THE DIGITAL SHIELD OR THE SURVEILLANCE SWORD? UNMASKING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

by

Balpreet Kaur Bhatti,
&
Akshat Hegde.

Abstract-

In an era where data is power and surveillance lurks behind digital convenience, the Digital Personal Data Protection Act, 2023 emerges as India's most ambitious attempt to regulate personal data. But beneath its promises of empowerment and privacy lies a stark paradox: while the law equips citizens with new rights, it simultaneously grants the State sweeping exemptions, unchecked access, and opaque authority. This research dissects the DPDPA's evolution, its core provisions, and the constitutional tensions it creates—juxtaposing its protective aspirations against its potential to legitimize mass surveillance. Drawing comparisons with global standards and earlier drafts, the paper asks the central question: Is the DPDPA truly a digital shield safeguarding Indian citizens, or a surveillance sword veiled in legalese? As India races to become a global digital powerhouse, the answer will determine whether privacy remains a constitutional cornerstone—or a casualty of national ambition. The battle for India's digital soul has just begun.

THE DIGITAL SHIELD OR THE SURVEILLANCE SWORD? UNMASKING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

I. INTRODUCTION[1]

In the digital age, personal data has emerged as both an asset and a vulnerability. With India's rapid technological transformation—driven by mass smartphone adoption, digital payments, Aadhaar-based governance, and expanding internet penetration—the volume of personal data being collected, stored, and processed has reached unprecedented levels. This explosion of digital footprints has brought privacy concerns to the forefront, especially in a country where legal safeguards for data protection have long lagged behind technological innovation.

The Supreme Court's recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy (2017)* catalyzed the demand for a comprehensive data protection framework. After years of deliberation, revisions, and political scrutiny, the Digital Personal Data Protection Act, 2023 (DPDPA) was enacted to regulate the collection and use of personal data by both state and private entities. It introduces a rights-based approach to data governance while also allowing significant exemptions for government agencies.

This research critically examines the DPDPA's dual nature—is it a digital shield protecting citizens' informational autonomy, or a legal sword enabling unchecked state surveillance? The Act's language, structure, and enforcement mechanisms raise pivotal questions about transparency, accountability, and the future of privacy in India.

II. HISTORICAL DEVELOPMENT AND LEGISLATIVE ORIGINS[2]

The Act was born out of growing concerns about informational autonomy, data sovereignty, and the need for a strong legal framework in the face of the digital economy's rapid expansion. India's lack of a comprehensive data protection regime forced the country to rely on a number of provisions found in laws like the Information Technology Act, 2000 (IT Act), especially

[1] The Digital Personal Data Protection bill, 2023, PRS Legislative Research (2025), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023. (last visited Jun 4, 2025).

[2] Ishwar Ahuja, Digital Personal Data Protection Act, 2023 – a brief analysis Bar and Bench - Indian Legal news, https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis. (last visited Jun 4, 2025).

Section 43A and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. However, in light of changing technological realities, these provisions were judged insufficient. A comprehensive data protection law was codified as a result of the Supreme Court's historic ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India [(2017) 10 SCC 1]*, which unanimously affirmed the right to privacy as a fundamental right under Article 21 of the Constitution. The Justice B.N. Srikrishna Committee was established as a result, and in 2018 it submitted its report and draft Personal Data Protection Bill. However, after being criticized for their operational viability, lack of clarity, and governmental overreach, later versions—such as the Personal Data Protection Bill, 2019 and the Data Protection Bill, 2021—were either withdrawn or referred to parliamentary committees.

The Act's Main Goals and Declared Intent[3]

The Act's main legislative goal is 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 data for lawful purposes," according to the Statement of Objects and Reasons appended to the Act. The following is an expression of the Act's primary goals:

1. *Recognition of Data Principals' Rights:* The Act upholds the rights of people, known as Data Principals, to access, amend, delete, and file a grievance pertaining to their personal information. This creates enforceable statutory rights and is consistent with Article 21 constitutional protections.
2. *Establishment of Obligations on Data Fiduciaries:* As Data Fiduciaries, entities that decide how and why to process data are subject to obligations like consent-based processing, data minimization, purpose limitation, and the implementation of organizational and technical safeguards.
3. *Consent Architecture and Notice Framework:* Prior to processing, free, explicit, informed, unconditional, and unambiguous consent is a crucial component. In order to ensure transparency and facilitate well-informed decision-making, notice must be given in plain, unambiguous language.
4. *The Data Protection Board of India (DPBI):* The Data Protection Board of India (DPBI) was established by the Act as a quasi-judicial regulatory body to decide cases

[3] Ishwar Ahuja, Digital Personal Data Protection Act, 2023 – a brief analysis Bar and Bench - Indian Legal news, https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis. (last visited Jun 4, 2025).

of non-compliance, enforce sanctions, and monitor the application of the Act's provisions.

5. *Cross-border Data Transfers:* The Act strikes a balance between data localization and international interoperability by permitting cross-border data transfers to jurisdictions that have been notified by the Central Government. The statute emphasizes proportionality and deterrence by instituting a tiered penalty system that can reach ₹250 crore for specific infractions. By providing a framework for voluntary undertakings and corrective action, it promotes voluntary compliance.
6. *Focus on Digital-Only Data:* It is noteworthy that the DPDPA only covers digital personal data, regardless of whether it was gathered offline or online and then converted to digital form. This is different from previous versions that contained non-digital personal information.
7. *Protecting State Interests and Public Order:* Although this has raised concerns about possible executive overreach, the Act provides exemptions for State instrumentalities, specifically for national security, public order, and legal compliance under any existing law.

A fundamental change in India's data governance framework is represented by the DPDPA, 2023. It aims to achieve a balance between individual liberty, technological advancement, and sovereign interests. It is based on constitutional principles and responsive to international data protection standards (like the GDPR). The way it is implemented will have a significant impact on how India's digital rights framework develops over the next ten years.

III. KEY PROVISIONS OF THE DPDPA, 2023[4]

A. Scope and Applicability

The Digital Personal Data Protection Act, 2023 is designed to apply universally to entities handling digital personal data within India and, in certain cases, even beyond its borders. It governs the processing of digital personal data—whether collected online or digitized later—from individuals in India. The Act applies to:

- Individuals and Organizations within India processing personal data digitally.
- Government Bodies, which are major data processors in India, especially through welfare schemes and digital identity systems like Aadhaar.

[4] The Digital Personal Data Protection bill, 2023, PRS Legislative Research (2025), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023. (last visited Jun 4, 2025).

- Foreign Entities, if they process personal data in connection with offering goods or services to individuals within India.

The Act defines "personal data" as any data about an individual who is identifiable by or in relation to such data. It covers digital personal data only, excluding offline and anonymized data. Additionally, the DPDPA is technology-agnostic and sector-neutral, applying across industries, whether fintech, healthcare, e-commerce, or governance platforms.

B. Principles Of Data Processing[5]

The DPDPA incorporates globally recognized seven foundational principles of data processing, inspired by instruments like the GDPR:

- *Lawfulness:* Processing must be based on free, informed, and specific consent or legitimate use.
- *Purpose Limitation:* Data can only be used for the purpose specified at the time of collection.
- *Data Minimization*: Only data that is necessary for the specified purpose must be collected.
- *Accuracy:* Data must be accurate and kept up-to-date to the extent necessary.
- *Storage Limitation:* Data must not be retained longer than required.
- *Integrity and Confidentiality:* Reasonable safeguards must be taken to ensure security of personal data.
- *Accountability:* Data Fiduciaries must be accountable for compliance and have mechanisms in place to demonstrate it.

These principles form the ethical and operational backbone of the Act, seeking to enhance trust in digital governance.

C. Rights of Data Principals

The Act empowers individuals—termed Data Principals—with significant rights, modeled loosely on international norms:

- *Right to Access:* To obtain information on what personal data is being processed, the purpose, and the identity of data fiduciaries.

[5] The Digital Personal Data Protection bill, 2023, PRS Legislative Research (2025), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023. (last visited Jun 4, 2025).

- *Right to Correction and Erasure:* To correct inaccurate or outdated data and request deletion once the purpose is fulfilled.
- *Right to Restrict or Object:* To limit the processing of personal data in certain contexts.
- *Right to Data Portability:* To receive data in a structured, commonly used digital format.
- *Right to Nominate:* To nominate another person to exercise rights in case of death or incapacity.

These rights are not absolute and are subject to lawful processing by the State under legitimate grounds, raising debates on the balance between citizen empowerment and State prerogatives.

D. Obligations of Data Fiduciaries[6]

- Entities processing data—called Data Fiduciaries—bear key responsibilities under the Act. These include:
- *Consent Requirements:* Data must be processed only after obtaining valid, free, specific, informed, and unambiguous consent. Consent must be easily revocable.
- *Security Safeguards:* Fiduciaries must implement reasonable security practices to protect against data breaches, unauthorized access, and misuse.
- *Breach Notification:* Mandatory reporting of personal data breaches to both the Data Protection Board and affected Data Principals.
- *Data Deletion:* Once the purpose of processing is fulfilled or consent is withdrawn, data must be deleted unless retention is legally required.

Further, entities classified as Significant Data Fiduciaries (SDFs)—based on factors like data volume, sensitivity, and risk—have enhanced obligations, including conducting Data Protection Impact Assessments (DPIAs), periodic audits, and appointing a Data Protection Officer (DPO).

E. Special Provisions

The Act contains tailored provisions for certain sensitive categories:

- *Children's Data:* Processing of personal data of children (defined as individuals under 18) requires verifiable parental consent. Data Fiduciaries are barred from tracking, profiling, or behavioural advertising targeted at children.

[6] CS Isha Deshwal, Digital Personal Data Protection Act, 2023: Key features and implications for data privacy in India LexComply Blog (2024), https://lexcomply.com/blog/digital-personal-data-protection-act-2023-key-features-and-implications-for-data-privacy-in-india/. (last visited Jun 4, 2025).

- *Exemptions for State and Certain Entities:* Under Section 17, the Central Government is empowered to exempt any agency from the Act's provisions in the interest of national security, public order, or for enforcing legal rights. This sweeping exemption, without robust judicial or parliamentary oversight, has sparked fears of potential misuse.
- *Voluntary Undertaking & Penalties:* Fiduciaries may provide a "voluntary undertaking" in case of minor violations, while significant breaches attract heavy penalties—up to ₹250 crore.

In essence, the DPDPA, 2023 introduces a structured framework for managing personal data in the digital economy. However, the extent to which its provisions empower citizens versus enabling government oversight remains at the heart of ongoing legal and policy debates.

IV. THE DIGITAL SHIELD: BENEFITS AND DEFENSES UNDER THE 2023 DPDPA[7]

A major piece of legislation that establishes a thorough framework for the protection of digital personal data in India is the Digital Personal Data Protection Act, 2023 (henceforth referred to as "the Act" or "DPDPA"). It aims to create a legitimate, rights-based, and accountable system of data governance that strikes a balance between the operational needs of data processors (Data Fiduciaries) and the privacy rights of individuals (Data Principals).

A. Individual Empowerment via Expanded Rights

The statutory recognition and enforcement of the Data Principal's rights is a fundamental component of the DPDPA. These rights give people the ability to decide how their personal information is gathered and processed. Important rights consist of:

1. *Right to Information Access:* Data Principals are entitled to information from Data Fiduciaries about the types of personal data that are processed, why they are processed, and what kinds of data are processed.
2. *Right to Correct and Erasure:* Subject to the legitimate interests of the Data Fiduciary, individuals have the right to request that inaccurate data be corrected and that personal data that is no longer required or unlawfully processed be erased.
3. *Right to Grievance Redressal:* Under the Act, each Data Fiduciary must set up a grievance redressal procedure and reply to complaints within a fair amount of time.

[7] CS Isha Deshwal, Digital Personal Data Protection Act, 2023: Key features and implications for data privacy in India LexComply Blog (2024), https://lexcomply.com/blog/digital-personal-data-protection-act-2023-key-features-and-implications-for-data-privacy-in-india/. (last visited Jun 4, 2025).

4. *Right to Nominate:* Under a new clause, people can designate a substitute to carry out their rights in the event of their demise or incapacity.

B. Data Fiduciary Responsibilities and Accountability Systems[8]

Data Fiduciaries—those who choose the methods and purposes of data processing—are subject to stringent compliance requirements under the Act. Among their responsibilities are:

1. *Lawful Processing Based on Consent:* Only with the Data Principal's valid consent or in accordance with certain "legitimate uses" may data be processed.
2. *Data Minimization and Purpose Limitation:* Fiduciaries are required to gather only the information that is required and process it for the specified purpose.
3. *Security Measures:* To stop data breaches, reasonable security measures must be put in place. The fiduciary is required to notify the affected parties and the Data Protection Board of India in the event of a breach.

C. The Function and Authority of the Indian Data Protection Board (DPBI)

The Data Protection Board of India (DPBI), a regulatory body with adjudicatory and enforcement powers, is established by the Act. The Board has the authority to:

1. *Investigate Complaints:* It may start a case on its own initiative or in response to a complaint.
2. *Penalties:* Depending on the type and seriousness of the infraction, the Board may levy fines of up to ₹250 crore for non-compliance.
3. *Issue Instructions:* It might instruct Data Fiduciaries to implement remedial actions and guarantee adherence in the future.

Although the Board's structural independence has been contested because of the central government's role in appointments, its quasi-judicial nature guarantees independent oversight.

D. Enforcement and Redress of Grievances

A two-tiered enforcement model is established by the DPDPA:

1. *Internal Mechanism:* Effective grievance redress systems must be maintained by data fiduciaries.

[8] CS Isha Deshwal, Digital Personal Data Protection Act, 2023: Key features and implications for data privacy in India LexComply Blog (2024), https://lexcomply.com/blog/digital-personal-data-protection-act-2023-key-features-and-implications-for-data-privacy-in-india/. (last visited Jun 4, 2025).

2. *Regulatory Oversight:* Unresolved complaints may be brought before the DPBI, which is empowered by law to make decisions.

The Act also includes provisions for voluntary undertakings, which enable organizations to acknowledge their mistakes and suggest solutions, thereby decreasing adversarial proceedings and encouraging a compliance culture.

Overall, by requiring fiduciary responsibility, creating institutional oversight, and giving individuals enforceable rights, the DPDPA framework provides strong data protection. Although its effectiveness will be tested in practice, the Act offers a solid legal basis for protecting digital personal data in India.

V. THE SURVEILLANCE SWORD: CRITICISMS AND CONCERNS[9]

While the **Digital Personal Data Protection Act, 2023 (DPDPA)** is hailed as a landmark legislation, it has been sharply criticized for granting **broad exemptions to the government**, thereby compromising the very privacy it claims to protect.

A. Broad Exemptions for Government

One of the most contentious aspects of the Act is *Section 17(2)* (often compared with Section 36 and Rule 22 of earlier drafts), which empowers the Central Government to *exempt any "instrumentality of the State"* from complying with key provisions of the Act. These include requirements such as obtaining consent, adhering to data processing principles, and honoring the rights of data principals.

Such exemptions can be issued *"in the interests of sovereignty, integrity, security of the State, public order, or preventing incitement to any cognizable offence."* However, these grounds are undefined, overbroad, and subjective, creating potential for misuse. There is no judicial or independent oversight, and such notifications are shielded from challenge under the usual checks and balances of administrative law.

Moreover, *Rule 22 (when notified)* is expected to allow government agencies to demand personal data without the knowledge or consent of individuals, bypassing basic data protection standards under the guise of "legitimate use."

[9] Drawbacks and criticisms of the Digital Personal Data Protection Act, 2023, Lex Locum, https://www.lexlocum.in/drawbacks-and-criticisms-of-the-dpdp-act-2023. (last visited Jun 4, 2025).

B. Potential for Mass Surveillance[10]

These provisions create a legal infrastructure for mass surveillance. By failing to define terms like "public order" or "security of the state," the Act leaves room for interpretive abuse, potentially targeting dissent, whistle-blowers, journalists, or minority groups. The absence of parliamentary scrutiny or judicial review in these exemptions allows unfettered access to citizen data, reminiscent of concerns raised in the *Pegasus spyware scandal* and surveillance practices uncovered by investigative reports.

Unlike many global data protection regimes, the DPDPA *does not mandate a "necessity and proportionality" test,* which was firmly emphasized by the Supreme Court in *Puttaswamy (2017)*. This omission allows the state to prioritize national security over individual liberties without meaningful justification or transparency.

C. Impact on Privacy and Fundamental Rights

The DPDPA's surveillance-friendly architecture directly contradicts the principles laid down in *Justice K.S. Puttaswamy v. Union of India*, where the Court declared that any infringement of privacy must satisfy the *tests of legality, necessity, and proportionality*. The Act, however, fails to codify these constitutional safeguards.

Furthermore, the lack of an independent Data Protection Authority (as initially proposed in earlier drafts) undermines the constitutional promise of informational autonomy. The *Data Protection Board of India*, as per the 2023 Act, is functionally controlled by the Executive—raising doubts about its impartiality and independence.

This setup could legitimize unchecked surveillance under the garb of national security and dilute the fundamental right to privacy into a privilege controlled by executive discretion.

D. Transparency and Accountability Deficits

Another significant concern is the erosion of public oversight. The DPDPA excludes personal data from the ambit of the *Right to Information Act, 2005*, potentially weakening transparency in public administration. *Section 8(1)(j) of the RTI Act* previously allowed access to personal data of public officials when it was linked to public interest; this balance is now disturbed.

[10] Digital Personal Data Protection Act, 2023 – key highlights, azb (2023), https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/. (last visited Jun 4, 2025).

Moreover, the Act does not provide for independent audits of state surveillance programs, parliamentary oversight, or real-time accountability mechanisms for misuse of exemptions. This opacity risks creating a surveillance state under the veneer of digital governance.

VI. COMPARATIVE ANALYSIS[11]

A. Comparison with Previous Drafts

The *2018 and 2019 Personal Data Protection Bills* (based on the Justice B.N. Srikrishna Committee's recommendations) provided for:

- A robust, independent Data Protection Authority.
- Stronger restrictions on state surveillance.
- Mandatory data localization and data fiduciary categorization.
- Detailed safeguards for data transfer and cross-border processing.

In contrast, the *DPDPA, 2023* significantly dilutes these protections by:

- Removing the requirement of an independent authority.
- Granting sweeping exemptions to state agencies.
- Making data localization optional, subject to government discretion.
- Framing citizen rights more narrowly, often subject to ambiguous "legitimate use" clauses.

B. Comparison with Global Standards

When compared with the *EU's General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA):*

Feature	GDPR	CCPA	DPDPA, 2023
Independent regulator	Yes	Yes	No

[11]The Digital Personal Data Protection Act, 2023 ..., https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf. (last visited Jun 4, 2025).

Surveillance safeguards	Strong	Moderate	Weak
Right to be forgotten	Explicit	Limited	Vague
Consent framework	Explicit & revocable	Opt-out system	Limited scope
Judicial oversight of exemptions	Yes	Yes	No

Unlike the GDPR, which allows exemptions only under strict legal and constitutional conditions, the DPDPA relies on executive notifications, devoid of mandatory review mechanisms. This makes India's law more state-centric and less citizen-focused, raising alarms among privacy scholars and civil liberties advocates.

VII. IMPLICATIONS AND FUTURE DIRECTIONS[12]

A. Impacts on Businesses, Civil Society, and Citizens

For businesses, the Act brings regulatory clarity, especially for startups and tech companies. The relatively relaxed cross-border data transfer norms and reduced compliance burden (compared to GDPR) may boost ease of doing business.

However, civil society groups and digital rights activists warn that the Act may chill free speech, curb dissent, and enable profiling of individuals, particularly in politically sensitive contexts. Whistleblowers, journalists, and vulnerable populations could become targets under loosely defined surveillance justifications.

For ordinary citizens, the rights framework appears promising on paper but may prove illusory without enforcement mechanisms or legal remedies in cases of state overreach or corporate misuse.

B. Potential for Legal Challenges and Reform[13]

[12] Sarvesh Mathi, Fifteen major concerns with India's Data Protection Bill, 2023 MEDIANAMA (2023), https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/. (last visited Jun 4, 2025).

[13] Sarvesh Mathi, Fifteen major concerns with India's Data Protection Bill, 2023 MEDIANAMA (2023), https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/. (last visited Jun 4, 2025).

The Act may face **constitutional challenges** on multiple grounds:

- Violation of Article 21 (Right to Privacy)
- Absence of proportionality and necessity tests
- Lack of judicial oversight in executive exemptions
- Failure to ensure independence of regulatory authorities

Public interest litigations could revisit the *Puttaswamy* standards and test the Act's compliance with the Constitution. There is also a growing chorus for parliamentary review, especially of *Section 17*, to restore public trust.

C. Recommendations for Strengthening the DPDPA

1. *Establish an Independent Data Protection Authority:* Modeled after GDPR's supervisory authorities with transparency and operational autonomy.
2. *Introduce Judicial Oversight of Surveillance Exemptions:* All requests for exemptions or access to personal data should be subject to judicial scrutiny or parliamentary review.
3. *Codify the "Necessity and Proportionality" Test:* Following the *Puttaswamy* judgment, these principles should be explicitly embedded in the Act.
4. *Ensure Transparency of Government Access Requests:* Through public reporting, redress mechanisms, and audit trails.
5. *Preserve RTI and Whistleblower Protections:* Amend the RTI carve-outs to prevent misuse and safeguard public interest disclosures.
6. *Widen and Strengthen Data Principal Rights:* Include stronger rights to explanation, objection to profiling, and access to human intervention in automated decisions.

The *Digital Personal Data Protection Act, 2023* reflects India's ambition to govern its digital economy and assert cyber sovereignty. But while the law aims to protect citizens' data, its expansive state exemptions and weakened accountability structures risk turning it into a tool for surveillance. Unless the Act is rebalanced with robust safeguards and independent oversight, it may not serve as a digital shield—but rather a surveillance sword cloaked in the language of protection.

VIII. CONCLUSION [14]

As a legislative safeguard for privacy, the Digital Personal Data Protection Act, 2023, supposedly strengthens the informational autonomy of Data Principals through codified rights and fiduciary obligations. However, the State's concurrently granted broad exemptions, particularly under Section 36 and Rule 22, along with its extensive surveillance powers without independent oversight, raise concerns about possible executive overreach. This contradiction threatens the constitutional sanctity of fundamental rights and creates a noticeable conflict with the Supreme Court's privacy jurisprudence. As a result, the DPDPA serves as a sword that permits state surveillance even as it establishes the fundamental framework for data governance. Judicial review, strong oversight procedures, and legislative improvement to balance privacy safeguards with sovereign requirements are necessary for the Act's continued effectiveness.

[14] CS Isha Deshwal, Digital Personal Data Protection Act, 2023: Key features and implications for data privacy in India LexComply Blog (2024), https://lexcomply.com/blog/digital-personal-data-protection-act-2023-key-features-and-implications-for-data-privacy-in-india/. (last visited Jun 4, 2025).

IX. References

The Digital Personal Data Protection bill, 2023, PRS Legislative Research (2025), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023. (last visited Jun 4, 2025).

What data does the India Digital Personal Data Protection act 2023 safeguard?: Data Protection in India, https://secureprivacy.ai/, https://secureprivacy.ai/blog/india-digital-personal-data-protection-act-2023-guide-protected-data. (last visited Jun 4, 2025).

The Digital Personal Data Protection Act, 2023 ..., https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf. (last visited Jun 4, 2025).

CS Isha Deshwal, Digital Personal Data Protection Act, 2023: Key features and implications for data privacy in India LexComply Blog (2024), https://lexcomply.com/blog/digital-personal-data-protection-act-2023-key-features-and-implications-for-data-privacy-in-india/. (last visited Jun 4, 2025).

Drawbacks and criticisms of the Digital Personal Data Protection Act, 2023, Lex Locum, https://www.lexlocum.in/drawbacks-and-criticisms-of-the-dpdp-act-2023. (last visited Jun 4, 2025).

Ishwar Ahuja, Digital Personal Data Protection Act, 2023 – a brief analysis Bar and Bench - Indian Legal news, https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis. (last visited Jun 4, 2025).

Sarvesh Mathi, Fifteen major concerns with India's Data Protection Bill, 2023 MEDIANAMA (2023), https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/. (last visited Jun 4, 2025).

Digital Personal Data Protection Act, 2023 – key highlights, azb (2023), https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/. (last visited Jun 4, 2025).