2026 Volume: 02 Issue: 06 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-26

A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: CHALLENGES AND OPPORTUNITIES

***Manjit Singh**

LL.M. (Master of Laws), University Institute of Legal Studies (Department of Law), Chandigarh University, Mohali, Punjab, India.

Article Received: 23 April 2026
Article Revised: 13 May 2026
Published on: 02 June 2026

***Corresponding Author: Manjit Singh**
LL.M. (Master of Laws), University Institute of Legal Studies (Department of Law), Chandigarh University, Mohali, Punjab, India.

DOI: https://doi-doi.org/101555/ijrpa.9540

ABSTRACT

The rapid expansion of the digital economy and the increasing collection, processing, and transfer of personal data have raised significant concerns regarding privacy, data security, and individual rights. In response to these challenges, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), marking a significant step toward establishing a comprehensive legal framework for the protection of personal data. The Act seeks to balance the right to privacy of individuals with the legitimate need of the State and private entities to process personal data for lawful purposes. It reflects India's commitment to strengthening data governance while promoting innovation and digital transformation.

This research paper critically examines the Digital Personal Data Protection Act, 2023, with a particular focus on its key provisions, implementation challenges, and potential opportunities. The study analyzes the legislative background of the Act, including the influence of the landmark judgment in *Justice K.S. Puttaswamy v. Union of India*, which recognized privacy as a fundamental right under the Constitution of India. The paper evaluates important aspects of the Act such as consent-based data processing, rights and duties of data principals, obligations of data fiduciaries, cross-border data transfers, grievance redressal mechanisms, and the establishment of the Data Protection Board of India.

While the Act represents a progressive development in India's digital regulatory framework, several concerns remain regarding its practical implementation. The research highlights issues such as broad exemptions granted to government agencies, the absence of strong safeguards against surveillance, limited provisions relating to children's data, ambiguity in certain definitions, and challenges associated with enforcement and institutional capacity.

Furthermore, concerns regarding transparency, accountability, and the effectiveness of remedies available to data principals are critically assessed. The paper also examines the extent to which the Act aligns with international standards, particularly the European Union's General Data Protection Regulation (GDPR), and identifies areas where further legislative refinement may be necessary.

At the same time, the Digital Personal Data Protection Act, 2023, presents significant opportunities for enhancing trust in digital services, promoting responsible data governance, attracting investment in the digital economy, and strengthening cybersecurity practices. By providing a structured legal framework for personal data protection, the Act has the potential to foster greater confidence among citizens, businesses, and international stakeholders.

The study adopts a doctrinal research methodology based on the analysis of statutes, judicial decisions, government reports, policy documents, and scholarly literature. It concludes that while the DPDP Act, 2023, constitutes a landmark reform in India's data protection landscape, its long-term success will depend upon effective implementation, institutional independence, regulatory clarity, and continuous adaptation to emerging technological challenges. The paper recommends strengthening oversight mechanisms, enhancing transparency, and ensuring a balanced approach that safeguards both individual privacy rights and the objectives of digital governance.

KEYWORDS: Digital Personal Data Protection Act, 2023; Data Privacy; Right to Privacy; Data Governance; Data Protection Board of India; GDPR; Digital Economy; Cybersecurity.

1.1 INTRODUCTION

India’s dedication to ensuring privacy and the use of trusted data has gone from being merely a policy goal to a full-blown statutory framework with the establishment of the “Digital Personal Data Protection Act, 2023”. The law recognizes this as a dual imperative. On the one hand, it protects the individual’s right to privacy of personal data and, on the other hand, it allows the processing of data for lawful purposes. Accordingly, the act finds a balance between individual freedom and the economic vibrancy of a digital economy characterized by platformization, widespread analytics, and the use of digital public infrastructure. The law serves as a baseline that replaces sectoral patchworks, makes the key actors’ roles more transparent, and creates a Board that has the authority to investigate and punish. Moreover, it reforms the traditional aspects of Indian digital regulation by linking with the “Information Technology Act, 2000”, and the “Right to Information Act, 2005”, as well as co-existing with

other laws via a non-deduction clause. The paper, therefore, through a doctrinal lens, analyses the legislative choices, the design of the enforcement mechanism, and the pathways for compliance, recognizing that aspects such as consent, legitimate uses, children's safeguards, and cross border restrictions define the practical tradeoffs both for the protection of rights and for data driven growth. The investigation is based on the statutory provisions, without looking at case law, and it also takes into account the comparative frames. Finally, it identifies the directions for rulemaking, sectoral coherence, and institutional capacity so that enforcement can be principled, predictable, and proportionate.[1]

1.2 CONSTITUTIONAL AND DOCTRINAL BACKDROP

Privacy is among the most significant rights in India and is protected by laws that are applicable both at the state and central levels and in the public and private sectors. A data governance model based on rights would need a law that translates constitutional principles into operational tasks, institutional checks, and remedies. The statement of the objects and the structure of the statute reflect a move towards purpose specification, transparent processing, and redress, while also recognizing some legitimate uses for state delivery and emergencies. The law uses proportionality as its guiding principle, which requires that the processing be legal and based on a statute, that the necessity be linked to a specified purpose, and that the safeguards reduce the risks and prevent overreach. The non derogation clause ensures that the Act cooperates with other laws, whereas a conflict clause maintains the Act's primacy in case of inconsistency, a

---

[1] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 164 (HarperCollins India, Noida, 1st edn.,

Design that acknowledges simultaneous regulatory regimes and regulates fragmentation. These elements bring the law into line with reality by linking rules on consent, retention, and security to exact sections and giving a specialized Board the authority to apply proportional penalties that take into account harm, repetitiveness, and mitigation.[2]

1.2.1 Evolution of Privacy Jurisprudence

Indian privacy jurisprudence has been transformed through the years starting from a minimal understanding of physical intrusion to a comprehensive account of informational self-determination and decision-making independence. The legislative response is in line with this understanding without depending on judge made remedies for everyday processing. Rights are

legislated in terms of statutory access, correction, erasure, grievance redress, and nomination, and individuals are also entrusted with responsibilities to refrain from impersonation and making frivolous complaints. The organization of the Act is also indicative of a change from an ad hoc executive policy to an adjudicatory mechanism with definite procedures and graduated penalties. This institutional design is a translation of constitutional values into more or less fixed rules that data fiduciaries and state entities can understand and abide by while the conflict clause keeps the primacy during the overlap with other laws. Privacy is made practical by the help of notice, consent, purpose limitation, storage limitation, security, and accountability, among others, each being a legal duty that the Board can enforce by way of investigation, mediation, voluntary undertakings, and imposition of penalties as specified in the Schedule.

1.2.2 Doctrinal Principles for Analysis

Throughout this analysis, the criteria for the evaluation are the principles of legality, necessity, proportionality, and procedural safeguards. Legality requires that the grounds for the processing of data be clearly stated and that the notices be understandable. Necessity requires that there be a real connection between the specified purpose and the personal data that is being sought. Proportionality requires that the least intrusive means of the effective alternatives be chosen, with children and high-risk processing being given more scrutiny. Procedural safeguards require, among other things, transparent grievance mechanisms, reasoned orders, and avenues for appeal. The Act reflects these principles by linking processing to “consent under Section 6” or “certain legitimate uses under Section 7”, by requiring “notice under

[2] Anirudh Burman, "Understanding India's New Data Protection Law", *available at:* https://carnegieendowment. org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited on October 25,

Section 5”, by stipulating “reasonable security safeguards and breach intimation under Section 8”, and by providing a “appeal to the Appellate Tribunal under Section 29” with penalty factors that are quantified in “Section 33” as the way forward. These textual anchors allow for the principled application of the law in different facts.[3]

1.3 SCOPE AND DEFINITIONS UNDER THE ACT

Understanding scope and definitions helps to determine the compliance level and system structure. The Act is applicable to the processing of digital personal data of individuals within

India, if such data is either collected digitally or digitized later. The Act has an extraterritorial effect and the processing outside India is covered if it is connected to the offering of goods or services within India. The Act does not cover the personal or domestic processing of data and the publicly available personal data that is made available by the data principal or is under a legal obligation. The definitions point out that a "Data Principal" is the identified individual, a "Data Fiduciary" is the one who determines the purpose and means, the "Data Processor" is the one who acts on behalf, and the "Consent Manager" is the one that offers an interoperable user facing interface. A "Significant Data Fiduciary" is a notified category subject to enhanced obligations and the "personal data breach" definition covers the cases of unauthorized processing and incidents that compromise confidentiality, integrity, or availability. These terms are used to define roles, trigger rights and obligations, and specify the route for redress; thus, they reduce the level of uncertainty.

1.3.1 Statutory Definitions

Definitions set the parameters for the language of governance. The Act specifies "Data Principal" as the inclusion of parents or lawful guardians of children and lawful guardians of persons with a disability, "Data Fiduciary" as the determinant of the purpose and means, and "Data Processor" as the agent carrying out processing. "Consent Manager" needs to be registered with the Board and should offer an accessible, transparent, interoperable platform for giving, managing, reviewing, and withdrawing consent. "Personal data" is any information about an identifiable individual, and "processing" covers the full life cycle such as collection, use, disclosure, restriction, and erasure when it is automated in whole or in part. "Significant Data Fiduciary" is any class notified by the Central Government under "Section 10", linking enhanced governance to risk indicators. When read together, these definitions distinguish the control of decision making from the execution of service and thus the correct counterpart can be identified when rights are exercised or duties are imposed.[4]

1.3.2 Applicability and Exclusions

The application of the law depends on the material form and purpose. The law is applicable to any digitally recorded personal data, and it applies to digitized personal data that were originally collected offline. The law does not apply to personal or domestic use, e.g., a private contact list, and it does not apply to personal data that have been made publicly available by the data subject or by another person under a legal obligation. These exclusions serve to limit the intervention in the use of households and prevent the creation of copies when the law already provides for the publication, e.g., regulatory disclosures. For regulated processing, the

law provides for a lawful purpose and grounds by consent or certain legitimate uses, with examples that clarify practice. The framework acknowledges that not every revelation of a person's information deserves regulatory intervention, but it extends the coverage to those cases where an entity systematically processes digital personal data for a specified purpose. The method limits the number of border cases while keeping a wide baseline for organizational processing.

1.3.3 Territorial Reach

Territorial reach employs an effects-based test that is in line with modern extraterritorial principles. The Act is related to the processing of data outside India if it is connected with activities of offering goods or services to data principals in India. Such a formulation captures cross border digital services, apps, and platforms that target Indian users regardless of the physical location of the server. It closes the gaps that otherwise arise in cross border cloud and outsourcing arrangements and ensures that duties and redress remain meaningful for Indian data principals. For implementation, the Board is empowered to issue directions and, in certain situations, the Central Government is authorized to give the order of blocking access to information which is of general public interest after the hearing and reasons recorded. Therefore, statutory design constitutes a combination of applicability, inquiry, and enforcement levers to make extraterritoriality feasible.

1.4 RIGHTS OF DATA PRINCIPALS

The law delineates rights as actionable claims accompanied by procedural routes. These rights encompass receiving a summary of one's personal data being processed, knowing the data fiduciaries and processors with whom the data is shared, and also other processing related information. Correction and erasure rights function where consent is the basis, and they are limited by legal retention and specified purposes. The provision for grievance redressal should be there in a manner which is very easy to access, along with the timelines for the response, and the right to appoint another person in case of death or incapacity thereby creating continuity. The obligations of the data principals are aimed at ensuring that there is reciprocity whereby impersonation is prohibited, suppression of material information for identity proofs and the making of frivolous complaints. Individually, these rights and responsibilities constitute the independence of the individual without disabling legitimate processing or public delivery. The Act constructs these routes as commands of the statute and not as aspirational statements, thus, it is direct invocation and Board oversight that is enabled.[5]

1.4.1 Notice, Access, and Grievance

Notices are documents that go with or come before consent requests and have to indicate the personal data and purposes, the ways in which rights can be exercised, and the ways how a complainant can address the Board. Access rights allow the data principal to get an extract of the data being processed, the identities of sharing counterparties, and other information as prescribed. Complaint redress should be available without any difficulty through the data fiduciary or a consent manager and must be responded to within the given timelines. The communication may be opened in English or any of the languages listed in the Eighth Schedule, and if it applies, the contact information of a Data Protection Officer or a person authorized must be given. These textual requisites serve as an interface for transparency in standard forms that systems can execute, and they constitute a basis for fair processing over time.

1.4.2 Correction and Erasure

A data principal may request correction, completion, updating, and erasure of their personal data if the processing is based on their consent, including consent for certain legitimate uses that refer to consent. Upon receiving a request for correction or completion or updating, the data fiduciary is obligated to correct inaccurate or misleading data, complete incomplete data, and update the data as necessary. Regarding erasure, the law associates the removal of data to

[5] Talat Fatima, *Cyber Crimes* 150 (Eastern Book Company, Lucknow, 1st edn., 2021).

The withdrawal of consent and the absence of legal necessity for retention and also indicates that requests should be made in the prescribed manner. The Act also provides that certain purposes may come to an end due to non-performance of the data principal for a prescribed period, which results in storage limitation. These calibrated triggers give more understanding to both individuals and organizations about the exact time when records have to be removed.[6]

1.4.3 Consent Withdrawal and Nomination

Consent should be able to withdrawn just as easily as it was given. The law specifies that withdrawal does not change the legality of the processing prior to consent, but at the same time it requires the fiduciary to stop the processing based on consent within a reasonable time and the processors to stop as well where there is no other lawful ground. The right to appoint another person makes it possible to continue the exercise of rights where the data subject is dead or disabled, with the disability being defined as unsoundness of mind or infirmity of the body. This combination guarantees that individual agency stays at the core while families or guardians are allowed to manage the records in a difficult situation. The withdrawal and

nomination becoming more formalized is pushing the systems to provide interoperable, logged and time bound workflows.

1.4.4 Duties of Data Principals

Duties as provided in the statute serve to moderate the rights of the data principals with the aspect of responsible use. Data principals when exercising their rights are obliged to comply with the laws that are in force. They should not, while giving personal data for a certain purpose, pretend to be someone else. In addition, they have to give correct information when providing identifiers or proofs issued by the State or its instrumentalities. They should not file a false or frivolous complaint with a data fiduciary or the Board, and in case of seeking correction or erasure, they should provide only authentic information that can be verified. Violation of these duties leads to a penalty of up to ten thousand rupees as per the Schedule. These duties limit system misuse, facilitate data quality, and save adjudicatory resources for real cases of harm, thus enhancing trust without limiting essential rights.

[6] Gaurav Thote, "Unravelling 'Consent' Under the Digital Personal Data Protection Act, 2023 — A Barrier to Data Principal Rights", *available at:* https://www.scconline.com/blog/post/2024/11/13/unravelling-consent-under-the-digital-personal-data-protection-act-2023-a-barrier-to-data-principal-rights/ (last visited on October 22, 2025).

1.5 OBLIGATIONS OF DATA FIDUCIARIES

At a minimum, fiduciaries have baseline duties that, through the life cycle, create accountability. Processing should be based on consent or a few legitimate uses, and in any case, the processing should be for a lawful purpose not contradicted by law. Notices should be understandable and in a simple language. Fiduciaries are required to install the suitable technical and organizational measures and to keep personal data which they have control over, including those data processed by processors, safe. Informing the Board about the breach and the affected data principals is obligatory. The requirement of storage limitation entails that the data should be removed in the case of the withdrawal of consent and when the specified purposes do not apply anymore, except for the retention that is mandated by law. Where applicable, fiduciaries should make available the contact details of the DPO and set up the efficient grievance mechanisms. The law extends these obligations to processors via the valid contracts and hence, assigns the responsibility of compliance to the fiduciary, thus ensuring

that the outsourcing of obligations is not weakened.[7]

1.5.1 Lawful Grounds and Consent Architecture

Theorem 4 provides the fundamental grounds for processing and when read along with section 6, it refers to consent and section 7 to certain legitimate uses. Consent should be free, specific, informed, unconditional, and unambiguous indicating a clear affirmative action and be limited to the personal data necessary for the specified purpose. The law establishes a "Consent Manager" as a registered, interoperable platform which is like a single point for issuing, managing, checking, and revoking consent. It requires that the language used be clear and also that there be an option to access notices and consent requests in English or Eighth Schedule languages. The Act stipulates that the withdrawal of consent should be as easy as the giving of consent. Such a layout is one of the ways through which the user is given real control while also allowing machine readable, standardized interfaces across services and sectors.

1.5.2 Purpose and Storage Limitation

The principle of purpose limitation is reflected in the notion of a "specified purpose" and the stipulation that only data necessary for that purpose should be processed. Storage limitation is also evident from the obligations to erase personal data upon withdrawal of consent and when it is reasonable to assume that the specified purpose is no longer served, however, it is subject to retention required by law. The law specifies that the designated purpose may be considered as no longer being served if the data subject does not contact the fiduciary for performance nor exercise rights for a certain time, thus, allowing the rules to determine inactivity periods by class of fiduciary or purpose. These articles drive the retention schedules, deletion workflows, and processor backflush procedures. In addition, they incentivize data minimization by linking the collection of fields to the purposes disclosed in the notices.[8]

1.5.3 Security Safeguards and Breach Response

Fiduciaries are required to put in place security measures that are reasonably adequate and at the same time protect any personal data that comes under their control either directly or through a processor. Besides that, they must also guarantee that the data used for making decisions or disclosures are complete, accurate, and consistent. When there is a personal data breach, the fiduciary is required to inform the Board and each affected data principal in the prescribed form and manner. These commands necessitate controlled documented vendor security oversight, incident response playbooks, and registries of processing. The obligation to report a breach goes along with sectoral incident reporting and thus allows for coordinated oversight. The

penalty bands in case of security lapses are quite significant, which, therefore, indicates that prevention and timely disclosure are at the core of the enforcement strategy. Together, these provisions constitute a set of enforceable expectations for confidentiality, integrity, availability, and breach transparency throughout the lifecycle.

1.5.4 Transparency, Recordkeeping, and Governance

Transparency should not only be limited to notices. Fiduciaries are required to make public the business contact information of the DPO if it is applicable and they have to support the effective grievance mechanisms. It is necessary to have contracts between processors and they should reflect the statutory duties. Risk based governance is visible through obligations that vary depending on the decision making, use and disclosures, therefore, it is required that there are assurances of completeness and consistency. In case of big ecosystems, recordkeeping should be able to follow consent, sharing counterparties, decision uses, retention events, and erasure confirmations in order to meet access and correction rights. The Act foresaw technical standardization through rules, such as formats for breach intimations, verifiable consent, and timelines for deeming purposes no longer served. Hence, governance becomes auditable and can be verified by machines, thus, it is more predictable for both regulated entities and the Board.[9]

1.5.5 Significant Data Fiduciary Toolkit

As per the Act, the Central Government is authorized to designate a "Significant Data Fiduciary" depending on criteria such as the volume and sensitivity of personal data, the risks to rights, and the effects on sovereignty, elections, security, and public order. Entities handling significant amounts of data are required to have a "Data Protection Officer" who is India based and answers to the Board of Directors or an equivalent governing body and is the contact point for grievances. They are required to appoint an independent data auditor to assess their compliance, carry out periodic "Data Protection Impact Assessments" and audits, and implement various other measures that may be prescribed. The present toolkit takes risk management as part of corporate governance, goes further to locate the senior roles as accountable, and makes it a feature of the organization independent oversight to manage the high-risk processing.

1.6 ENFORCEMENT AND REMEDIES

Enforcement mainly depends on a specialized regulator who has the powers of inquiry, mediation, and imposition of penalties. The Act defines the "Data Protection Board of India" as an independent entity with a corporate body, a perpetual succession, and a common seal. It

provides the constitution, appointments, the term of office, and disqualifications in the law and rules and characterizes members and staff as public servants. The Board may hold hearings on the internet, sign its decisions, and, with the prior consent of the person concerned, appoint officers and employees. It is also empowered to receive voluntary undertakings from the parties concerned, facilitate their mediation appointment, and impose money fines in case of major violation, after giving due opportunity of being heard to the concerned person. On Appeals, the matter is taken to the Appellate Tribunal. The Penalty amounts become a credit to the Consolidated Fund of India, and the Central Government can seek information and give directions under certain circumstances.

1.6.1 Data Protection Board of India

On notification, the Board's creation is formalized. It is a corporative body that can, among other things, buy property, enter into a contract, and sue or be sued. It will be notified by the

[9] Shoshana Zuboff, *The Age of Surveillance Capitalism* 210 (PublicAffairs, New York, 1st edn., 2019).

Central Government where the Board's headquarters are located. The Board comprises a chairperson and other Members as may be notified, appointed in the prescribed manner. The members must have the skills, honesty, and theoretical or practical knowledge of one or more of the following areas: data governance, dispute resolution, ICT, digital economy, law, regulation, or other related areas, and there must be at least one member who is a legal expert. The law provides for salaries, allowances, terms, and a ban on post-employment except with prior approval for a year. Among the disqualifications are insolvency, moral turpitude, incapacity, conflicting interest, and misuse of position. The features mentioned above, thus, form the basis of the Board's independence and its capacity to perform its adjudicatory functions.[10]

1.6.2 Penalties and Aggravating Factors

Monetary sanctions outlined in the Schedule may be enforced by the Board in case of a significant breach. In doing so, the Board should take into account the nature, gravity, duration, type of data affected, repetitive nature, gain realized or loss avoided, mitigation actions and timeliness, proportionality and deterrence, and the likely impact of penalties on the person alongside other factors. The Schedule establishes bands of up to 2.5 billion rupees for the security of the failure to take reasonable measures, up to 2 billion rupees for failure to notify breaches, up to 2 billion rupees for breach of children's obligations, up to 1.5 billion rupees for

breach by a Significant Data Fiduciary, and up to 50 million rupees for other provisions. A fine of up to ten thousand rupees may be imposed for breach of data principal duties.

1.6.3 Appellate Structure and Judicial Review

Any person who feels that they have been wronged by a Board order or direction can appeal to the "Appellate Tribunal". As defined in the "Telecom Regulatory Authority of India Act, 1997", it is the Telecom Disputes Settlement and Appellate Tribunal. Appeals should be made within sixty days, with a chance of condonation for a reasonable cause. After the hearing, the Tribunal may keep, change, or annul the order. The Tribunal decisions have the same effect as the ones of civil courts and the Tribunal can send the orders to the competent civil courts for the implementation of the orders. The Tribunal is supposed to be a digital office for appeals under the Act. Further appeals follow the TRAI Act route. Thus, this appellate framework not only provides a layer of external oversight but also allows for swift, digital by nature, adjudication.[11]

1.6.4 Redress for Data Principals

The law directs the handling of grievances to the data fiduciary or a consent manager as the first point of contact. The response time of the fiduciary or consent manager is limited to certain periods. Only after an employee has thoroughly checked this channel can he come to the Board. The Board can accept voluntary undertakings that prevent further proceedings on the same issue and can, if it deems it suitable, direct the parties to mediation. It also has the authority to caution and impose charges on the originators of false or frivolous complaints. This multi-tier layout is the main idea of a quick resolution close to the controller; thus, the adjudicatory bandwidth is saved for serious infringements and, at the same time, the access to a specialized regulator is ensured where disputes have not been resolved. It mirrors a calibrated approach to redress which is in harmony with proportionality and due process.

1.6.5 Transitional and Implementation Timelines

The law provisions will be enforced by a different date for each provision through a notification. According to the law, the Central Government has the authority to declare that a certain provision will not be applicable to fiduciaries or a class of them, i.e., startups for a period notified, considering the volume and nature of processing. In addition, the law provides for the State's exemption from processing under certain conditions and makes Special Provisions for cross border transfers through a limited jurisdictions approach. The formation of the Board, registration of consent managers, and notification of Significant Data Fiduciaries will, thus, mark the first compliance cycle. The penalty money is deposited in the Consolidated Fund of India. Besides, the law changes "Section 43A of the Information Technology Act,

2000" by deleting and replacing "Section 8(1)(j) of the Right to Information Act, 2005" to keep personal information protections intact during the transition.

1.7 SPECIAL REGIMES AND EXEMPTIONS

The Act establishes different calibrated regimes that adjust its overall duties and rights to sensitive contexts and sovereign functions. This multi layered approach is key to understanding how compliance will function in reality. The central point is a broad applicability rule, then exceptions are pointed out for personal or domestic use and data that has been made publicly available by the data principal or under a legal obligation. This keeps the law concentrated on significant risk. Subsequently, the document introduces a range of targeted exceptions for public order, national security, prevention detection investigation of offences, and legal claims. These are considered as statutory authorizations with a requirement of notification or lawful basis, in most cases, being embedded. When referred to the governance architecture, these carve outs do not remove accountability but change the location of it to specific legal regimes. At the same time, the general principles of purpose limitation, storage limitation, and security still constitute the baseline expectation for private actors processing digital personal data. The subsequent analysis delves into children's data, cross border transfers, state exemptions, research, and employment. It also links these areas to parallel obligations under sectoral and public law frameworks to demonstrate how the Act is harmonizing data protection with the concrete delivery needs and system safety. The framework is based on explicit provisions such as "Section 3" on scope, "Section 7" on certain legitimate uses, and "Section 17" on exemptions, which together establish the limits for these special regimes.[12]

1.7.1 Children and Age Assurance

Children's data is treated differently and given special protection based on a clear legal definition of a child as a person under the age of eighteen. This definition puts a very high standard for consent and safety even in areas such as educational technology, gaming, social media, and digital health. The Act provides for parental consent that can be verified for the processing of children's data and prohibits activities such as tracking, targeted advertising, or any other processing that may cause a harmful effect on the child's well-being. At the same time, these responsibilities are accompanied by the broader obligation of data fiduciaries to put in place reasonable safeguards, issue clear and understandable notices and ensure that consent is obtained from the user and is free, specific, informed, and unambiguous. Besides, the child interfaces are expected to meet the standards of clarity and accessibility. Practically speaking, controllers are required to set the age gate and verification in such a way that the latter is both

efficient and proportionate, thus, overcollection of identity proofs or perpetual retention should be avoided. The obligation to provide grievance redress and erasure options is still there, and the edtech and school systems should thereby parental dashboards and auditable consent trails for aligning their data flows that are interoperable with consent managers. This system is based on the definitions of "child" and the obligations linked with "consent" and "certain legitimate uses". The age limit is indicated in "Section 2(f)" while the parental representation is in "Section 2(j)".[13]

1.7.2 Cross Border Data Transfers

On the basis of principles, cross border data flows are allowed, with a mechanism for restricted jurisdictions, according to which the Central Government may notify countries or territories to which transfers are restricted. This policy move is contrary to the idea of a blanket localization rule and instead adopts a negative list that can be adjusted for national security and diplomatic reasons, while still allowing companies to organize global processing through contracts and technical safeguards. The statutory language refers to "Section 16" as the location of this design and connecting it to the rulemaking powers that can determine the way and the timing of the notifications. Until a negative list is in place, data fiduciaries should operate on the basis of purpose limitation, necessity, and security obligations, and maintain transfer registers and risk assessments in order to be able to provide evidence that processing overseas is still in line with lawful purpose and data minimization. If the processing is used to provide cross border digital services to residents of India, the extraterritorial clause of the Act brings those actors within the scope, if they target Indian data principals, as explained in "Section 3(b)". The outcome is an efficient system that facilitates trade and at the same time, retains the government's ability to control flows to regions with a high level of risk via notification.

1.7.3 State and Public Interest Exemptions

The Act recognizes that different functions of the government or public sectors which are of sovereign or public interest may need certain flexibilities, hence, it provides exemptions for processing that is necessary for the performance of the State or its instrumentalities of any function, for the enforcement of legal rights or claims, for prevention, detection, investigation, or prosecution of offences or cyber incidents, and for compliance with any judgment or decree. These carve outs are not a carte blanche. They function within the legal and purpose framework and can be interpreted in line with constitutional proportionality which requires suitability and minimal impairment where measures interfere with privacy. The literal wording of "Section 17(1)" lists the heads of exemption, while "Section 17(2)" refers to further classes such as research, archiving, and statistical purposes subject to conditions. When government agencies

process data for regular service delivery, the Act still demands notice, security, and breach reporting, though some rights and transparency obligations may be weakened where decision making is not affected or where separate legislation governs disclosure. Therefore, controllers dealing with public systems should determine whether they are working under a specific statutory mandate or a general service arrangement as the compliance posture is different.[14]

1.7.4 Research and Employment Uses

The law acknowledges various types of data processing such as those done for research, archiving, and statistical purposes, as well as processing related to employment, prevention of corporate fraud, internal investigations, and service provision where obtaining consent is impractical or disproportionate, within "Section 7" on certain legitimate uses. If these grounds are interpreted correctly, they do not allow unlimited collection but require a close connection to the specified purposes and the necessity being able to be demonstrated. In the case of research, controllers ought to use strong de identification, obtain ethics approval if necessary, and follow governance that separates identifiers from the analytic datasets. In the case of employment, attendance, payroll, benefits administration, and workplace security, for instance, can qualify but employers must still ensure that there are storage limitations, access controls, and grievance handling in place. Controllers should document their assessment of the feasibility of obtaining consent and keep DPIAs if the scale or sensitivity elevates the risk. The Act's examples and illustrations serve to confirm this equilibrium by linking the continued processing to a currently specified purpose and to the compliance with other applicable laws. This permission which is calibrated serves to preserve the welfare and the research value while at the same time being in line with the principles of proportionality and accountability.

1.8 SECTORAL INTERPLAY AND REGULATORY COHERENCE

The Act would be coexisting with and reshaping a dense stack of digital regulations that already impose duties with respect to platform due diligence, cybersecurity, financial sector resilience, telecom retention, and digital public infrastructure governance. Hence, a realistic compliance stance must consider the Act as one of the related laws "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", the CERT Instructions on six-hour incident reporting, RBI's master directions on outsourcing of IT services, SEBI's cyber resilience framework, IRDAI's information and cybersecurity guidelines and domain specific frameworks such as the Aadhaar Act and the Account aggregator architecture. The DPDP Act

[14] Data Protection Standards for Cross-Border Data Transfer: A Global Perspective, *available*

at: https://www. livelaw.in/articles/cross-border-data-transfer-regulations-global-trade-digital-services-data-protection-229472

mandates horizontal rights and responsibilities, while sectoral instruments detail the operational aspects, incident timelines, and supervisory scrutiny by sector regulators. Such a relationship results in both overlaps and gaps, and organizations should handle DPDP compliance as the spine that links privacy notices, consent records, risk assessments, and breach playbooks to sectoral anchors, rather than as a siloed programme. This enables them to harmonies incident response clocks, vendor controls, and disclosure duties across different regimes.[15]

1.8.1 IT Act and Intermediary Rules

On account of their platform governance, intermediaries are already required to have published rules, remove unlawful content on knowledge, and have grievance officers and nodal contacts as per the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" as updated. These obligations of theirs comprise due diligence, user notice transparency, and periodic reporting. The DPDP Act is a layer over the base which has privacy rights and breach duties and platforms have to make sure their terms of service, transparency reports, and notice templates are in harmony with both content and privacy law. The getting amendments to deepfakes and synthetic media that are talking about how content authenticity and privacy are two sides of one coin is an indication that labeling and takedown flows may require biometric or face related data processing. Therefore, controllers should present DPDP notice content in their terms and community guidelines, make sure biometric processing is by consent or legitimate use grounds, and privacy complaint queues should be aligned with those of content so that they do not get stuck. In case State takedown orders or court orders resulting in disclosures, "Section 17" exemptions may be there but logging and auditability should still be there.

1.8.2 CERT-In Directions and Cybersecurity

The CERT In directions of 28 April 2022 specify the six hours timeline within which cyber incidents that are prescribed must be reported, the requirement for synchronization with NTP servers, and the retention of logs locally in India for 180 days. These stipulations are DPDP breach notification to the Board and to affected data principals which will be done in a manner and form yet to be prescribed. The upshot is that organizations ought to regard CERT In reporting as the first timer that starts at the moment an incident is known, and then privacy notifications should be coordinated once personal data is confirmed to be impacted, at the same time, ensuring that containment is done in a forensic integrity preserving manner. Vendor

contracts should already be reflecting log retention, time synchronization, and cooperation obligations for enabling timely reporting. The Act's breach duties are located in "Section 8(6)" and rulemaking powers, while CERT In's obligations are derived from "Information Technology Act, 2000" under "Section 70B". It is better to harmonize both regimes so as to avoid repeated reporting and reduce the risk of being checked by the technical and privacy regulators at the same time.[16]

1.8.3 Financial Sector Guidelines

Financial services are compelled to meet a higher standard through the RBI "Outsourcing of Information Technology Services Directions, 2023", which requires regulated entities to be responsible for customer data, prepare exit plans, evaluate concentration risk, and bind service providers and their subcontractors by flow down clauses. SEBI's cyber security and resilience circulars stipulate architecture, SOC, drills, and incident classification for market infrastructure and intermediaries, while IRDAI's guidelines strengthen the controls in the insurance sector. These regimes collectively necessitate detailed asset inventories, third party risk scoring, and a tested incident response that is in line with DPDP's security and accountability obligations. Financial institutions should incorporate DPDP rights handling into the current KYC and grievance systems, tree into core banking or policy administration workflows the erasure and correction steps and contracting outsourcing should be done in such a way that captures DPDP breach reporting and audit rights. Consent artefacts and audit trails generated under AA directions can thus reinforce DPDP compliance and serve as a demonstration of purpose limitation if controllers are participating in the Account Aggregator framework.

1.8.4 Telecom and Digital Public Infrastructure

Telecom service providers that operate under license conditions are required to retain call data and records of internet usage for at least two years. They are also required to maintain the login and logout details of subscribers. This practice is in conflict with storage limitation but continues as a lawful retention obligation. Consequently, the storage limitation rule of the DPDP Act is subordinate to explicit legal mandates. At the same time, controllers should make a record of these legal holds and keep the retained records separated with strict access and security. India's digital public infrastructure stack that includes Aadhaar and the Account Aggregator is using consent-based flows and there are strong limitations on core biometrics under "Section 29" of the Aadhaar Act and "Aadhaar (Sharing of Information) Regulations, 2016". These frameworks can provide the basis for verifiable, revocable, and audit friendly consent that is in line with the DPDP's consent manager model. Telecom operators and DPI participants should coordinate their consent logs, key management, and grievance redress to

comply with both sector and DPDP requirements without the need for duplicative interfaces.[17]

1.8.5 Health, Edtech, and Govtech

Digital health initiatives under the Ayushman Bharat Digital Mission are described as privacy and consent centric designs, with policies that promote federated records, consented sharing, and strong authentication. Coordinating ABDM consent artefacts with DPDP notice and withdrawal flows can, very effectively, reduce the interaction barrier and create trust in longitudinal health records. Protecting the data of children in edtech and obtaining parental consent raise particular design challenges for age assurance and classroom analytics, thus requiring interfaces that guardians understand and that do not allow for persistent identifiers where it is not necessary. Govtech platforms need to reconcile DPDP rights with archival mandates and transparency laws, thereby ensuring that disclosures made to the public do not contain personal data unless authorized. Furthermore, privacy risk management and the regular performance of DPIAs should be considered as standard practice across these sectors, with links between sector policies and DPDP rights to provide citizens with a better understanding of their rights. Additionally, controllers should be prepared for the rulemaking that will define the formats for notices, withdrawal, and complaints, which can be integrated with the existing sector portals.

1.9 COMPLIANCE CHALLENGES AND OPPORTUNITIES

On the one hand, the compliance journey will reveal the same kind of problems as small businesses will have to deal with consent experience, vendor ecosystems, legacy data, and cost but on the other hand, it also enables trust-based innovation and more reliable data sharing. The rights and breach framework of the Act provide strong motivators for keeping data inventories clean and for cutting down on unnecessary data collection. Managers of consent and federated consent logs can be usual means that lessen the repetition across sectors and apps. The six-hour CERT In clock will move organizations to continuous monitoring and incident response that is rehearsed, and, therefore, will raise overall resilience. MSMEs should be provided with privacy notice, consent, and grievance handling templates and shared services, while bigger businesses can be expected to develop privacy engineering skills to make minimization and retention features a part of their products. Cross border models will be able

[17] Annual Report 2024–2025, Ministry of Electronics and Information Technology, *available at:* https://www. eity.gov.in/static/uploads/2024/12/10fcadec462c330211502fed3d24ea83.pdf (last visited on October 24, 2025).

to use modular contractual clauses and tested transfer assessments which can be switched on if a restricted list arises. These issues and prospects will determine the emergence of an Indian privacy culture that is practical.[18]

1.9.1 Consent Fatigue and UX Design

Consent focused on individuals is difficult to maintain when services require repeated permissions from the user across different screens and channels. According to the Act, consent should be given freely, be specific, be informed, be unconditional, and be unambiguous through a clear affirmative action. Also, language options should be available in a user-friendly manner. Achieving that level without exhausting users requires having layered notices, privacy nutrition labels, and progressive consent whereby optional purposes are separated and presented at the right moment. The consent managers who are registered with the Board can make it easier for users to centralize their preferences and withdrawals, thus lowering the friction. On the other hand, controllers should monitor provenance so that downstream processors can honor those choices. Dark patterns are at risk of noncompliance because they have the potential to weaken consent and, thus, attract enforcement. Incorporating DPDP compliant consent as part of the app should be viewed as a strategic move, especially in the case of children and assisted users, as well as in multilingual contexts where clarity and brevity are important. The statutory framework of “Section 5” referring to notice and “Section 6” to consent sets out the legal standard against which these interfaces will be evaluated.

1.9.2 Vendor Risk and Data Mapping

Third party ecosystems increase the risk of privacy violations in that processors and sub processors may gather telemetry, logs, and support data that the controller may not have full visibility of. The Act attributes accountability to the data fiduciary, which entails having complete data flow maps, records of processing, and contract schedules outlining purposes, security controls, breach cooperation, and deletion timelines. The experience of the financia sector is of great advantage in this case since the RBI and SEBI already require strong outsourcing governance and audit rights that can be easily adjusted to privacy. Controllers ought to be very firm on standard breach notification clauses that are in line with both CERT In and DPDP requirements and mandate that processors keep India resident log retention that is in harmony with incident timelines. The annexure method where each processing activity has a purpose, lawful basis, retention, and transfer description can make audits and Board inquiries less surprising. By starting to develop this habit, you will be less exposed to penalties and there will be less operational noise during the time of incidents.[19]

1.9.3 Age Verification and Identity Risks

Age assurance is a great example of the balance that needs to be struck between privacy and inclusion. Verification methods have to be accurate to strictly enforce the under eighteen thresholds, however, they should not result in excessive collection of identity data or exclusion of teens who do not have documents. Some privacy friendly techniques such as age estimation from biometric data, attestations in a tokenized form from trusted identity providers, or parental consent workflows that do not involve the perpetual storage of ID documents can reconcile these issues. Controllers must handle facial images and biometrics with increased facial images and biometrics with increased caution and, at the same time, document minimization and the use of secure, revocable tokens should be preferred. The child centric provisions of the law make it clear that unnecessarily wide tracking or profiling of children is not allowed, while there should be accessible complaint and erasure mechanisms that can be used by guardians. Pilots in the education sector have revealed that facial recognition for attendance and similar schemes cause significant privacy issues, and the designers should opt for less intrusive methods wherever it is possible. The legal basis for parental representation and children's rights can be found in the definitions as well as the special obligations related to children's data and consent.

1.9.4 Legacy Systems and Security Upgrades

Legacy architectures make it difficult to limit the purpose of data and to erase data since monolithic databases and flat logs do not have data lineage. The storage and purpose limitation rules of the Act at the very least make enterprises modernize to modular services, tagged datasets, and automated retention engines that can enforce destruction or anonymization on schedule. CERT In's six-hour reporting window means continuous detection, validation of time synchronization, and tamper evident logging, which usually necessitates the use of a security data lake and playbooks integrated with ticketing and communications. Encryption at rest and in transit should be done for everyone, with key management kept separate from cloud providers if possible and vendor contracts should be documented. Regular restoration drills, red team exercises, and data breach rehearsals help to lower the response time and give better evidence to the Board. Additionally, controllers are required to align erasure with legal holds under telecom, financial, tax, or archival regulations so as not to commit spoliation. Privacy engineering must be considered alongside security and reliability as a primary design constraint throughout all these changes.[20]

1.9.5 MSMEs, Startups, and Cost of Compliance

Smaller entities are often in a position where they have difficulty absorbing the costs of compliance and at the same time, they face a concentrated risk of damage to their reputation

and penalties. Due to the technology neutral design of the Act, there is still a possibility for shared utilities such as consent manager integrations, template notices, grievance portals, and open-source privacy dashboards that lower unit costs. Sector bodies and incubators can assemble standard contractual clauses for processors, DPIA templates, and breach notification playbooks. Following sectoral guidance, for instance, RBI outsourcing directions, where relevant, can create a win-win situation even for unregulated startups as it helps in building strong vendor governance from day one. It will be crucial to have a phased implementation plan linked to rulemaking and public consultation indicating that formats and thresholds will be specified keeping feasibility in view. Privacy conscious startups can turn compliance into a trust signal to their customers and partners; thus, they can increase their conversion and retention rates in congested markets.

1.9.6 Innovation, Trust, and Data Economy

A strong privacy framework is necessary for data driven innovation, as it helps to lower the uncertainty aspect of sharing and reuse. The Act's consent manager, notice, and grievance system can be in line with finance, health, and public services for interoperable consent, thus enabling secure switching and competition. Cross border processing is still allowed under the restricted jurisdictions model; thus, Indian companies can be part of global cloud ecosystems while keeping records of transfer assessments and safeguards. Research and statistical activities are allowed with certain limitations, thereby supporting the use of anonymization toolchains and governance that ensure the protection of individuals. Companies that put money into privacy engineering will be in a position to create trust as a product via dashboards, preference centers, and transparent data receipts, thus strengthening user agency. Gradually, a privacy maturity curve across the whole economy will be able to attract capital that is responsible and lower the risk of large breaches. The healthier data economy is the main consequence where the rights and growth co-exist rather than compete.[21]

1.10 COMPARATIVE INSIGHTS

Through a comparative lens, India's decisions and the given paths for future rulemaking seem clearer. The negative list of the Act for cross border transfers and its consent manager model move away a bit from some established global templates, but they both reach a pragmatic middle ground that tries to keep the flows intact while still asserting sovereign control. The rights package is in line with international standards regarding access, correction, and erasure, and also provides nomination which reflects the cultural and legal aspects of representation at incapacity or death. The center of enforcement is an adjudicatory Board, with penalty schedules

that have the capacity to scale up to systemic noncompliance, however, the overall tone of the law is directed towards compliance supported by guidance and not punishment. This law will grow together with regulations that will determine the formats, thresholds, and processes, and coordination with sectoral frameworks will be the factor that facilitates the delivery of clarity. References from the comparative perspective to GDPR, Singapore's PDPA, and Brazil's LGPD serve as good differences in lawful bases, transfer mechanisms, and enforcement posture.

1.10.1 Alignment and Divergence with GDPR

The Act and GDPR share core principles such as lawfulness, fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability, and both also provide rights of access, correction, and erasure. Differences can be seen in lawful bases and transfers. The GDPR identifies several bases including legitimate interests, contract, legal obligation, vital interests, and public task, whereas the Indian Act directs non consent processing through a specially prepared list of "certain legitimate uses", thus making policy decisions more explicit

---

[21] The Confluence of AI and Data Privacy: Aligning Data Privacy Regime in India for the Age of AI, *available at:* https://www.barandbench.com/view-point/the-confluence-of-ai-and-data-privacy-aligning-data-privacy-

and narrower. Regarding transfers, GDPR uses adequacy, appropriate safeguards, and derogations, while India considers a restricted jurisdictions approach by notification under "Section 16". There are also differences in governance. Under GDPR, independent supervisory authorities are given investigative powers, whereas India provides for an adjudicatory Board along with techno legal measures and rulemaking assistance. These decisions indicate constitutional design and market realities, but the agreement on transparency, security, breach notification, and rights makes interoperability possible.[22]

1.10.2 APAC and Global South Models

Singapore's PDPA mixes consent with exceptions for legitimate interests and business improvement, which is supported by a proactive regulator that issues advisory guidelines and undertakings, thereby providing a model for calibrated flexibility. Brazil's LGPD is heavily influenced by GDPR but adjusts enforcement to a data authority that is new and a market that is still developing, with transfers being dependent on adequacy like mechanisms and contractual safeguards. India's decision to have a negative list for transfers and a consent manager layer is different but still in line with the Global South trend of trade in data being

balanced with the sovereignty of the state and limitations of the capacity. Rulemaking may take the best of both worlds from Singapore's clear guidance culture and Brazil's gradual elaboration of DPIA triggers and standard clauses, while still having India's DPI and consent artefacts. These comparators suggest that stable data protection is a result of communication between regulator and industry, and the creation of operational tools that everyday controllers can use.

1.10.3 Reform and Rulemaking Priorities

It is expected that the subsequent stage will specify formats for notice, consent withdrawal, and grievance; set thresholds and disclose content for breach notification to the Board and data principals; establish criteria for designation of Significant Data Fiduciary; and make available the model contractual clauses for processors and cross border transfers to ease negotiation. Alignment guides for harmonizing DPDP with CERT In timelines, sectoral incident definitions, and telecom retention will help people to understand the situation during crises. Age assurance standards should focus on privacy friendly methods and specify the acceptable evidence and retention limits. Lastly, the rules should talk about registration, accountability, and audit requirements of the consent manager to ensure real interoperability. The draft DPDP rules public consultation process and government communications regarding release timelines suggest that these priorities are acknowledged and will probably be dealt with in staged notifications.[23]

1.10.4 Capacity Building and Awareness

Regimes that are successful, spend money on their people and skills. As a result, regulators and the Board secretariat will require coaching in areas such as privacy engineering, incident forensics, statistical disclosure control, and DPIA evaluation. The industry will require role-based training for product managers, engineers, marketers, and support teams, with the provision of clear playbooks for rights handling and breaches. MSMEs will have the advantage of commonly used templates, helplines, and sandboxes. The coordinators of different sectors should regulate glossaries and taxonomies in such a way that incident classes and severity levels have the same understanding in both privacy and cybersecurity. Awareness of the public can utilize the already existing DPI rails, such as consent managers and grievance portals, to provide citizens with easy dashboards for their data relationships. Universities and research labs can enhance their potential through clinics and applied research consortia which can serve as a testing ground for anonymization, edge processing, and privacy preserving analytics that are suitable for Indian datasets. The law will be more doable and efficient if there is a comprehensive ecosystem approach.

1.11 CONCLUSION

India's Act establishes a realistic basis that acknowledges the rights and at the same time allows lawful processing that is based on necessity and accountability. The governance framework will become more effective when the rules provide details of formats, thresholds, and registers. Organizations should not be waiting. By creating good data maps, rationalizing purposes, tuning notices, and operationalizing withdrawal and erasure, organizations will lessen their exposure to risk and will save money. Sectoral overlays and CERT In clocks must be combined into a single incident posture. When it comes to children's data and high-risk analytics, implement privacy preserving methods and be more secure with retention. In the case of cross border services, have modular transfer packets ready and be careful with restricted lists. The Board, sector regulators, and industry can together turn compliance into trust, which is the real dividend for a data economy at the scale of India. The law's center of gravity is in "Sections 3 to 12" that deal with scope, rights, and fiduciary duties, "Section 16" on transfers, and "Section 17" on exemptions and these anchors will guide India in building a right based digital future.

BIBLIOGRAPHY

1. Anirudh Burman, "Understanding India's New Data Protection Law", *available at:* https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited on October 25, 2025).
2. Annual Report 2024–2025, Ministry of Electronics and Information Technology, *available at:*https://www.meity.gov.in/static/uploads/2024/12/10fcadec462c330211502fed3d24ea83.pdf (last visited on October 24, 2025).
3. Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W. W. Norton & Company, New York, 1st edn., 2015).
4. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing, New York, 1st edn., 2016).
5. Data Protection Standards for Cross-Border Data Transfer: A Global Perspective, *available at:* https://www.livelaw.in/articles/cross-border-data-transfer-regulations-global-trade-digital-services-data-protection-229472 (last visited on October 16, 2025).
6. Digital Personal Data Protection Act, 2023 – A Brief Analysis, *available at:* https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis (last visited on October 18, 2025).
7. Draft Digital Personal Data Protection Rules, 2025 — Key Takeaways, *available at:* https://law.asia/draft-digital-personal-data-protection-rules-2025/ (last visited on October

17, 2025).

8. Finn Brunton, Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (MIT Press, Cambridge, 1st edn., 2015).
9. Gaurav Thote, "Unravelling 'Consent' Under the Digital Personal Data Protection Act, 2023 — A Barrier to Data Principal Rights", *available at:* https://www.scconline.com/blog/post/2024/11/13/unravelling-consent-under-the-digital-personal-data-protection-act-2023-a-barrier-to-data-principal-rights/ (last visited on October 22, 2025).
10. India AI Report 2023 (MeitY), *available at:* https://www.meity.gov.in/static/uploads/2024/02/b57a6bb5ef870329a94e0131ca108f6e.pdf (last visited on October 20, 2025).
11. India's DPDP Act, 2023: Are You Ready?, *available at:* https://www.barandbench.com/view-point/india-dpdp-act-2023-are-you-ready (last visited on October 17, 2025).
12. Julie E. Cohen, Configuring the Networked Self: Law, Code, *and the Play of Everyday Practice* (Yale University Press, New Haven, 1st edn., 2012).
13. Mira Burri, "Approaches to Digital Trade and Data Flow Regulation Across Jurisdictions: Implications for the Future EU–ASEAN Agreement", 23 *Journal of International Economic Law* 220 (2020).
14. Navigating Fiduciaries, Processors, and India's DPDP Act, *available at:* https://www.barandbench.com/view-point/intricate-web-data-protection-fiduciaries-processors-india-dpdp-act (last visited on October 21, 2025).
15. Rahul Matthan, *Privacy* 3.0: Unlocking Our Data-Driven Future (HarperCollins India, Noida, 1st edn., 2018).
16. Shiv Shankar Singh, "Privacy and Data Protection in India: A Critical Assessment", 53 *Journal of the Indian Law Institute* 672 (2011).
17. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, New York, 1st edn., 2019).
18. Talat Fatima, *Cyber Crimes* (Eastern Book Company, Lucknow, 1st edn., 2021).
19. The Confluence of AI and Data Privacy: Aligning Data Privacy Regime in India for the Age of AI, *available at:* https://www.barandbench.com/view-point/the-confluence-of-ai-and-data-privacy-aligning-data-privacy-regime-in-india-for-the-age-of-ai (last visited on October 19, 2025).
20. Understanding India's New Data Protection Law, *available at:* https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en (last visited on October 23, 2025).
21. Vakul Sharma, *Information Technology Law and Practice* (Universal Law Publishing,

New Delhi, 1st edn., 2011).

22. Virendra Kumar, "Dynamics of the 'Right to Privacy': Its Characterization Under the Indian Constitution", 61 *Journal of the Indian Law Institute* 68 (2019).