

---

# A CRITICAL ANALYSIS OF DATA PROTECTION LAW IN SAFEGUARDING DIGITAL PRIVACY IN INDIA

---

Hari Basker K, VISTAS

Stella Jennifer, VISTAS

## 1. Introduction

The rise of India's digital economy has transformed how personal data is collected, processed, and stored. From Aadhaar-based identification systems to UPI transactions, e-commerce platforms, and social media networks, individuals constantly share sensitive information online. This rapid digitization has created unprecedented opportunities for innovation and governance but has also raised serious concerns about **digital privacy** and **data misuse**.

Globally, frameworks like the **General Data Protection Regulation (GDPR)** in the European Union have set high standards for safeguarding personal data. India, however, has historically relied on fragmented provisions under the **Information Technology Act, 2000** and sectoral regulations. The enactment of the **Digital Personal Data Protection Act, 2023 (DPDP Act)** marks a significant step toward codifying privacy protections, but its adequacy remains contested.

### 1.1. Object of the Research

The object of this research is to critically examine India's data protection laws in their constitutional, statutory, and comparative dimensions, to assess their adequacy in safeguarding digital privacy, and to propose reforms that balance state interests with individual rights while ensuring global compatibility. To analyse whether exemptions granted to the government are **proportionate, necessary, and subject to oversight**, or whether they undermine individual privacy

### 1.2. Scope of the Research

The scope of this research encompasses constitutional jurisprudence, statutory provisions, sectoral regulations, and comparative perspectives to critically evaluate whether India's data

protection laws adequately safeguard digital privacy. It extends to practical implications for citizens, businesses, and democracy, while proposing reforms to strengthen the framework. However, the study is limited to legal analysis and does not cover technical cybersecurity measures or non-legal aspects of privacy. It is limited to a doctrinal and analytical study of the DPDP Act, 2023.

### **1.3. Hypothesis:**

India's data protection framework under the DPDPA, 2023 fails to provide effective safeguards for digital privacy due to weak institutional enforcement mechanisms and significant divergence from global standards such as the EU GDPR, thereby undermining citizen rights.

### **1.4. Research Problem**

The research problem lies in the inadequacy of India's current data protection framework to effectively safeguard digital privacy. Despite constitutional recognition of privacy as a fundamental right, statutory provisions remain fragmented, enforcement mechanisms weak, and government exemptions broad. This creates a gap between the promise of privacy and its practical realization, raising urgent questions about autonomy, accountability, and India's global credibility.

### **1.5. Research Questions:**

This critical analysis seeks to answer the following key questions:

1. How is digital privacy defined and recognized in India?
2. What are the strengths and limitations of India's current data protection laws?
3. How does the DPDP Act, 2023 balance state interest and individual privacy?
4. How does India's framework compare with global standards such as GDPR?
5. What reforms are necessary to ensure effective safeguarding of digital privacy?

### **1.6. Limitation:**

This research is limited by the recent enactment of the DPDP Act with limited judicial

precedents and reliance on secondary sources rather than empirical fieldwork. Comparative analysis with GDPR is constrained by contextual differences and the dynamic nature of privacy law may alter interpretations in the future.

## 2. Critical Gaps in Data Protection Framework

Despite constitutional recognition of privacy as a fundamental right, India's data protection framework suffers from critical gaps: broad government exemptions, weak enforcement, diluted consent, fragmented sectoral rules, and vague cross-border provisions. These shortcomings undermine the safeguarding of digital privacy, leaving citizens vulnerable and weakening India's global credibility.

Although the Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive attempt at regulating personal data, its structural weaknesses undermine the constitutional right to privacy. The most significant concerns arise from the **breadth of State exemptions**, the **weak independence of the Data Protection Board** and the **limited scope of individual rights**. These gaps must be examined against the constitutional standards laid down in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) and comparative frameworks like the EU's General Data Protection Regulation (GDPR).

## 3. Comparative Analysis of Data Protection Framework

Comparative analysis reveals that while India's DPDP Act marks progress toward codifying digital privacy, it remains weaker than GDPR in terms of rights, consent, enforcement, and penalties. Compared to the US, India benefits from a unified law but suffers from weak enforcement and broad government exemptions. This highlights the urgent need for reforms to align India's framework with global standards and build trust in its digital economy.

The European Union's General Data Protection Regulation (GDPR), enacted in 2018, is widely recognized as the most comprehensive and rights-based data protection framework globally. It has become the benchmark against which other jurisdictions are measured. India's Digital Personal Data Protection (DPDP) Act, 2023, represents the country's first consolidated attempt to legislate privacy protections following the Supreme Court's landmark recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017). However, when placed side by side with the GDPR, the DPDP Act reveals significant deficiencies. This chapter

undertakes a comparative analysis of the two frameworks, focusing on five critical dimensions: individual rights, regulatory independence, proportionality and necessity, horizontal obligations on corporations and global adequacy standards. The analysis demonstrates that the DPDP Act falls short of both constitutional expectations and international best practices.

The DPDP Act falls short of global standards in every critical dimension: rights, regulatory independence, proportionality, corporate obligations, enforcement and adequacy. By prioritizing state convenience and corporate flexibility over individual dignity and autonomy, the Act undermines both constitutional privacy rights and international credibility. To align with global best practices, India must reform the DPDP Act to embed proportionality, strengthen individual rights, ensure regulatory independence and impose robust obligations on corporations. Only then can India position itself as a credible privacy jurisdiction in the global digital economy

This insufficiency has profound implications. For individuals, it means reduced autonomy and vulnerability to both state surveillance and corporate exploitation. For businesses, it creates compliance uncertainty and hinders global operations. For India's global standing, it undermines credibility as a privacy jurisdiction, limiting trade and technology partnerships.

GDPR represents the **gold standard** in data protection, embedding comprehensive rights, independent regulators, proportionality and corporate accountability. The DPDP Act, by contrast, is **insufficient**: it prioritizes state convenience and corporate flexibility over individual dignity and autonomy. This comparative analysis underscores that India's framework fails both **constitutionally (Article 21, dignity and autonomy)** and **internationally (GDPR adequacy standards)**. For India to align with global best practices and uphold constitutional privacy rights, the DPDP Act must be reformed to embed proportionality, strengthen individual rights, ensure regulatory independence and impose robust obligations on corporations.

### 3.1 Comparative Analysis of the IT Act, 2000

The IT Act was enacted in **2000**, primarily to regulate **e-commerce, digital signatures, and cybercrime**. At that time, **privacy was not recognized as a fundamental right** in India. In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court declared privacy a fundamental right under Article 21.

The IT Act is **transaction-centric**, while modern frameworks like GDPR and India's DPDP Act are **rights-centric**, embedding privacy as a core principle.

### 3.2 Comparative Analysis of the SEBI

SEBI has successfully strengthened transparency and accountability in financial markets, its framework remains transaction-centric, not privacy-centric. In the era of digital trading and fintech innovation, SEBI's approach to data protection lags behind global standards

## 4. Recommendations and Way Forward

The insufficiencies of the Digital Personal Data Protection (DPDP) Act, 2023, have been analyzed in detail across previous chapters. While the Act represents a significant step forward in legislating privacy protections in India, its limitations undermine both constitutional guarantees and international credibility. This chapter sets out recommendations and a way forward, focusing on five critical areas: strengthening individual rights, embedding proportionality and judicial oversight in exemptions, ensuring independence of the Data Protection Board, aligning with GDPR to enable global data flows and building a rights-based data protection culture in India. Together, these recommendations provide a roadmap for reforming the DPDP Act to meet constitutional standards and global best practices.

### 4.1 Strengthening Individual Rights

The DPDP Act currently grants only basic rights of correction and erasure. To empower individuals in the digital economy, the rights framework must be expanded.

### 4.2 Embedding Proportionality and Judicial Oversight in Exemptions:

Section 17 of the DPDP Act allows blanket state exemptions without proportionality or oversight. Embedding proportionality and oversight would align the DPDP Act with constitutional jurisprudence (*Puttaswamy*, *Anuradha Bhasin*) and global standards.

### 4.3 Ensuring Independence of the Data Protection Board

The Data Protection Board, as currently structured, lacks independence due to government control over appointments. An independent regulator is essential for procedural safeguards, ensuring that individuals have effective remedies against misuse of personal data.

#### 4.4 Aligning with GDPR to Enable Global Data Flows

India's digital economy is increasingly integrated with global markets. To enable trusted cross-border data flows, the DPDP Act must align with GDPR. Alignment with GDPR would enhance India's global credibility, strengthen trade partnerships and position India as a leader in digital governance.

### 5. Conclusion

The Digital Personal Data Protection (DPDP) Act, 2023, represents India's first consolidated attempt to legislate privacy protections following the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017).<sup>1</sup> While the Act is a landmark in acknowledging the importance of data protection, the preceding chapters have demonstrated that it is insufficient both constitutionally and internationally. This conclusion restates the insufficiencies of the DPDP Act, emphasizes the need for reforms to meet constitutional and global standards and offers final reflections on privacy as a cornerstone of democracy in the digital age.

#### 5.1 Closing Statement

The Digital Personal Data Protection (DPDP) Act, 2023, is a milestone in India's legislative journey, but it is ultimately insufficient in its current form. Throughout this dissertation, it has been demonstrated that the Act suffers from structural weaknesses: a truncated rights framework, blanket state exemptions without proportionality, a regulator lacking independence, minimal corporate obligations, weak enforcement mechanisms and inadequate alignment with global standards such as the GDPR. These deficiencies collectively undermine the protection of privacy as a fundamental right under Article 21 of the Constitution and compromise India's credibility in the global digital economy.

The way forward is clear. India must reform the DPDP Act to embed proportionality and judicial oversight, strengthen individual rights to include portability, objection and algorithmic transparency, ensure the independence of the Data Protection Board, impose robust obligations on corporations and align with GDPR to enable trusted cross-border data flows. These reforms are not merely technical adjustments; they are constitutional imperatives and democratic

---

<sup>1</sup> (2017) 10 SCC 1

necessities. Without them, privacy protections risk becoming symbolic rather than substantive, leaving citizens vulnerable to both state surveillance and corporate exploitation.

Privacy is the cornerstone of democracy in the digital age. It safeguards autonomy, dignity and liberty, ensuring that individuals remain free and empowered in a world increasingly shaped by data. It is also an economic imperative, fostering trust in digital ecosystems and enabling global integration. For India to uphold its constitutional values and global aspirations, privacy must be placed at the heart of its digital governance framework.

The closing reflection is therefore both a warning and a call to action: unless India reforms the DPDP Act to meet constitutional and global standards, it risks weakening democracy, eroding trust and diminishing its global standing. But with bold reforms, India has the opportunity to build a rights-based data protection regime that safeguards democracy, empowers citizens and positions itself as a leader in the global digital economy

Privacy is the cornerstone of democracy in the digital age. It protects autonomy, dignity and liberty, ensuring that individuals remain free and empowered in a world increasingly shaped by data. For India to uphold its constitutional values and global credibility, privacy must be placed at the heart of its digital governance framework. The way forward lies in building a rights-based data protection regime that safeguards democracy, empowers citizens and positions India as a leader in the global digital economy.