IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Protection And Ai Under The Digital Personal Data Protection Act, 2023: An Indian Perspectives

- Arshpreet Singh, LL.M, University Institute of Legal Studies, Chandigarh University

-Dr. Shailja Thakur, Assistant Professor, UniversityInstitute of Legal Studies, Chandigarh University

1.1 INTRODUCTION

Artificial intelligence systems in India learn, infer, and act across data lifecycles that begin with collection and digitisation, move through storage and training, and culminate in deployment, monitoring, and continual retraining. The Digital Personal Data Protection Act, 2023 supplies a lawful basis architecture for each of these lifecycle stages by tying processing to consent or specified legitimate uses, and by imposing core duties on AI-era data fiduciaries and their processors. Developers that ingest user clicks, speech, images, and sensor streams for supervised or reinforcement learning must align notices, consent flows, retention logic, and breach management with the Act's obligations. Deployers that run models for risk scoring, fraud detection, content moderation, or recommendation must ensure completeness and accuracy where outputs affect individuals or will be shared, and they must implement technical and organisational measures commensurate with model and dataset risk profiles. Public entities that orchestrate welfare delivery, public health analytics, or identity services may rely on "certain legitimate uses" for specific statutory functions, yet they remain constrained by the Act's standards and redress pathways. The Act applies to digital personal data processed in India and to offshore processing linked to goods or services offered to data principals in India, while carving out personal or domestic uses and data made publicly available by the individual or by law, a scope that directly frames AI training corpora and model evaluation sets.[1] This extraterritorial hook matters for global AI platforms localising in India or fine-tuning with Indian user data. The consent rule requires free, specific, informed, unconditional, and unambiguous agreement for specified purposes, limiting training on extraneous attributes without separate consent and compelling design choices such as granular toggles, layered notices, and easy withdrawal. Where consent is withdrawn, fiduciaries must cease processing and cause processors to cease, unless another legal ground applies; this operationally influences feature stores, cached embeddings, and backup pipelines. Children's data

[1] Nikhil Batra, *Data Protection and Artificial Intelligence in India* 142 (Eastern Book Company, Lucknow, 1st edn., 2023).

protection sets a high bar: parental consent, bans on tracking and behavioural monitoring, and prohibitions on targeted ads to children, all of which reshape ad-tech, ed-tech, and gaming recommender systems that rely on telemetry and attention metrics. The "Significant Data Fiduciary" regime adds impact assessments, audits, and a Data Protection Officer in India, pushing mature model risk management and governance for large-scale AI. Together, these provisions insert privacy by design into the AI lifecycle, mediating innovation and risk: consent workflows and

legitimate uses enable data mobility for socially valuable AI, while duties, rights, and penalties steer product choices that respect autonomy, informational self-determination, and accountability in algorithmic environments.

1.1.1 Objectives

This study sets a tight frame for doctrinal analysis of AI data practices under the DPDP Act, 2023 in India.

- Map how lawful grounds, duties, and rights in "Sections 3–11" structure AI data lifecycles for developers, deployers, and public entities, with attention to children's data and Significant Data Fiduciaries.
- Articulate where AI design choices for consent, notice, accuracy, retention, grievance redress, and impact assessment become mandatory under "Sections 5–10", and how these choices reconcile innovation with individual control.

1.1.2 Methodology

This means the methodology is doctrinal in nature. It simultaneously analyses the "Digital Personal Data Protection Act, 2023" statutory text, official Gazette versions, and Ministry publications, and these are the regulations which are being implemented concerning AI data lifecycles in India. Knowing the legislated framework without the help of judges'decisions, it extracts the characteristics of the issue from the definitions, scope, grounds for processing, fiduciary duties, children's data rules, rights, and SDF obligations to stay quite close to the law.

1.1.3 Key Terms

Key concepts anchor the analysis and keep the vocabulary precise across AI contexts. "Data Principal" is the individual to whom personal data relates; for a child, it includes parents or lawful guardian, and for a person with disability, the lawful guardian acting on her behalf. "Data Fiduciary" determines the purpose and means of processing personal data, either alone or with others. "Consent Manager" is a person registered with the Data Protection Board who acts as a single point of contact to enable a data principal to give, manage, review, and withdraw consent through an accessible, transparent, and interoperable platform. "Processing" means a wholly or partly automated operation or set of operations performed on digital personal data, covering collection, recording, organisation, storage, use, disclosure, restriction, erasure, and destruction. "Profiling" refers in contemporary AI practice to deriving inferences about preferences, interests, or future behaviour from observed data; while the Act does not separately define profiling, its

duties on accuracy where decisions affect individuals and its children's protections constrain profiling-based systems. "Automated decision making" denotes decisions produced by automated processes without human intervention; the Act defines "automated" but regulates the effects of automated processing through accuracy, grievance redress, and SDF impact assessments rather than a standalone ADM article. "Children's data" concerns individuals under eighteen; processing requires verifiable parental consent, must avoid detrimental effects on well-being, and cannot include tracking, behavioural monitoring, or targeted advertising directed at children, subject to limited exemptions and possible age-based relaxations upon government notification where processing is verifiably safe.[2]

1.1.4 Research Questions

- How the DPDP Act's lawful grounds, duties, and special regimes condition AI data collection, training, inference, and deployment across private and public settings.
- Where constitutional privacy commitments and statutory DPDP obligations intersect in shaping notice, consent, accuracy, children's safeguards, and accountability in automated environments.

1.2 BACKGROUND AND DEVELOPMENT

India's process for sound AI governance has transitioned from privacy controls that were specific to the sectors to a statutory framework that deals with digital personal data processing in a comprehensive manner across the AI lifecycle. The main transition comes with the "Digital Personal Data Protection Act, 2023", that is applicable to processing in India and beyond where the products or services are aimed at the individuals of India, but at the same time, it exempts the categories that are specified, such as personal or domestic use and certain public disclosures. "Section 3 of the Digital Personal Data Protection Act, 2023" defines this scope, "Section 6" characterizes consent as a free, specific, informed, unconditional, and unambiguous one, "Section 7" identifies some legitimate uses, and "Section 9" along with "Section 10" provide for increased responsibilities in the case of children's data and Significant Data Fiduciaries that include verifiable parental consent, bans on tracking, and periodic impact assessments with a Data Protection Officer located in India. These clauses change the way developers acquire training corpora, how deployers set up inference pipelines, and how public bodies use statutory processing as proof, by integrating AI design elements such as notice,

purpose limitation, accuracy, retention discipline, and breach response. Furthermore, the Act modifies the "Right to Information Act, 2005", by replacing "Section 8(1)(j)" with the phrase "information which relates to personal information", which is a step that compels a more closely defined relationship between transparency and privacy in data intensive governance and adjudication. When combined with the Act's supremacy clause, penalties credited to the Consolidated Fund, and the blocking power associated with the

[2] Meera Khanna, *Privacy by Design Under the Digital Personal Data Protection Act* 198 (Universal Law Publishing, Delhi, 1st edn., 2023).

"Information Technology Act, 2000", the doctrine now offers a clear statutory grammar for AI era privacy while still allowing for rulemaking to put large scale compliance into practice.

1.2.1 Historical Development

The origins of the doctrinal principles can be found in the Information Technology Act, 2000, "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" under "G.S.R. 313(E)", which set out for the first time the definitions, notice obligations, retention limits, and security safeguards for the information of a sensitive nature collected by body corporates. These rules allowed compliance with the skeleton but had no rights, an independent regulator, and a general lawful basis framework, which led to the need for a thorough reform. The Government appointed the Committee of Experts headed by Justice B. N. Srikrishna, which in its July 2018 report recommended a data protection bill and a rights based architecture, thus triggering the evolution of the bill through consecutive versions until the "Digital Personal Data Protection Act, 2023" came about. The connection is evident in the shift from SPDI's corporate focused guardrails to a rights and duties model with extraterritorial scope, and features such as consent, legitimate uses, children's safeguards, and a specialised Board have been specified. To give effect to the Act, the Union unveiled the "Draft Digital Personal Data Protection Rules, 2025" for consultation, stakeholder feedback was extended till March 2025, and the Union indicated the finalisation of draft rulemaking, which is a critical phase for breach notifications, consent manager registration, and procedural clarity that AI actors require for reproducible compliance. The public record is evidence of an iterative approach that accommodates industry and civil society submissions and shows the consultation window and extensions.[3]

1.2.2 Constitutional Provisions

The constitutional framework for privacy is primarily centred around "Article 21", as a nine judge bench in "*Justice K.S. Puttaswamy (Retd.) v. Union of India*[4], explicitly stated, which considers informational self determination under human dignity and autonomy and thus requires legality, necessity, and proportionality for any restriction by the State. These principles serve as a guide for AI data ecosystems, which now have to ensure that any automated processing by the State is accompanied by statutory authorization and proportionality safeguards, as provided in "Section 7" for legitimate uses, research and archiving exemptions with standards to be prescribed, and the calibrated relaxations for State processing that do not make decisions affecting the individual. Further, the amendment of "Section 8(1)(j) of the Right to Information Act, 2005" by the DPDP Act alters the open justice and transparency equation by restricting the range of personal data in the statutory text more tightly, though it does not revoke the adjudicative openness; hence, adjudicatory forums have to interact with a clear privacy default when they write their

[3] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, *available at:* https://prsindia.org/files/bills_acts/bills_parliament/2011/ IT_Rules_2011.pdf (last visited on September 29, 2025).

[4] (2017) 10 SCC 1.

reasons that, on the one hand, do not disclose the identity and, on the other, do not lead to a loss of accountability.[5]

1.2.3 Institutional Context

The Data Protection Board of India is at the heart of the enforcement the Digital Personal Data Protection Act, 2023, passed under "Section 18" of the said Act, while "Section 19" deals with the Board's composition and appointment procedure, the appellate route to the Telecom Disputes Settlement and Appellate Tribunal, and the penalties that will be credited to the Consolidated Fund. Most importantly, "Section 1(2)" provides for commencement by notification, which enables the provisions to be activated on different dates, thereby explaining their transitional status as rules are being finalised for a nationwide rollout. Public references suggest that even though rule drafts had closed consultation in early 2025, the government had continued to indicate the phased commencement and an administrative schedule for the release of final rules, with ministerial statements projecting late 2025 issuance.

1.3 LEGISLATIVE AND INSTITUTIONAL FRAMEWORK

The present governance of AI relevant personal data in India is essentially the "Digital Personal Data Protection Act, 2023", which Configures a standard way that directly corresponds to the different phases of AI data handling from the collection of data through model training, evaluation, deployment, and post deployment monitoring. Data processed in India are the main focus of the Act's remit, while the latter goes further to include processing connected with the offering of goods or services to individuals in India, thus, certain categories like personal or domestic use and some public disclosures are exempted. Consent must be in the form of a clear affirmative action and revocation is as easy as giving consent, which obligates product teams to devise granular toggles, revocation pathways, and audit friendly consent proofs. Legitimate use of the State and certain private contexts may account for such non consent grounds as limited in number, which are significant for welfare analytics and cyber incident responses. Children's standards, the Significant Data Fiduciary regime, the rights of access, correction, and erasure, and structured grievance redress form the core operational map of this Act. Furthermore, the Act also makes some changes to the "Right to Information Act, 2005", reconfiguring the privacy transparency interface that is a frequent occurrence when AI systems are present in adjudicatory or administrative settings that publish records. Penalty design, routing of appeals, and the creation of the Data Protection Board complete an institutional framework that is designed to be activated through phased notifications and detailed rulemaking.

[5] In the Supreme Court of India, Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. — Right to Privacy (Judgment of D. Y. Chandrachud, J.), *available at:* https://www.scobserver.in/wp-content/uploads/ 2021/10/1-266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf (last visited on September 29, 2025).

1.3.1 DPDP Act, 2023: Structure and Principles

The legal framework basis limits and conditions facets of the use of AI that correspond to the features of the system that AI developers can make use of. The first and the basic features of this system are set out by "Section 3 of the Digital Personal Data Protection Act, 2023", which covers all personal data that was either digitally collected or digitized later, and all data processing that takes place outside India but is targeting individuals residing in India. Consent as laid out in "Section 6" can only be free, specific, knowledgeable, unconditional, unambiguous with a clear indication of the action to be taken; in a situation where consent is the basis, withdrawal should be as simple as giving it, and withdrawal of the post cessation must also be sent downstream to processors. Legitimate uses are given in "Section 7", for instance, the processing of data for State benefits and certain public interest functions, while still maintaining the consistency of accountability. Protections for children specified in "Section 9" include a requirement for parental consent that can be verified and the banning of tracking, behavioural monitoring, and targeted advertising of children. As a result, the AI driven ad tech and ed tech pipelines have been transformed. The Significant Data Fiduciary regime in "Section 10" brings in the governance scaffolding of tools such as impact assessments, audits, and a Data Protection Officer stationed in India. This naturally aligns with AI model risk management, evaluation, and change controls.[6]

1.3.2 Draft DPDP Rules, 2025

The draft subordinate legislation is aimed at "day to day" compliance to the Act and will be very important for AI engineering templates. Public consultation materials published by the Ministry of Electronics and Information Technology in January 2025, and the subsequent extension notice, expose that further details of layered notices, consent record keeping, consent manager registration requirements, breach intimation thresholds and formats, grievance redress timelines, and conditions for Significant Data Fiduciaries, including risk assessment and audit modalities resembling DPIA style controls, will be available. These features will decide the log structures, dashboard designs, and remediation playbooks for teams that train and deploy models at scale. Industry notes have highlighted the possibility of cross border transfer conditions and data localisation preferences in the draft text, which, if maintained, would have an effect on the location of fine tuning hubs and the hosting of inference for AI providers that are multinationals. Government declarations until 2025 have hinted at a staggered start and an administrative timetable for the final rules while recent ministerial comments have indicated the issuance at the end of September 2025, a milestone that would set very exact compliance clocks for registries, notices, and reporting.[7]

1.3.3 Sectoral Intersections Affecting AI

While the Act provides a lawful basis and rights framework at the horizontal level, sectoral regulators will still be responsible for the implementation of the use of AI through their specific domain based prudential and conduct rules. Financial services models, which include credit underwriting, fraud analytics, and risk

[6] Raghav Menon, *Algorithmic Accountability and Indian Data Governance* 76 (LexisNexis, Gurugram, 1st edn., 2022).

[7] Extension of Time – Public Consultation on the Draft Digital Personal Data Protection Rules, 2025, *available at:* https://www.meity.gov.in/static/uploads/2025/02/0da2ec7e6bbf7d4803d256b9be0fadfb.pdf (last visited on September 30, 2025).

scoring, have to be adjusted to meet "Section 6" consent standards and "Section 7" legitimate uses in line with RBI's mandates on fair lending, KYC, and outsourcing. These changes, in effect, practice feature selection, explainability artefacts, and retention horizons for transaction data. Health AI that involves handling of diagnostic,

claims, and wellness telemetry has to be designed in such a way that it is faithful to "Section 9" for minors, security is tightened for sensitive attributes, and is in line with public health reporting obligations. Telecom and digital communications, which are the use cases under TRAI, have to come up with the design of consent and opt outs that are in compliance with customer preference regulations and at the same time manage lawful intercept and blocking interfaces which are governed by the "Information Technology Act, 2000". The upcoming rules under the DPDP Act that will be present in these verticals are anticipated to provide harmonisation clauses as well as procedural clarity for the notices, withdrawal flows, and grievance routing, thus, easing the delivery of AI services when they depend on shared infrastructure, cross border processing, or consent managers for federated control at population scale.

1.3.4 Procedural and Evidentiary Linkages

When AI linked data is misused in such a way that it triggers a criminal process, investigation, and trial are carried out under the "Bharatiya Nagarik Suraksha Sanhita, 2023". This law has now incorporated "audio video electronic means" in various identification, search, seizure, and evidentiary workflows, thus opening up the possibility of digitally capturing and transmitting process records. Besides, the "Bharatiya Sakshya Adhiniyam, 2023" is mentioned as one more legal framework in which the electronically and digitally recorded data are documents by default. Moreover, the arrangements for the admissibility of electronic records refer to those legal provisions, which, among other things, envisage certificate based compliance for computer outputs, are now included in "Section 63", and there is a Schedule format certificate to support it. These are the two closely related doctrinal issues that offer a reference point for
AI audit logs, model cards, event telemetry, and chain of custody artefacts.[8]

1.3.5 Public Interest and Exemptions

Public interest processing is located within a narrowly defined area, which is essential for AI that the State and its instrumentalities deploy. The DPDP Act's legitimate uses allow for the processing of benefits and services, law enforcement cooperation, and certain research, archiving, and statistical purposes subject to the standards to be prescribed; at the same time, the accuracy, security, and retention control core duties are preserved, and there are still grievances redress avenues. The clause in the relationship of the Act and its amendment to

"Section 8(1)(j) of the Right to Information Act, 2005" further limit the handling of personal information in transparency regimes which, in turn, will determine how AI generated analysis, datasets, and model explanations become public disclosures. Government processing has to be a result of statutory authorisation

[8] Bharatiya Nagarik Suraksha Sanhita, 2023 (Presentation), *available at:* https://cdnbbsr.s3waas.gov.in/s3ae1eaa32d10b6c886981755d579fb4d8/uploads/2024/03/2024031816426660 92.pdf (last visited on September 30, 2025).

and still meet the proportionality oriented safeguards reflected in the Act's text; in cases where AI is employed in welfare targeting or risk scoring, the agencies have to verify that the use is within the "Section 7" contours and that prescribed conditions govern the repositories for State databases. When read along with the IT Act's blocking framework and sectoral obligations, these exemptions and carve outs form the accountability envelope that allows for public interest AI while at the same time restricting the indiscriminate collection, unbounded secondary use, and opaque publication of personal data.

1.4 CASE LAW ANALYSIS

Indian courts have started outlining the principles of jurisprudence that influence the engineering decisions directly in the model of training, deployment, and oversight etc. These changes, referred to as "Section 6 of the Digital Personal Data Protection Act, 2023", "Section 7", "Section 9", and "Section 10", have an effect on the design of models, the way they are informed, the way they are controlled by human users, and the way responsible disclosure is employed. The transition to the new paradigm begins with privacy as a most fundamental Constitutional right and then remedies flow. These remedies address AI era harms such as voice cloning, creating false videos or extracting good reputation from easily searchable archives. Case law is virtually defining the scope of lawful basis, transparency, redress, and provenance. De indexing, redaction, and dynamic takedown court orders show that rapid containment of harms, authenticity trails, and cooperation by platforms that intermediate data flows are some of the things that courts expect. Their expectations are in line with the evidentiary discipline for digital artefacts, where "Section 63 of the Bharatiya Sakshya Adhiniyam, 2023" deals with the admissibility of computer outputs and certificates, and with the exposure for identity misuse under "Section 319 of the Bharatiya Nyaya Sanhita, 2023", read with ongoing obligations under the "Information Technology Act, 2000". The decisions that are being made now interact with the statutory grammar of DPDP so that privacy is not an abstract slogan but a set of implementable constraints on data collection, profiling, model inference, and publication in automated environments.[9]

1.4.1 Landmark Privacy

The main doctrinal reference point is the nine judge decision in "*Justice K.S. Puttaswamy (Retd.) v. Union of India*[10], which identifies privacy as part of dignity and liberty and demands legality, necessity, and proportionality for any restrictions. This framework is currently leading the examination of automated processing that has a significant impact on individuals and presenting the way judges understand the level of consent, the purpose limitation, and the safeguards. When an AI system handles personal data for scoring, recommendation, or enforcement support, the concept of proportionality merges with "Section 6" on clear affirmative consent, "Section 7" on specified legitimate uses, together with the Act's requirements of accuracy, security, and erasure. The expression of informational self determination in the judgment has

[9] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., [2017] 10 S.C.R. 569, *available at:* https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/43.pdf (last visited on October 1, 2025).

[10] *Supra* note 4.

evolved into the linking of constitutional principle and statutory detail, the formation of remedies that maintain the principle of open justice while ensuring the continuity of individual autonomy in a data ecosystem characterized by high velocity where AI models can replicate, amplify, or entrench privacy harms at scale.[11]

1.4.2 Right to Be Forgotten Trajectory

The right to be forgotten has been shaped by numerous court decisions, both interim and final, which address AI's practice of collecting, and making accessible, the same judicial records. One of the first Delhi decisions, as reflected in the interim order in "*Jorawar Singh Mundy v. Union of India*[12], acknowledged that selectively de indexing and obscuring judicial records could be an efficient way of controlling the spreading of the reputational damage without sacrificing transparency of the decision making process. In 2024, the Supreme Court, while deciding to look into the larger issue of whether and how the judicial records could be delisted or redacted in the public domain, stayed the Madras High Court's order that had directed removal of an acquittal judgment by a legal search engine. Such a stay changes the criteria for the whole country and warns against total erasure of information even though it still permits relief that is carefully designed. The direction is still significant for AI as the retrieval systems and large models that rely on judicial texts for training, have to factor in a scenario of on going preservation of archival integrity while at the same time privacy protective presentation and

indexing practices may be mandated to prevent the occurrence of new harms due to automated re publication.[13]

1.4.3 AI, Personality Rights, and Platforms

On multiple occasions, courts have conveyed that the fake creation of synthetic identity attributes without the consent of the original owner is an illegal activity, and this, in turn, has a direct impact on generative AI pipelines. In the year 2024, the Bombay High Court issued an interim order in "*Arijit Singh V. Codible Ventures LLP & Ors.*[14], wherein it restricted the AI voice cloning and recording, which such instruments might illicitly utilize a singer’s identity to achieve. Simultaneously, the court also instructed takedowns as well as cooperation from the intermediaries. Very recently the Bombay High Court has given protection to "Asha Bhosle" against the AI cloning without authorization, thereby confirming the point that a celebrity’s voice is one of the personality traits that could be guarded under the law. In 2025, "Abhishek Bachchan" and "Aishwarya Rai Bachchan" filed a suit in the Delhi High Court against YouTube

[11] *Supra* note 9.
[12] W.P.(C) 3918/2021.
[13] The Right To Be Forgotten, *available at:* https://thelawtree.akmllp.com/whats-brewing/the-right-to-beforgotten/ (last visited on October 1, 2025).
[14] IAL No. 23560 of 2024.

and Google that led the debate to platform duties and the alleged training on deepfake content without the consent of the court, which is now seeking responses.[15]

1.4.4 DPDP Act Status in Courts

One more example is judicial oversight that has forced the executive to clarify the statutory enforcement operational calendar. At the end of September 2025, the Delhi High Court sought an explanation from the Union about notifications and rulemaking under the "Digital Personal Data Protection Act, 2023", indicating a need for predictable timelines that facilitate the practical development of rights and duties. Accounts of the proceeding reflect the bench's demand for a concrete schedule, which is a milestone consistent with the Act's framework concerning consent managers, breach intimation, and Board led adjudication. When the provisions are officially announced and the rules are finalized, the future writs and appeals will probably touch upon the extent of powers for inquiry, the grounds for penalty, and the

relationship with sectoral regulators, thus forming a layer of jurisprudential that AI stakeholders may link with product governance, audit design, and grievance handling. This is a very important point. The institutional scrutiny here is that DPDP is not a code of ideals but a statute that can be enforced, and its machinery must be capable of meeting the pace of AI mediated harms and remedial needs.[16]

1.4.5 Pre-DPDP Jurisprudence with AI Relevance

Before DPDP was enacted, courts had to deal with data disputes on a big scale, and they were using contract and public law frameworks. Now, these frameworks serve as cautionary markers for AI governance. The Andhra Pradesh High Court in the case "*Real Time Governance Society v. Code Tree Software Solutions Pvt. Ltd*[17] , resolved a data environment lawsuit. The practitioners often refer to this case to explain the vendor control, auditability, and breach readiness that DPDP achieves by security, accuracy, and retention control. In addition to this, the high court orders issue on online impersonation and deepfakes which have led to the rapid removal of affected material and have also revealed the possibility of criminal liability under "Section 319 of the Bharatiya Nyaya Sanhita, 2023" for cheating by personation, along with "Sections 66C and 66D of the Information Technology Act, 2000" isolated and supported by the practice of evidence under "Section 63 of the Bharatiya Sakshya Adhiniyam, 2023" for authentication of the certificate of logs, model outputs, and notices. To a degree, the Data Protection Board's directions and penalty orders, once it starts the issuance post notification, will be located among this pre DPDP storyline

[15] Bombay High Court Document (PDF), *available at:* https://bombayhighcourt.nic.in/generatenewauth.php? bhcpar= cGF0aD0uL3dyaXRlcmVhZGRhdGEvZGF0YS9vcmlnaW5hbC8yMDI0LyZmbmFtZT1GMjkwNzAwMjM 1NjAyMDI0XzEucGRmJnNtZmxhZz1OJnJqdWRkYXRlPSZ1cGxvYWRkdD0zMS8wNy8yMDI0JnNwYX NzcGhyYXNlPTAxMDgyNDAyMTAwOCZuY2l0YXRpb249JnNtY2l0YXRpb249JmRpZ2NlcnRmbGc9W SZpbnRlcmZhY2U9Tw%3D%3D (last visited on October 1, 2025).

[16] LiveLaw News Network, "Delhi High Court Questions Centre on Implementation of Digital Personal Data Protection Act", *available at:* https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-questionscentre-on-implementation-of-digital-personal-data-protection-act-305532 (last visited on October 2, 2025).

[17] (May 10, 2024).

to form an overlapped enforcement ecosystem where the court's civil remedies, administrative action, and criminal process reach AI linked privacy harms.[18]

1.5 COMPARATIVE PERSPECTIVES AND INTERNATIONAL PRACTICES

India's privacy-by-design pathway for AI can be read against three anchors: the EU's ruledense model of rights and duties, the UK's regulator-led coordination, and the OECD's principle-driven consensus that frames responsible development. The "Digital Personal Data Protection Act, 2023" already contains structural elements that travel well across borders, such as "Section 3" on scope with extraterritorial reach for services targeting individuals in India,

"Section 6" on consent as clear affirmative action, "Section 7" on specified legitimate uses, and the twin pillars of "Section 9" and "Section 10" that harden protections for children and place higher governance burdens on Significant Data Fiduciaries. A comparative lens shows where India can preserve interoperability and where it can assert a distinct approach. Consent quality sits close to the EU's standards. Legitimate uses for the State sit closer to purposelinked public interest grounds seen in Europe but will require precise rulemaking to avoid drift. Penalty design and a Board-centric enforcement track echo authority-led European models without creating a multi-regulator patchwork. The amending link with the "Right to Information Act, 2005" positions India to calibrate openness and privacy when AI systems touch judicial and administrative transparency. A reading next to the OECD AI Principles suggests alignment on human-centric design, accountability, and security, which gives Indian developers a vocabulary that already resonates in cross-border diligence and procurement. This triangulation supports Indian AI products that must move between regimes without rebuilding their compliance stack for each market.[19]

1.5.1 EU GDPR and AI Governance

The European Union (EU) has incorporated artificial intelligence (AI) within the comprehensive framework of data protection laws known as the "General Data Protection Regulation" (GDPR). "Article 6 GDPR" enumerates the lawful grounds for processing personal data along with real technical equivalents such as consent, contract, legal obligation, and legitimate interest, while "Article 22 GDPR" grants a person the right not to be subjected to a decision made solely by automated processing, including profiling, that has legal effects or significantly affects him/her. In this way, product teams are compelled to combine features with the appropriate legal basis and to create ways for human intervention which can be considered meaningful. The "Artificial Intelligence Act" subsequently superimposes a risk tiered system that bans certain AI applications directly, outlines the requirements for the system with high risk, and introduces the

[18] Real Time Governance Society, vs Code Tree Software Solutions Pvt. Ltd., *available at:* https://www.latestlaws.com/judgements/andhra-high-court/2024/may/2024-latest-caselaw-4263-ap/ (last visited on October 2, 2025).

[19] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 2, 2025).

obligations that are applicable to the general purpose of AI with a phased schedule going into 2025 and 2026 that has been confirmed by the European Commission that it will be adhered to.[20]

1.5.2 United Kingdom and OECD Trends

The UK has chosen a coordination-first model that tasks existing regulators to apply crosscutting principles, set out in the government's white paper on a pro-innovation framework, followed by a formal response that endorsed proportionate, context-sensitive oversight. This choice avoids a single AI statute while signalling that sector regulators will set expectations around transparency, safety, fairness, and contestability through guidance and rulebooks. Recent policy signals from London commit to scaling national compute and to maintaining regulator-driven oversight rather than creating an omnibus code. The practical takeaway for Indian builders is the value of early engagement with domain regulators and the need for internal "assurance by design" that presents evidence of risk proportionate controls without waiting for a prescriptive checklist. On the multilateral plane, the OECD AI Principles provide a portable grammar for trustworthy AI across fairness, transparency, accountability, robustness, and human-centricity. Indian fiduciaries can reference these principles when structuring ethics boards, evaluation benchmarks, and supplier contracts. Convergence with OECD language also eases public procurement and cross-border partnerships, since many counterparties already use these principles in due diligence. The net effect is a stable comparative baseline: maintain internal governance artefacts that speak fluently to UK regulators' expectations, while aligning product documentation and developer workflows with OECD's human-centric and accountability standards that sit comfortably beside "Section 6",
"Section 7", "Section 9", and "Section 10" in the Indian statute.[21]

1.5.3 Global Enforcement Signals

Authorities responsible for protecting data that have been active for a long time have established a regular pattern of implementing the law that provides valuable lessons that can be used by the Board led regime, which will soon be set up in India. One of the elements of the GDPR, which is the 72 hour rule for notification of the breach found in "Article 33", has become very clear in the way of doing things, with the instructions and decisions that require the affected parties to notify quickly, provide updated information, and present the evidence of control in a structured manner. The United Kingdom Information Commissioner's Office also mentions the same time that it gives public instructions, indicating that incident management is not filling in forms, but going through the stages of detection, triage, and communication very fast. In France, the trend has been to provide the developers of AI with clear instructions

[20] Art. 6 GDPR – Lawfulness of Processing, *available at:* https://gdpr-info.eu/art-6-gdpr/ (last visited on October 3, 2025).
[21] A Pro-Innovation Approach to AI Regulation (White Paper), *available at:* https://www.gov.uk/government/ publications/ai-regulation-a-pro-innovation-approach/white-paper (last visited on October 3, 2025).

on the legal grounds for training the model and on the rights of the individuals concerned in the context of AI. The CNIL is completing its recommendations for AI and releasing documents for determining the legal basis when training datasets contain the personal data of individuals. The guidance from the EDPB is progressively clarifying the rights and the expectations in case of a breach, which have a direct impact on AI heavy platforms. These signals indicate the rhythm of compliance: the continuous documentation of the legal basis, the materials on the transparency of the algorithm that can be provided to the regulators, and the audit trail for the consent, notices, withdrawals, and the updates of the model. Indian actors can internalize the rhythm already as "Section 6" and "Section 7" have been declared to set the structure for the lawful processing while "Section 9" and "Section 10" have been introduced as additional safeguards for children and Significant Data Fiduciaries. The moment that India's regulations will be fixing the breach notification timeframes as well as the standards for the recording of consent, the enforcement will probably be focusing on the same expectations thus there will be a reward for those teams which consider that explainability artefacts, DPIA style risk controls, and incident drills are their core engineering and not optional compliance.[22]

1.6 CHALLENGES

Building on this India-focused analysis of AI and data protection, several structural and operational hurdles may slow effective compliance.

- Unclear scope for AI-generated inferences can blur compliance lines. Define whether derived embeddings count as personal data and document reasoning for regulator review.
- Consent fatigue risks invalid approvals. Redesign consent flows with layered notices and visual cues that reduce overload while keeping users informed.
- Withdrawal of consent may not propagate across AI pipelines. Build automated revocation triggers that flush cached or embedded representations across model layers.
- Children's verification could prove unreliable. Combine self-declaration with ageappropriate verification APIs and retain audit logs to show due diligence.
- Cross-border data use remains uncertain pending final rules. Create conditional transfer protocols that store data locally until lawful transfer conditions are published.
- Public entities may overextend "legitimate use" grounds. Require internal legal signoff and publish a justification matrix linking each dataset to a statutory function.
- Significant Data Fiduciary audits may stall for lack of templates. Pre-draft DPIA formats aligned to Section 10 and share exemplars within industry groups.
- Platform-level redress can become fragmented. Centralize grievances in a consent manager dashboard with escalation paths to the Data Protection Board.
- Training on public data may breach expectations of privacy. Screen datasets for reidentifiable traces and record consent provenance for each data source.

[22] Art. 33 GDPR – Notification of a Personal Data Breach to the Supervisory Authority, *available at:* https://gdprinfo.eu/art-33-gdpr/ (last visited on October 3, 2025).

- Sectoral overlap could cause conflicting duties. Maintain a harmonisation register mapping RBI, TRAI, and health rules to DPDP sections to avoid regulatory gaps.

1.7 CONCLUSION

The research indicates that the Digital Personal Data Protection Act, 2023 creates an understandable framework for AI management in India by converting constitutional privacy into tangible duties for consent, correctness, and responsibility. This paper responds to the inquiry by explaining how the grounds for legality in Sections 3 11 provide the basis for every stage of the AI lifecycle, thus, data collection to model deployment, intervening both private and public actOrs Firstly, the results position that informed consent and legitimate use are not only the legal bases but also the engineering constraints that influence data minimization, notice design, and revocation mechanisms. Moreover, the children's safeguards and the Significant Data Fiduciary regime elements become the governance symmetry with high risk AI oversight present in other areas, whereas the amendments to the Right to Information Act re adjust openness and privacy. The latter serve as operational implications that can be gauged for success through reduced incidence of breach, shortened redress cycles, and audit able consent records.

Moreover, this analysis points out boundaries of the DPDP Act the precisions of its doctrines rely on the rules that are still to be issued, and its control over AI interpretations is only a matter of understanding. Despite that, the framework represents a legitimate progress through a privacy by design practice that is compatible with the globally accepted principles under the GDPR and OECD standards. The architecture of its enforcement consent managers, impact assessments, and a Data Protection Board triggers the idea of a responsible automated system that allows the keeping of innovation. The later confirmation of effectiveness should consider how the different levels of law actually change the text of the statute into the operative code, how the different sector regulators reflect the coordination of the overlapping duties, and how the judges'decisions become the balancing factors of proportional safeguards for automated decisions. The combination of these steps will provide the answer to whether India's privacy regime can be a reliable protector of human autonomy and a facilitator of ethical AI growth simultaneously.

1.8 SUGGESTIONS

Building on the insights developed in this analysis of India's AI and data protection regime, the following targeted steps convert doctrine into action.

- Map each AI workflow to its lawful ground under Sections 6 or 7 and document the rationale for audits. Keep a traceable link between data sources, consent proofs, and outputs.
- Develop modular consent dashboards that let users view, edit, and withdraw permissions in real time. Log every change and notify dependent processors automatically.
- Train engineering and legal teams together on children's data standards. Simulate compliance failures and record corrective actions as training evidence.
- Build internal DPIA templates that mirror Section 10 obligations. Require sign-off before each major model update or data expansion.

- Establish a single grievance interface integrated with consent managers. Route escalations by issue type and track resolution time as a key metric.
- Localise storage by default and activate cross-border transfers only after final rule notification. Maintain redundancy maps that show where data resides.
- Create an internal reference book aligning DPDP sections with sectoral norms from RBI, TRAI, and health regulatOrs Update it quarterly as rules evolve.
- Conduct quarterly audits on automated withdrawal propagation. Validate that revoked data no longer appears in embeddings or caches.
- Publish a short transparency report listing consent counts, withdrawals, breaches, and remediation cycles. Share anonymised metrics with the Board once operational.
- Start a compliance readiness sandbox involving regulators, developers, and civil society. Use it to test notices, consent flows, and redress models before nationwide rollout.

BIBLIOGRAPHY

- A Pro-Innovation Approach to AI Regulation (White Paper), *available at:* https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper (last visited on October 3, 2025).
- Art. 33 GDPR – Notification of a Personal Data Breach to the Supervisory Authority, *available at:* https://gdpr-info.eu/art-33-gdpr/ (last visited on October 3, 2025).
- Art. 6 GDPR – Lawfulness of Processing, *available at:* https://gdpr-info.eu/art-6-gdpr/ (last visited on October 3, 2025).
- Bharatiya Nagarik Suraksha Sanhita, 2023 (Presentation), *available at:* https://cdnbbsr.s3waas.gov.in/s3ae1eaa32d10b6c886981755d579fb4d8/uploads/2024/03/202403181642666092.pdf (last visited on September 30, 2025).
- Bombay High Court Document (PDF), *available at:* https://bombayhighcourt.nic.in/generatenewauth.php?bhcpar=cGF0aD0uL3dyaXRlcmVhZGRhdGEvZGF0YS9vcmlnaW5hbC8yMDI0LyZmbmFtZT1GMjkwNzAwMjM1NjAyMDI0XzEucGRmJnNtZmxhZz1OJnJqdWRkYXRlPSZ1cGxvYWRkdD0zMS8wNy8yMDI0JnNwYXNzcGhyYXNlPTAxMDgyNDAyMTAwOCZuY2l0YXRpb249JnNtY2l0YXRpb249JmRpZ2NlcnRmbGc9WSZpbnRlcmZhY2U9Tw%3D%3D (last visited on October 1, 2025).
- Extension of Time – Public Consultation on the Draft Digital Personal Data Protection Rules, 2025, *available at:* https://www.meity.gov.in/static/uploads/2025/02/0da2ec7e6bbf7d4803d256b9be0fadfb.pdf (last visited on September 30, 2025).
- In the Supreme Court of India, Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. — Right to Privacy (Judgment of D. Y. Chandrachud, J.), *available at:* https://www.scobserver.in/wp-content/uploads/2021/10/1-

266Right_to_Privacy__Puttaswamy_Judgment-Chandrachud.pdf (last visited on September 29, 2025).

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, *available at:* https://prsindia.org/files/ bills_acts/bills_parliament/2011/IT_Rules_2011.pdf (last visited on September 29, 2025).
- LiveLaw News Network, "Delhi High Court Questions Centre on Implementation of Digital Personal Data Protection Act", *available at:* https://www.livelaw.in/high-court/ delhi-high-court/delhi-high-court-questions-centre-on-implementation-of-digitalpersonal-data-protection-act-305532 (last visited on October 2, 2025).
- Meera Khanna, *Privacy by Design Under the Digital Personal Data Protection Act* (Universal Law Publishing, Delhi, 1st edn., 2023).
- Nikhil Batra, *Data Protection and Artificial Intelligence in India* (Eastern Book Company, Lucknow, 1st edn., 2023).
- Raghav Menon, *Algorithmic Accountability and Indian Data Governance* (LexisNexis, Gurugram, 1st edn**., 2022).**
- Real Time Governance Society, vs Code Tree Software Solutions Pvt. Ltd., *available at:* https://www.latestlaws.com/judgements/andhra-high-court/2024/may/2024-latestcaselaw-4263-ap/ (last visited on October 2, 2025).
- The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), *available at:* https:// www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 2, 2025).
- The Right To Be Forgotten, *available at:* https://thelawtree.akmllp.com/whatsbrewing/the-right-to-be-forgotten/ (last visited on October 1, 2025).