
SAFEGUARDING PERSONAL DATA IN THE AGE OF ARTIFICIAL INTELLIGENCE: AN ASSESSMENT OF THE DPDP ACT, 2023

Swasti Gupta, Faculty Member, ICFAI University, Ranchi

ABSTRACT

Artificial Intelligence (AI) has emerged as a transformative force in contemporary governance, business operations, and social infrastructure. Its ability to process and analyse vast volumes of data has significantly enhanced efficiency, innovation, and decision-making across multiple sectors. However, the increasing reliance on AI-driven systems has also raised serious concerns regarding privacy, data protection, transparency, accountability, and individual autonomy. The collection and processing of personal data by AI technologies often create risks of algorithmic bias, discriminatory outcomes, automated decision-making without adequate human oversight, and intrusive surveillance practices. In India, the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) marks a significant step towards establishing a legal framework for protecting personal data in the digital age. Nevertheless, the Act primarily focuses on data protection and does not comprehensively address the unique challenges posed by artificial intelligence systems. This paper critically analyses the adequacy of the DPDP Act in regulating AI-related privacy concerns and compares its provisions with the European Union's General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act (AI Act). Through a comparative and doctrinal approach, the study identifies regulatory gaps within the Indian framework and proposes a risk-based, rights-oriented, and technology-sensitive legal model capable of balancing innovation with the protection of privacy and fundamental rights.

Keywords: Artificial Intelligence (AI), Data Privacy, Data Protection, Digital Personal Data Protection Act, 2023 (DPDP Act), Surveillance, Privacy Rights.

I. INTRODUCTION

Artificial Intelligence (AI) systems operate through a continuous data lifecycle involving data collection, digitisation, storage, training, deployment, monitoring, and periodic retraining. The Digital Personal Data Protection Act, 2023 (DPDP Act) establishes the legal framework governing each of these stages by requiring that personal data processing be based either on valid consent or specified legitimate uses. The Act also imposes obligations on data fiduciaries and data processors to ensure responsible handling of personal data in AI-driven environments. Organisations developing AI systems frequently rely on large volumes of user-generated data, including clicks, voice recordings, images, videos, and sensor-generated information for supervised, unsupervised, or reinforcement learning. Such entities must ensure compliance with statutory requirements relating to notice, consent, data retention, and breach reporting. Similarly, entities deploying AI systems for purposes such as fraud detection, credit scoring, content moderation, predictive analytics, and recommendation services are required to maintain the accuracy and completeness of data where decisions may affect individuals or where data is shared with third parties. Appropriate technical and organisational safeguards must also be implemented depending on the level of risk associated with datasets and AI models. Government agencies using AI for welfare administration, public health programmes, digital identity management, and other public functions may rely on the “certain legitimate uses” provisions under the DPDP Act. Nevertheless, such authorities remain subject to statutory obligations, accountability requirements, and grievance redressal mechanisms established under the Act. The DPDP Act applies to digital personal data processed within India as well as to processing activities conducted outside India when such processing relates to offering goods or services to individuals located in India. At the same time, the Act excludes personal or domestic activities and information that has been voluntarily made publicly available by the individual or under any law. These provisions significantly influence the composition of AI training datasets, testing environments, and model evaluation frameworks. The extraterritorial application of the Act is particularly important for multinational AI companies that process or fine-tune models using data relating to Indian users. Consent under the Act must be free, specific, informed, unconditional, and unambiguous. This requirement limits the use of personal information for purposes beyond those originally disclosed and necessitates transparent consent mechanisms such as layered notices, granular user controls, and simple withdrawal procedures. Where consent is withdrawn, data fiduciaries are required to cease processing activities and ensure that associated processors also discontinue processing

unless another lawful basis exists. This has important implications for AI infrastructure, including training datasets, feature stores, cached embeddings, and backup systems. The Act also provides enhanced safeguards for children's personal data. Processing such data requires verifiable parental consent and prohibits tracking, behavioural monitoring, and targeted advertising directed at children. These restrictions significantly affect sectors such as educational technology, gaming platforms, and digital advertising systems that depend on behavioural analytics and engagement metrics. Furthermore, the regulatory framework relating to Significant Data Fiduciaries introduces additional governance obligations, including Data Protection Impact Assessments, independent audits, and the appointment of a Data Protection Officer based in India. These requirements encourage stronger oversight, accountability, and risk management practices in organisations deploying large-scale AI systems. Collectively, the DPDP Act incorporates privacy-by-design principles into the AI lifecycle. By balancing consent-based processing and legitimate uses with duties, rights, and penalties, the legislation seeks to promote innovation while safeguarding privacy, autonomy, transparency, and accountability in increasingly data-driven and algorithmic environments.

II. Historical Background and Development

The evolution of Artificial Intelligence (AI) governance in India reflects a gradual transition from fragmented sector-specific privacy protections to a comprehensive statutory framework governing digital personal data. As AI technologies increasingly rely on large-scale data collection, processing, and automated decision-making, concerns relating to privacy, transparency, accountability, and misuse of personal information have gained significant importance. In response to these challenges, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), establishing a unified legal framework for the processing of digital personal data across various sectors and technological environments. The DPDP Act applies to digital personal data processed within India as well as to processing activities conducted outside India when such processing is connected to the offering of goods or services to individuals located in India. At the same time, the Act excludes certain categories of processing, including personal or domestic activities and specific forms of publicly available information. Section 3 defines the scope and applicability of the legislation, while Section 6 establishes consent as the primary lawful basis for processing personal data. Such consent must be free, specific, informed, unconditional, and unambiguous¹. Section 7 provides for certain

¹ Schuck, P. H., Rethinking Informed Consent, 103(4) The Yale Law Journal (YLJ) 899, 915 (1994),

legitimate uses where consent may not be required, and Sections 9 and 10 introduce additional safeguards relating to children's personal data and Significant Data Fiduciaries. These provisions have direct implications for the development and deployment of AI systems. Developers collecting large datasets for machine learning and AI training must design mechanisms for notice, consent, retention, and security compliance. Similarly, organisations deploying AI applications are required to integrate privacy-by-design principles into data collection and processing workflows. Public authorities relying on statutory functions for processing personal data must also ensure compliance with the safeguards and accountability measures prescribed under the Act. Consequently, the DPDP Act establishes a legal foundation that influences the entire AI lifecycle, from data acquisition and model training to deployment and monitoring².

The origins of India's modern data protection framework can be traced to the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules introduced basic obligations relating to notice, consent, security measures, and retention of sensitive personal information by corporate entities. However, the framework lacked comprehensive data subject rights, independent regulatory oversight, and a general lawful basis structure applicable across sectors. As digital technologies expanded rapidly, the limitations of the existing framework became increasingly evident. Recognising the need for comprehensive reform, the Government of India constituted the Committee of Experts under the chairmanship of Justice B. N. Srikrishna. The Committee's report, submitted in July 2018, recommended the enactment of a dedicated data protection law based on individual rights, accountability, and responsible data governance. The recommendations formed the basis for successive legislative drafts that eventually culminated in the enactment of the Digital Personal Data Protection Act, 2023.

The DPDP Act represents a significant shift from the earlier SPDI framework by introducing a rights-based model with extraterritorial application, consent-centric processing requirements, safeguards for children, obligations for Significant Data Fiduciaries, and institutional enforcement mechanisms through the Data Protection Board of India. To facilitate implementation of the Act, the Government subsequently released the Draft Digital Personal

<https://doi.org/10.2307/797066>(1994).

² Samuel D. Warren and Louis D. Brandeis, *The Right To Privacy*, 4 HARVARD LAW REVIEW (HLV) 193, 193 (1890)

Data Protection Rules, 2025, for public consultation. The consultation process invited comments from industry stakeholders, legal experts, civil society organisations, and technology companies, reflecting an inclusive and iterative approach to regulatory development. The evolution of India's data protection regime demonstrates a conscious effort to balance technological innovation with the protection of privacy and fundamental rights. As AI systems become increasingly embedded in governance, commerce, healthcare, education, and public services, the DPDP Act and its accompanying rules are expected to play a crucial role in shaping responsible AI governance and ensuring accountability in data-driven decision-making environments.

III. CONSTITUTIONAL PROVISIONS

The constitutional foundation of data privacy and protection in India is primarily derived from Article 21 of the Constitution, which guarantees the right to life and personal liberty. The scope of Article 21 was significantly expanded by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*³, wherein a nine-judge Constitution Bench unanimously recognised the right to privacy as a fundamental right. The Court held that privacy is an intrinsic part of human dignity, autonomy, and personal liberty, thereby establishing informational self-determination as a constitutional value. The judgment further laid down that any restriction upon privacy by the State must satisfy the tests of legality, necessity, and proportionality. These constitutional principles have become particularly relevant in the age of Artificial Intelligence, where extensive collection, processing, and analysis of personal data form the basis of algorithmic decision-making. The principles enunciated in *Puttaswamy* provide important constitutional safeguards for AI-driven data ecosystems. State authorities and private entities involved in automated processing must ensure that the collection and use of personal data are supported by valid legal authority and are proportionate to the objectives sought to be achieved. The Digital Personal Data Protection Act, 2023 reflects these constitutional requirements by providing lawful grounds for processing personal data, including consent-based processing and certain legitimate uses under Section 7. The Act also permits specific exemptions for research, archiving, and public interest purposes, subject to prescribed safeguards. Further, the framework recognises limited relaxations for certain State functions, while maintaining

³ (2017) 10 SCC 1

accountability mechanisms intended to protect the rights and interests of data principals⁴.

The constitutional discourse on privacy has also influenced the relationship between privacy rights and transparency obligations. A notable development is the amendment to Section 8(1)(j) of the Right to Information Act, 2005, through the Digital Personal Data Protection Act, 2023. The amendment narrows the circumstances under which personal information may be disclosed under the RTI regime, thereby strengthening privacy protections for individuals. At the same time, it does not eliminate the principle of transparency in public administration or judicial proceedings. Consequently, adjudicatory bodies and public authorities are required to balance the competing values of privacy and accountability by ensuring that personal information is protected while preserving the transparency necessary for public scrutiny and good governance. Thus, the constitutional framework established under Article 21, as interpreted in *the Justice K.S. Puttaswamy case*, continues to serve as the normative foundation for India's evolving data protection regime. The principles of dignity, autonomy, legality, necessity, and proportionality provide essential guidance for regulating Artificial Intelligence and ensuring that technological innovation remains consistent with constitutional guarantees and individual rights⁵.

IV. LEGISLATIVE AND INSTITUTIONAL FRAMEWORK

The legislative and institutional framework governing Artificial Intelligence-related personal data processing in India is primarily anchored in the Digital Personal Data Protection Act, 2023 (DPDP Act). The Act establishes a comprehensive legal framework for regulating the collection, storage, use, sharing, and processing of digital personal data throughout the AI lifecycle, including data acquisition, model training, testing, deployment, and post-deployment monitoring. It represents India's first dedicated data protection legislation and serves as the principal legal instrument for balancing technological innovation with the protection of individual privacy rights. The scope of the Act extends to the processing of digital personal data within India and also possesses extraterritorial application where personal data is processed outside India in connection with offering goods or services to individuals located in India. At the same time, the Act excludes certain categories of processing, including personal or domestic activities and personal data that has been made publicly available by the data

⁴ Tandon, U., & Gupta, N. (2025). Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. *Legal Issues in the Digital Age*. <https://doi.org/10.17323/2713-2749.2025.2.87.117>

⁵ Right to Information Act, 2005, Section 8(1)(j), as amended by the Digital Personal Data Protection Act, 2023.

principal or under any law for the time being in force. This broad scope is particularly relevant for AI developers and technology companies that process large datasets containing information relating to Indian users.

A central feature of the DPDP Act is its consent-based framework. Consent must be free, specific, informed, unconditional, and unambiguous, and must be signified through a clear affirmative action. Data principals are also entitled to withdraw consent as easily as it was provided. These requirements have significant implications for AI systems that rely on personal data for training and analytics, compelling organisations to establish transparent consent mechanisms, granular user controls, auditable consent records, and effective withdrawal procedures. Where consent is withdrawn, data fiduciaries and processors must cease processing unless another lawful ground for processing exists⁶. Apart from consent, the Act recognises certain legitimate uses under which personal data may be processed without obtaining consent. These include specific State functions, compliance with legal obligations, medical emergencies, disaster management, and other purposes expressly recognised under the statute. Such provisions are particularly relevant in contexts involving public welfare programmes, digital governance initiatives, cybersecurity responses, and public health analytics, where AI technologies are increasingly utilised for decision-making and service delivery.³

The Act also incorporates special safeguards for children's personal data by requiring verifiable parental consent and restricting behavioural monitoring, tracking, and targeted advertising directed at children. Additionally, the legislation introduces the concept of Significant Data Fiduciaries, which are entities designated by the Central Government based on factors such as volume and sensitivity of data processed, risk to data principals, and impact on national interests. These entities are subject to enhanced obligations, including the appointment of a Data Protection Officer, the conduct of Data Protection Impact Assessments, periodic audits, and the implementation of robust compliance mechanisms⁷. Another important feature of the framework is the recognition of data principal rights, including the rights to access information about personal data processing, seek correction and erasure of personal data, nominate another person to exercise rights in certain circumstances, and avail themselves of grievance redressal mechanisms. These rights aim to strengthen individual control over personal information and enhance accountability in AI-driven environments where automated processing may

⁶ Digital Personal Data Protection Act, 2023, Section 6.

⁷ Digital Personal Data Protection Act, 2023, Sections 9 and 10.

significantly affect individuals. Institutionally, the Act establishes the Data Protection Board of India as the primary adjudicatory and enforcement authority. The Board is empowered to investigate breaches, impose penalties, direct remedial measures, and adjudicate complaints arising from violations of the Act. The legislation also provides a structured system for appeals and enforcement, thereby creating an institutional mechanism for ensuring compliance and accountability among data fiduciaries and processors⁸.

A. DPDP Act, 2023: Structure and Principles

The Digital Personal Data Protection Act, 2023 (DPDP Act) establishes the foundational legal framework governing the collection, processing, storage, and use of digital personal data in India. The Act is particularly significant in the context of Artificial Intelligence (AI), as AI systems heavily depend on the collection and processing of large volumes of personal data throughout their lifecycle. The principles embodied in the Act define the boundaries within which AI developers, deployers, and data fiduciaries must operate while designing, training, and deploying AI systems. The scope of the Act is defined under Section 3, which extends to all digital personal data collected in digital form as well as personal data initially collected in non-digital form and subsequently digitised. The Act also possesses extraterritorial application, covering processing activities undertaken outside India where such processing relates to offering goods or services to individuals located within India. This broad jurisdictional reach is particularly relevant for multinational technology companies and AI platforms that process data relating to Indian users. Consent forms the cornerstone of the DPDP Act. Section 6 provides that consent must be free, specific, informed, unconditional, and unambiguous, and must be expressed through a clear affirmative action. The provision seeks to ensure that individuals exercise meaningful control over their personal information. Where processing is based on consent, the data principal must be able to withdraw such consent with the same ease with which it was provided. Upon withdrawal, the data fiduciary and its processors are required to cease processing the relevant personal data unless another lawful basis exists. These requirements have significant implications for AI systems that rely on personal data for model training, analytics, profiling, and automated decision-making, necessitating transparent consent mechanisms and effective data management processes. Apart from consent-based processing, Section 7 of the Act recognises certain legitimate uses that permit processing without obtaining

⁸ Adhithya, M., & K, K. (2026). Data Privacy and Protection in India: A Critical Doctrinal Analysis of the Digital Personal Data Protection Act, 2023 In The Light Of Constitutional Standards And International Benchmarks. *Indian Journal of Legal Review*. <https://doi.org/10.65393/Ijlr6i73>

prior consent. These include processing for State functions, provision of government benefits and services, compliance with legal obligations, medical emergencies, disaster management, and other specified purposes⁹. While these exemptions facilitate efficient governance and public service delivery, they continue to operate within a framework of accountability and statutory safeguards. In the context of AI, these provisions support the use of data for welfare administration, public health initiatives, cybersecurity measures, and other public interest functions. The Act also provides enhanced safeguards for children's personal data under Section 9. Data fiduciaries are required to obtain verifiable parental consent before processing personal data relating to children. Furthermore, the legislation prohibits tracking, behavioural monitoring, and targeted advertising directed at children. These restrictions have substantial implications for AI-driven platforms operating in sectors such as education technology, gaming, social media, and digital advertising, where algorithmic systems frequently rely on behavioural data and user profiling techniques. An important feature of the Act is the introduction of the Significant Data Fiduciary (SDF) framework under Section 10. The Central Government may designate certain entities as Significant Data Fiduciaries based on factors such as the volume and sensitivity of personal data processed, risk to the rights of data principals, and impact on national interests. Such entities are subject to additional compliance obligations, including conducting Data Protection Impact Assessments, undertaking periodic audits, appointing a Data Protection Officer based in India, and implementing enhanced governance measures. These obligations closely align with contemporary AI governance principles, particularly in relation to model risk management, accountability, algorithmic oversight, and regulatory compliance. The structure of the DPDP Act reflects a balanced approach that seeks to facilitate innovation while protecting privacy and individual autonomy. By combining consent-based processing, legitimate-use exceptions, child protection measures, and enhanced obligations for Significant Data Fiduciaries, the Act establishes a comprehensive governance framework capable of addressing many of the data protection challenges posed by AI technologies. As India continues to expand its digital economy and AI ecosystem, the principles embodied in the DPDP Act are likely to play a central role in shaping responsible and accountable AI development.

B. Draft DPDP Rules, 2025

The Draft Digital Personal Data Protection Rules, 2025 have been proposed to operationalise

⁹ Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age. *International Journal of Law in a Changing World*. <https://doi.org/10.54934/ijlew.v3i2.84>

and supplement the provisions of the Digital Personal Data Protection Act, 2023. While the Act establishes the broad legal framework governing digital personal data, the Draft Rules seek to provide procedural clarity regarding compliance obligations, implementation mechanisms, and regulatory oversight. These Rules are particularly significant for Artificial Intelligence (AI) systems, as they translate statutory requirements into practical compliance standards that organisations must follow during the development, training, deployment, and monitoring of AI technologies¹⁰.

The Ministry of Electronics and Information Technology (MeitY) released the Draft DPDP Rules, 2025 for public consultation in January 2025, inviting comments from stakeholders including industry representatives, technology companies, academics, civil society organisations, and legal experts. Subsequently, the consultation period was extended to facilitate wider participation and to ensure that diverse viewpoints were considered before finalisation of the Rules. The consultative approach adopted by the Government reflects the importance of creating a balanced regulatory framework capable of promoting innovation while safeguarding privacy and data protection rights¹¹. The Draft Rules provide greater clarity regarding the form and content of privacy notices, consent management mechanisms, maintenance of consent records, registration requirements for Consent Managers, and obligations relating to grievance redressal. They also prescribe procedural requirements concerning data breach notifications, including timelines, formats, and reporting obligations. These provisions are expected to significantly influence the design and operation of AI systems by requiring organisations to establish transparent consent processes, maintain auditable records of data processing activities, and develop robust accountability frameworks¹².

Another important aspect of the Draft Rules relates to Significant Data Fiduciaries (SDFs). The Rules contemplate detailed requirements concerning risk assessments, compliance audits, governance mechanisms, and oversight structures. These obligations closely resemble Data Protection Impact Assessment (DPIA) frameworks adopted in other jurisdictions and are particularly relevant for organisations deploying large-scale AI systems that process significant

¹⁰ Malhotra, C., & Malhotra, U. (2024). Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India. *Indian Journal of Public Administration*, 70, 516 - 531. <https://doi.org/10.1177/0019556124127157>

¹¹ Ministry of Electronics and Information Technology (MeitY), Draft Digital Personal Data Protection Rules, 2025 (Public Consultation Paper, January 2025).

¹² Meera Khanna, *Privacy by Design Under the Digital Personal Data Protection Act* (Universal Law Publishing, Delhi, 1st edn., 2023).

volumes of personal data. Such requirements encourage a risk-based approach to AI governance, requiring organisations to evaluate potential privacy harms, implement mitigation measures, and periodically review the effectiveness of their compliance programmes. The Draft Rules are also expected to influence technical and operational aspects of AI deployment. Requirements relating to consent management, record maintenance, breach reporting, and audit trails will directly affect data architecture, system design, logging mechanisms, dashboard functionalities, and internal compliance processes. Organisations involved in training and deploying AI models at scale will need to establish detailed governance protocols to demonstrate compliance with statutory obligations and regulatory expectations¹³.

Industry discussions surrounding the Draft Rules have also highlighted potential provisions concerning cross-border data transfers and data localisation preferences. If such provisions are retained in the final Rules, they may significantly influence decisions relating to data storage infrastructure, cloud computing arrangements, AI model training environments, and the location of fine-tuning and inference operations. For multinational AI companies processing data relating to Indian users, these requirements may have substantial operational and compliance implications. Government statements issued during 2025 have indicated a phased implementation strategy for the DPDP framework. Such an approach is intended to provide organisations with sufficient time to establish compliance systems and adapt existing business processes to the new regulatory requirements. Ministerial communications have also suggested that the final Rules would be issued following completion of stakeholder consultations, thereby marking a critical milestone in the operationalisation of India's data protection regime. Once notified, the Rules will activate detailed compliance timelines relating to consent management, registration requirements, breach reporting obligations, and other statutory duties under the DPDP Act¹⁴. The Draft Digital Personal Data Protection Rules, 2025 therefore represent a crucial component of India's emerging data governance architecture. By providing procedural clarity and operational guidance, the Rules are expected to strengthen the implementation of the DPDP Act while ensuring that AI innovation develops within a framework that promotes transparency, accountability, privacy protection, and responsible data processing practices.

¹³ Ministry of Electronics and Information Technology (MeitY), Official Statements and Consultation Updates, 2025.

¹⁴ Industry and stakeholder submissions on the Draft Digital Personal Data Protection Rules, 2025.

V. JUDICIAL APPROACH TO PRIVACY AND ARTIFICIAL INTELLIGENCE

The most significant judicial development in the field of privacy and data protection is the landmark decision of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* [(2017) 10 SCC 1]. In this historic judgment, a nine-judge Constitution Bench unanimously recognised the right to privacy as a fundamental right under Article 21 of the Constitution of India. The Court held that privacy is an essential component of human dignity, personal liberty, and individual autonomy. It further established that any restriction on the right to privacy must satisfy the constitutional requirements of legality, necessity, and proportionality. The principles laid down in *Puttaswamy* have acquired immense significance in the era of Artificial Intelligence and data-driven technologies. As AI systems increasingly rely on the collection, processing, and analysis of personal data, the constitutional safeguards articulated by the Court provide an important framework for evaluating the legality of such processing activities. Automated decision-making systems that influence employment opportunities, credit scoring, welfare distribution, law enforcement, and online recommendations must operate within the boundaries of legality and proportionality while respecting the privacy rights of individuals. The judgment has also influenced the structure of the Digital Personal Data Protection Act, 2023. The requirement of free, informed, and unambiguous consent under Section 6 reflects the constitutional emphasis on individual autonomy and informational self-determination. Similarly, the legitimate-use provisions under Section 7 attempt to balance public interests with privacy rights by permitting certain forms of processing while maintaining accountability safeguards. The statutory obligations relating to accuracy, security measures, and erasure rights further reinforce the privacy protections recognised by the Supreme Court. An important contribution of the *Puttaswamy* judgment is its recognition of informational self-determination as a core aspect of privacy. The Court acknowledged that individuals should have meaningful control over the collection, use, and dissemination of their personal information. This principle has become increasingly relevant in AI ecosystems where algorithms can analyse, replicate, and amplify personal information on an unprecedented scale. By establishing privacy as a constitutional value, the judgment provides a normative foundation for regulating AI technologies and preventing disproportionate intrusions into individual autonomy. The decision has also influenced the development of judicial remedies in cases involving digital privacy violations. Courts increasingly rely on the principles articulated in *Puttaswamy* when granting relief against unlawful disclosure of personal information, online harassment, identity misuse, deepfakes, and other technology-enabled harms. Through measures such as content

removal, de-indexing, redaction, and privacy-protective orders, the judiciary seeks to preserve individual dignity while maintaining the principles of transparency and open justice.

A. Right to Be Forgotten and Emerging Privacy Jurisprudence

The development of the right to be forgotten in India has significant implications for Artificial Intelligence, particularly in relation to the collection, storage, indexing, and dissemination of personal information through digital platforms and AI-driven systems. Although the right has not yet been expressly codified as an independent statutory right, Indian courts have increasingly recognised the need to balance privacy interests with transparency, freedom of expression, and the principle of open justice. Judicial decisions addressing requests for removal, de-indexing, or redaction of personal information have contributed to the evolution of this emerging doctrine¹⁵.

A notable development occurred in *Jorawar Singh Mundy v. Union of India*¹⁶, where the Delhi High Court granted interim relief by directing the removal and de-indexing of certain online records relating to criminal proceedings in which the petitioner had been acquitted. The Court recognised that continued accessibility of such records through search engines could cause serious reputational harm despite the petitioner having been exonerated. The decision highlighted that selective de-indexing and obscuring of records may serve as an effective mechanism for protecting privacy without completely undermining judicial transparency. The debate surrounding the right to be forgotten gained further significance when the Supreme Court considered issues relating to the removal or redaction of judicial records available in the public domain. In 2024, the Court stayed an order of the Madras High Court that had directed a legal search engine to remove an acquittal judgment from its database. By granting the stay, the Supreme Court recognised the broader constitutional and legal implications of balancing privacy rights against the principles of open justice and public access to judicial records. The matter highlighted the need for a carefully calibrated approach rather than complete erasure of information from public archives¹⁷.

¹⁵ Nikhil Batra, *Data Protection and Artificial Intelligence in India* (Eastern Book Company, Lucknow, 1st edn., 2023).

¹⁶ 2021 SCC OnLine Del 2306.

¹⁷ Saha, S., & Mukhopadhyay, S. (2024). A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023. *International Journal of Law and Social Sciences*. <https://doi.org/10.60143/ijls.v10.i1.2024.114>

B. AI, Personality Rights, and Platform Liability

The rapid development of Artificial Intelligence has generated significant concerns regarding the protection of personality rights, particularly in relation to voice cloning, deepfakes, synthetic media, and the unauthorised commercial exploitation of an individual's identity. Indian courts have increasingly recognised that the use of a person's name, image, voice, likeness, or other identifiable attributes without consent may constitute a violation of personality rights and privacy interests. These judicial developments have important implications for generative AI systems that are capable of replicating or imitating human characteristics through advanced machine learning techniques. A landmark development in this area occurred in *Arijit Singh v. Codible Ventures LLP & Ors*¹⁸. (Bombay High Court, 2024), where the Court granted interim protection against the unauthorised use of the singer's personality attributes. The Court restrained the defendants from using Artificial Intelligence tools to clone the singer's voice, reproduce his likeness, or exploit his identity for commercial purposes without authorisation. The Court also directed intermediaries and online platforms to cooperate in removing infringing content and preventing further dissemination. This decision highlighted the growing judicial recognition that AI-generated reproductions of an individual's identity can result in serious violations of privacy, reputation, and economic rights.

C. AI, Personality Rights and Platform Responsibility

Indian courts have increasingly recognised that the unauthorised creation and use of synthetic identity attributes through Artificial Intelligence may violate personality rights and privacy interests. Judicial decisions indicate that the replication of a person's voice, image, likeness, or other identifiable characteristics without consent is unlawful and may result in legal consequences. These developments have significant implications for generative AI systems, particularly those capable of producing realistic voice clones, deepfakes, and other forms of synthetic media.

A notable example is *Arijit Singh v. Codible Ventures LLP & Ors*.¹⁹, where the Bombay High Court granted interim protection against the unauthorised use of the singer's personality attributes through Artificial Intelligence technologies. The Court restrained the use of AI tools for voice cloning and other activities that could exploit the singer's identity without permission.

¹⁸ Bombay High Court, Interim Order, 2024.

¹⁹ Interim Order, Bombay High Court, 2024.

It also directed the removal of infringing content and required cooperation from intermediaries to prevent further misuse. This decision underscored the principle that technological innovation cannot justify the unauthorised commercial exploitation of an individual's identity. The Bombay High Court further strengthened this principle by extending protection to renowned singer Asha Bhosle against the unauthorised cloning of her voice through AI technologies. The Court recognised that a celebrity's voice constitutes a distinctive aspect of personality and is therefore entitled to legal protection. The decision reaffirmed that personality rights extend beyond physical likeness and may include unique personal attributes such as voice, reputation, and identity²⁰.

The debate concerning AI-generated content has also expanded to questions of platform liability and intermediary responsibility. In 2025, Abhishek Bachchan and Aishwarya Rai Bachchan initiated proceedings before the Delhi High Court against YouTube and Google concerning the circulation of alleged deepfake content and the use of personality attributes without consent. The litigation has brought attention to the responsibilities of digital platforms in preventing the dissemination of AI-generated misinformation and identity misuse. It has also raised broader concerns regarding the use of publicly available content for training AI models without obtaining the consent of affected individuals²¹. Indian courts have increasingly addressed disputes arising from digital data environments, online impersonation, and emerging AI-related harms. A significant example is *Real Time Governance Society v. Code Tree Software Solutions Pvt. Ltd.*, where the Andhra Pradesh High Court dealt with issues relating to data governance and technological systems. The case is frequently cited to illustrate the importance of vendor accountability, auditability, data security, and breach preparedness in technology-driven environments. The principles emerging from the case resonate with the objectives of the Digital Personal Data Protection Act, 2023, particularly concerning security safeguards, data accuracy, and responsible data management.

Courts have also responded proactively to cases involving online impersonation, deepfakes, and unauthorised digital representations. Various judicial orders have directed the prompt removal of misleading or harmful online content, recognising the serious risks posed by AI-generated misinformation and identity misuse. These decisions demonstrate the judiciary's willingness to provide immediate remedies where technological tools are used to infringe

²⁰ *Asha Bhosle v. Various Defendants*, Bombay High Court, 2024.

²¹ *Abhishek Bachchan and Aishwarya Rai Bachchan v. Google LLC & YouTube*, Delhi High Court Proceedings, 2025.

privacy, reputation, or personality rights²². The legal consequences of such conduct may extend beyond civil remedies. AI-generated impersonation and deceptive digital content can attract criminal liability under *Section 319 of the Bharatiya Nyaya Sanhita, 2023*, which deals with cheating by personation. In addition, *Sections 66C and 66D of the Information Technology Act, 2000* provide penalties for identity theft and cheating by personation through computer resources. These provisions create an important statutory framework for addressing AI-enabled fraud and digital identity misuse. The evidentiary aspects of AI-related disputes are equally significant. *Section 63 of the Bharatiya Sakshya Adhiniyam, 2023*, governs the admissibility of electronic records and computer-generated evidence. As a result, digital logs, AI-generated outputs, system records, notices, and electronic certificates play a crucial role in establishing authenticity and proving misconduct in legal proceedings. This evidentiary framework supports the effective adjudication of disputes arising from automated systems and digital platforms.

VI. Gaps in the Indian Legal Framework in Relation to AI and Data Privacy

The Digital Personal Data Protection Act, 2023, represents a significant step towards protecting personal data in India. However, the rapid growth of Artificial Intelligence has exposed several regulatory gaps that the existing framework does not adequately address. While the Act establishes general principles relating to data processing, consent, and accountability, it does not provide a comprehensive framework for managing AI-specific risks such as algorithmic bias, automated decision-making, explainability, and large-scale surveillance. These shortcomings create challenges for both individuals and organisations operating in an increasingly AI-driven environment.

A. Lack of AI-Specific Regulations

One of the most significant gaps in the current legal framework is the absence of specific regulations governing Artificial Intelligence systems. Although the DPDP Act provides safeguards for personal data, it does not address the unique characteristics of AI technologies. AI systems rely on continuous access to large volumes of data for training, testing, and improvement. This increases the possibility of data misuse, unauthorised processing, and

²² Bharatiya Nyaya Sanhita, 2023, s. 319; Information Technology Act, 2000, ss. 66C & 66D; Bharatiya Sakshya Adhiniyam, 2023, s. 63; Digital Personal Data Protection Act, 2023.

privacy violations, particularly when personal information is used beyond the purposes for which consent was originally obtained. As AI models evolve through machine learning processes, it becomes increasingly difficult to ensure that personal data remains protected throughout the entire lifecycle of the system.

B. Cross-Border Data Transfers

The global nature of AI systems presents significant challenges for data protection, particularly in relation to cross-border data transfers. Cross-border transfer refers to the movement of personal data from one country to another for processing, storage, or analysis. Such transfers are common among multinational corporations, cloud service providers, and organisations engaged in international business operations. The DPDP Act attempts to regulate cross-border data flows through Section 16(1), which empowers the Central Government to restrict transfers to countries that do not provide adequate levels of data protection or pose national security concerns. However, the Act does not clearly specify the criteria for identifying such countries. The lack of transparency regarding the process of permitting or restricting data transfers creates uncertainty for businesses and limits regulatory predictability.

C. Accountability and Transparency

Transparency and accountability are fundamental principles of responsible AI governance. However, the DPDP Act does not impose explicit obligations requiring AI developers or deployers to explain how algorithmic decisions are made. Many AI systems operate as “black box” models, making it difficult for users, regulators, and affected individuals to understand the reasoning behind automated outcomes. The absence of AI explainability requirements raises concerns regarding fairness, discrimination, and accountability.

D. Broad Exemptions for Government Processing

The DPDP Act grants broad exemptions to government agencies for processing personal data in matters relating to sovereignty, national security, public order, and similar public interests. While such exemptions may be necessary in certain circumstances, they raise concerns regarding surveillance, oversight, and accountability. The use of AI-powered systems by government authorities for monitoring, profiling, predictive analysis, and public service delivery may significantly affect individual privacy rights. Broad exemptions can potentially

reduce transparency and limit the ability of citizens to challenge intrusive data processing practices. Therefore, while government agencies may require flexibility to perform public functions, appropriate safeguards must be implemented to ensure that data principals are not subjected to arbitrary or disproportionate interference with their privacy rights.

E. Automated Decision-Making

Automated decision-making represents another significant gap within the Indian legal framework. AI systems are increasingly used in recruitment processes, financial services, credit assessments, insurance underwriting, law enforcement, and predictive policing. Decisions generated through these systems can directly affect an individual's rights, opportunities, and access to essential services. Unlike Article 22 of the General Data Protection Regulation (GDPR), which provides safeguards against decisions based solely on automated processing, the DPDP Act does not contain specific provisions regulating automated decision-making. The absence of such protections may result in biased, discriminatory, or unfair outcomes without adequate human oversight. Without explicit legal safeguards, individuals may have limited ability to challenge automated decisions or seek meaningful explanations regarding how such decisions were reached. Given the growing reliance on AI technologies in both public and private sectors, the regulation of automated decision-making should be recognised as a critical area requiring legislative attention.

VII. Recommendations

The existing legal framework governing data protection in India, particularly the Digital Personal Data Protection Act, 2023, primarily focuses on the protection of personal data and privacy rights. While the Act establishes important safeguards relating to consent, lawful processing, and data security, it does not comprehensively regulate the functioning of Artificial Intelligence systems throughout their lifecycle. AI technologies operate across multiple stages, including data collection, model training, deployment, monitoring, and automated decision-making. Consequently, India requires a more comprehensive and AI-specific regulatory framework that balances technological innovation with privacy, transparency, accountability, and public trust.

A. Risk-Based Classification of AI Systems

A risk-based approach should form the foundation of India's future AI governance framework.

At present, India lacks a formal mechanism for classifying AI systems according to the level of risk they pose to individuals and society. AI applications differ significantly in their impact, with some systems presenting minimal risks while others may directly affect fundamental rights, health, safety, and economic opportunities. Therefore, AI systems should be categorised based on the potential harms they may cause, including misuse of personal data, discrimination, loss of user autonomy, security vulnerabilities, and societal risks.

B. Algorithmic Audits and Transparency

Transparency and accountability should be central components of AI governance. Organisations processing personal data through AI systems should be required to conduct regular algorithmic audits to identify privacy risks, biases, discriminatory outcomes, and anti-competitive effects. Such audits may be conducted internally or by independent third parties to ensure objectivity and compliance with regulatory standards. Alongside audits, organisations should disclose essential information regarding the functioning of AI systems, including the nature of datasets used, model training methodologies, intended objectives, and key decision-making parameters. Increased transparency would reduce information asymmetry between AI developers, regulators, and affected individuals.

C. Privacy Impact Assessments and Design Safeguards

India should adopt the principle of Privacy by Design as a mandatory requirement for AI systems processing personal data. Organisations should be required to conduct Data Protection Impact Assessments (DPIAs) or AI Impact Assessments before deploying high-risk AI applications. These assessments would help identify potential privacy risks, security vulnerabilities, discriminatory outcomes, and adverse impacts on fundamental rights.

D. Oversight and Accountability Mechanisms

Effective regulation requires strong institutional oversight. India should strengthen its existing regulatory framework by expanding the role of the Data Protection Board or by establishing a specialised authority dedicated to AI governance and oversight. Such a body could monitor compliance, investigate complaints, conduct inspections, and impose penalties where necessary. Entities deploying high-risk AI systems should be subjected to periodic regulatory reviews and compliance audits. The grievance redressal framework under the DPDP Act should

also be expanded to specifically address harms resulting from AI-generated decisions and automated processing. Individuals should have the right to challenge algorithmic decisions, seek explanations regarding automated outcomes, and obtain appropriate remedies where harm occurs. Transparency obligations similar to those found in international frameworks should be incorporated into Indian law, ensuring that individuals are informed whenever AI systems significantly influence decisions affecting their rights or interests. The current absence of comprehensive accountability standards has created a regulatory vacuum that must be addressed through clear statutory obligations applicable to both AI developers and deployers.

E. Cross-Sectoral Coordination and Multi-Disciplinary Governance

AI regulation cannot operate in isolation from other areas of law. Because Artificial Intelligence impacts numerous sectors, including healthcare, finance, employment, consumer protection, competition law, and public administration, regulatory coordination is essential. Data protection laws must interact effectively with sector-specific regulations to ensure comprehensive governance. Independent audits, stakeholder consultations, and public participation mechanisms should form part of the governance process to ensure transparency, legitimacy, and public trust. Such a coordinated approach would facilitate the development of a balanced regulatory environment capable of supporting innovation while protecting individual rights and societal interests.

VIII. Conclusion

Artificial Intelligence presents immense opportunities for India in areas such as governance, healthcare, education, finance, and digital innovation. Its ability to process vast amounts of data, automate complex tasks, and enhance decision-making has the potential to accelerate economic growth and improve public service delivery. However, the rapid expansion of AI technologies also raises significant concerns relating to privacy, data protection, transparency, accountability, and individual autonomy. Without an effective regulatory framework, individuals may lose control over their personal information and become vulnerable to unfair, discriminatory, or opaque algorithmic decisions. The Digital Personal Data Protection Act, 2023, provides an important foundation for protecting personal data in the digital era. Nevertheless, the Act primarily focuses on data protection and does not comprehensively address the unique challenges posed by Artificial Intelligence. Issues such as algorithmic bias, automated decision-making, explainability, profiling, deepfakes, surveillance, and

accountability require specialised legal attention beyond the scope of traditional privacy regulation. To ensure responsible AI development, India must move towards an integrated AI and data protection framework that combines privacy safeguards with AI-specific governance measures. The introduction of risk-based AI regulation, mandatory algorithmic audits, transparency requirements, impact assessments, and stronger accountability mechanisms would help ensure that AI systems operate fairly and responsibly. Equally important is the establishment of effective oversight institutions capable of monitoring compliance and providing meaningful remedies for individuals affected by AI-driven decisions. Global regulatory developments demonstrate that Artificial Intelligence cannot be treated solely as a data protection issue.