and sectoral norms to avoid penalties, which could scale up to ₹250 crore in case of serious breaches. As emphasized by legal analysts, India's approach may offer a business-friendly framework, but its efficacy will ultimately depend on its implementation and enforcement strategy.

Consent Management

Under Section 6 of the DPDP Act, consent is the cornerstone of lawful data processing. It must be free, specific, informed, unconditional, and unambiguous, demonstrated through a clear affirmative action. IT teams must design consent flows that are transparent and accessible. Pre-ticked boxes or bundled consents are prohibited, requiring granular options for each purpose of data collection. Systems must support collection, validation, updates, renewal, and withdrawal of consent. This includes time stamping, purpose tagging, and multilingual support. Organizations must maintain detailed logs of consent actions for regulatory audits and dispute resolution. Entities may appoint or integrate with Consent Managers, intermediaries registered with the Data Protection Board, to facilitate secure and interoperable consent handling. The required technologies**:**

- Consent Management Platforms (CMPs)
- Metadata tagging and logging tools
- Multilingual UI frameworks
- APIs for real-time consent synchronization

DATA BREACH NOTIFICATION

The DPDP Act mandates that data fiduciaries promptly notify both the Data Protection Board of India and affected individuals in the event of a personal data breach. The Implications for IT Systems are Incident Response Plans (IRPs): IT departments must establish 24/7 breach detection and response protocols, including escalation workflows and containment strategies. Secondly, Monitoring & Detection: Real-time monitoring tools must be deployed to detect unauthorized access, data exfiltration, or system anomalies. Thirdly, Notification Systems; Automated systems must be capable of sending breach alerts to users via email, SMS, or in-app notifications, detailing the nature of the breach, its impact, and recommended safety measures. Regulatory Reporting: IT teams must prepare structured reports for the Data Protection Board within 72 hours, including root cause analysis, mitigation steps, and affected data categories.

The required Technologies for this are Security Information and Event Management (SIEM) tools, Data Loss Prevention (DLP) systems, automated breach notification platforms, Encryption and access control mechanisms.

CHILDREN'S DATA PROTECTION

The Act defines a child as anyone under 18 years of age, and requires verifiable parental consent before processing their personal data. It also prohibits behavioural tracking and targeted advertising directed at children. IT systems must follow, Age Verification Mechanisms: Platforms must implement robust age-gating systems, possibly integrating with DigiLocker or Aadhaar-based verification, Parental Consent Workflows: IT systems must support identity verification of parents or guardians and maintain records of their consent. Content Filtering: Algorithms must be adjusted to prevent behavioural profiling or targeted ads for minors. Data Segmentation: Children's data must be stored and processed separately, with enhanced safeguards and restricted access. For this required technologies are Identity verification APIs, Consent validation engines, Age-appropriate content filters, segregated data storage and access controls.

CHALLENGES AND OPPORTUNITIES

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a landmark shift in India's data governance framework, offering a structured approach to personal data protection. However, its implementation presents a complex mix of challenges and opportunities. One of the foremost challenges is the compliance burden on small and medium enterprises (SMEs), which often lack the financial and technical resources to meet the Act's stringent requirements, such as appointing Data Protection Officers and conducting Data Protection Impact Assessments. Additionally, the lack of clarity in certain provisions, especially around cross-border data transfers and deemed consent, has led to confusion among stakeholders. The broad exemptions granted to government agencies under Section 17 have also raised concerns about potential misuse and the erosion of individual privacy rights, especially in the absence of robust judicial oversight. Another challenge lies in the limited awareness and digital literacy among the general population, which could hinder the effective exercise of rights by data principals.

Moreover, the Data Protection Board's independence and capacity remain under scrutiny, with critics pointing to its executive-controlled structure as a potential threat to impartial enforcement. Despite these hurdles, the DPDP Act opens up significant opportunities. It provides a uniform legal framework that aligns India with global data protection standards, enhancing the country's credibility in international trade and digital services. The Act encourages the adoption of privacy-enhancing technologies, such as encryption and anonymization, fostering innovation in cyber security and compliance tools. For businesses, especially in sectors like e-commerce, fintech, and healthcare, the Act offers a chance to build consumer trust through transparent data practices and robust security measures. The emphasis on consent and accountability can lead to better data governance, reducing risks of breaches and reputational damage. Furthermore, the Act's flexible approach to cross-border data transfers—allowing them unless specifically restricted—supports India's growing digital economy and global partnerships. The DPDP Act also empowers individuals by granting those rights to access, correct, and erase their data, thereby promoting informational autonomy. In the long run, the Act could catalyze the development of a privacy-conscious culture, encouraging ethical data use and responsible innovation. To fully realize these opportunities, however, the government must ensure transparent rule-making, strengthen the Data Protection Board's independence, and launch public awareness campaigns to educate citizens and businesses alike. With thoughtful implementation and continuous refinement, the DPDP Act has the potential to transform India's digital landscape into one that respects privacy while enabling growth.

CONCLUSION

The Digital Personal Data Protection Act, 2023 serves as a pivotal cornerstone in India's journey toward data sovereignty and responsible information technology governance. As we've explored, the Act ushers in comprehensive obligations for IT stakeholders-ranging from managing user consent with precision, to deploying robust breach notification systems, to safeguarding the rights of children in digital spaces, and navigating the complexities of cross-border data transfers. These requirements not only reshape technical infrastructure but also demand a cultural shift toward privacy-by-design and ethical data practices.

While the DPDP Act offers a structured and forward-looking framework, challenges persist, including regulatory ambiguity, the resource strain on SMEs, and questions surrounding the independence of enforcement bodies. Yet, these hurdles are counterbalanced by remarkable opportunities: building public trust, fostering innovation, and positioning India as a global leader in digital privacy governance. The emphasis on individual rights and accountability aligns India with leading international standards while accommodating domestic needs through flexible compliance models. Ultimately, the success of the DPDP Act hinges on transparent implementation, continuous stakeholder engagement, and the evolution of supportive technologies and institutions. With thoughtful execution, this legislation has the potential not only to protect personal data but also to shape a digitally empowered, privacy-conscious society.

REFERENCES:

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
2. Spice route Legal, "A Deep Dive into the DPDP Act, 2023"
3. https://beta.spiceroutelegal.com/publications/the-digital-personal-data-protection-act-2023-a-deep-dive/?utm
4. https://www.ft.com/content/1923efa2-d6b2-4765-bbf3-2711c74ba611?utm_
5. https://arxiv.org/abs/2205.12350?utm_
6. https://www.reddit.com/r/StartUpIndia/comments/1i2mf0f?utm_
7. https://www.privacyanddatasecurityinsight.com/2023/11/breaking-down-indias-digital-personal-data-protection-act-2023/?utm_
8. https://lawfullegal.in/personal-data-protection-act-2023-a-step-forward-or-a-threat-to-privacy/?utm_
9. https://www.reddit.com/r/IndiaTrending/comments/18myu2v?utm
10. Internet Freedom Foundation (IFF) – "Concerns with DPDP Act"
11. European Commission – GDPR Text and Explanations
12. Vidhi Centre for Legal Policy – "Policy Brief on India's Data Protection Law"
13. The Digital Personal Data Protection Act, 2023 – Government of India Gazette
14. Taxmann's detailed breakdown of Section 16 of the DPDP Act –2023
15. Leegality's compliance guide on cross-border transfers 2023
16. Supra 14
17. Supra15
18. Consent Management under India's DPDP Act: Best Practices for Compliance.
19. ibid
20. Latest Laws' Legal Commentary 2025
21. Sansad's Official DPDP Bill Text – The original bill as introduced in Lok Sabah, detailing all clauses and provisions.