JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 3 (Jul.-Sep.) | 2026 Art. 6

Rights of Data Principals in the Era of Artificial Intelligence: Evaluating the Adequacy of the Digital Personal Data Protection Act, 2023

Deeksha Pandey
Research Scholar (Ph.D in Law, Pursuing)
Institute of Legal Studies, Shri Ram Swaroop Memorial University,
Lucknow – Deva Road, Barabanki

Dr. Purnima Bhardwaj
Assistant Professor,
Institute of Legal Studies, Shri Ram Swaroop Memorial University,
Lucknow – Deva Road, Barabanki

Recommended Citation
Deeksha Pandey and Dr. Purnima Bhardwaj, *Rights of Data Principals in the Era of Artificial Intelligence: Evaluating the Adequacy of the Digital Personal Data Protection Act, 2023*, 2 JILPS 94-132 (2026).
Available at www.jilps.in/current-issue/

Rights of Data Principals in the Era of Artificial Intelligence: Evaluating the Adequacy of the Digital Personal Data Protection Act, 2023

ABSTRACT

The growing integration of Artificial Intelligence (AI) into contemporary digital ecosystems has fundamentally transformed the manner in which personal information is collected, processed, and utilized. AI-powered technologies increasingly influence decisions relating to employment, education, healthcare, financial services, and public administration. While these innovations contribute to efficiency and technological advancement, they also create significant concerns regarding privacy, informational autonomy, transparency, and accountability. As AI systems depend heavily on large volumes of data, the protection of individuals' rights over their personal information has become a critical legal and policy concern. India's Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a statutory framework governing the processing of digital personal data and recognizes various rights of data principals. These rights are intended to provide individuals with greater control over their personal information and to promote responsible data governance. However, the emergence of AI-driven technologies raises questions about whether the existing legal framework is capable of addressing challenges such as algorithmic profiling, opaque decision-making processes, and large-scale automated data processing. This paper critically examines the adequacy of the rights available to data principals under the DPDP Act, 2023 in the context of artificial intelligence. The study adopts a doctrinal and analytical approach by examining legislative provisions, judicial developments, policy documents, and selected international regulatory frameworks. The analysis reveals that although the Act provides an important foundation for data protection in India, it does not comprehensively address several AI-specific concerns, including explainability, algorithmic accountability, and safeguards against automated decision-making. The paper argues that strengthening the existing framework through targeted regulatory reforms would enhance the protection of data principals and ensure that data governance mechanisms remain effective in an increasingly AI-driven environment.

KEYWORDS

Artificial Intelligence, Data Principal, DPDP Act 2023, Privacy,

Consent, Automated Decision-Making, Data Protection.

1. INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) has transformed the digital landscape by enabling systems to process vast quantities of data, identify patterns, and make predictions with unprecedented speed and accuracy. [1]AI technologies have become integral to various sectors, including healthcare, education, finance, e-commerce, governance, and law enforcement. The effectiveness of these technologies largely depends upon continuous access to personal data, making data collection and processing central to the functioning of modern AI systems.[2]

As organizations increasingly rely on AI-driven tools, concerns regarding privacy, surveillance, profiling, discrimination, and the misuse of personal information have become more pronounced. AI systems often operate through complex algorithms that make decisions affecting individuals without providing meaningful explanations regarding the basis of such decisions. This lack of transparency may adversely impact fundamental rights, particularly the right to privacy recognized under Article 21 of the Constitution of India. [3]Recognizing the need for a comprehensive legal framework governing personal data, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act). The Act establishes a rights-based approach to data protection by granting data principals several rights, including the right to access information, correction and erasure of personal data, grievance redressal, nomination, and withdrawal of consent.[4]These rights seek to strengthen individual control over personal information and promote accountability among data fiduciaries.

However, the increasing deployment of AI technologies raises important questions regarding the adequacy of these statutory protections. AI systems frequently engage in automated decision-making, algorithmic profiling, and large-scale data analytics, which may not be sufficiently addressed under the current provisions of the DPDP Act. Unlike regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR), the Indian legislation does not expressly recognize rights relating to explanation of automated decisions or protection against solely automated processing.[5]

---

[1] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–10 (4th ed. 2021).

[2] OECD, *OECD Principles on Artificial Intelligence* (2019).

[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

[4] Digital Personal Data Protection Act, No. 22 of 2023, §§ 11–15 (India).

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 22, 2016 O.J. (L 119)

Against this backdrop, the present study evaluates whether the rights available to data principals under the DPDP Act, 2023 are capable of addressing the challenges posed by AI-driven data processing. The study further examines existing regulatory gaps and proposes reforms necessary to ensure effective protection of individual rights in the evolving technological environment.

1.1 Research Problem

The Digital Personal Data Protection Act, 2023 was enacted to provide a legal framework for the protection of personal data and to establish rights for data principals in India. While the Act introduces significant safeguards relating to consent-based processing and individual control over personal information, its provisions primarily address traditional forms of data processing. The emergence of Artificial Intelligence (AI) has fundamentally altered the nature, scale, and complexity of personal data processing through automated decision-making, algorithmic profiling, predictive analytics, and machine learning systems.^1

AI systems often process vast amounts of personal data without meaningful human intervention, creating concerns regarding transparency, accountability, fairness, and informational privacy. Individuals may be subjected to decisions affecting employment opportunities, financial services, healthcare access, and public benefits based on algorithmic assessments that remain opaque and difficult to challenge.^2 The DPDP Act, 2023 does not expressly provide safeguards against solely automated decision-making, nor does it establish a specific right to explanation regarding AI-generated outcomes. Consequently, questions arise as to whether the existing rights of data principals are adequate to protect individuals in AI-driven environments.

The central research problem of this study is to examine the extent to which the rights guaranteed under the DPDP Act, 2023 effectively safeguard data principals against emerging risks associated with Artificial Intelligence and whether additional regulatory measures are required to address existing legal gaps.

1.2 Research Questions

The present study seeks to answer the following questions:

1. What rights are available to data principals under the Digital Personal Data Protection Act, 2023?

2. How do Artificial Intelligence systems process and utilize personal data?[6]

3. What challenges do AI-driven technologies pose to the exercise and protection of data principal rights?

4. Whether the existing provisions of the DPDP Act, 2023 adequately address concerns relating to algorithmic profiling, automated decision-making, and transparency?

5. What lessons can India derive from international regulatory frameworks governing AI and data protection?

6. What legal and policy reforms are necessary to strengthen the protection of data principals in the age of Artificial Intelligence?

1.3 Research Objectives

The study aims to achieve the following objectives:

1. To examine the concept and scope of data principal rights under the Digital Personal Data Protection Act, 2023.

2. To analyze the relationship between Artificial Intelligence and personal data processing.

3. To identify the challenges posed by AI technologies to privacy and data protection.

4. To evaluate the adequacy of the DPDP Act, 2023 in safeguarding data principal rights within AI-driven ecosystems.

5. To undertake a comparative analysis of international legal frameworks relating to AI governance and data protection.

6. To propose recommendations for strengthening the Indian data protection framework in response to emerging AI-related risks.[7]

1.4 Research Methodology

The present study adopts a doctrinal and analytical research methodology. The research is primarily based on the examination of legal sources, including statutes, judicial decisions, government reports, policy documents, and international regulatory instruments.^3 The

[6] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 27–39 (4th ed. 2021).
[7] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–18 (2015).

Digital Personal Data Protection Act, 2023 serves as the principal legislative framework for analysis.

The study further relies upon secondary sources such as books, scholarly articles, research papers, reports published by international organizations, and expert commentaries relating to Artificial Intelligence, privacy, and data protection. A comparative approach has also been employed to examine relevant provisions of the European Union General Data Protection Regulation (GDPR), the European Union Artificial Intelligence Act, and other international standards. Through critical analysis of these sources, the study evaluates existing legal protections and identifies regulatory gaps within the Indian framework.

1.5 Scope and Limitations of the Study

The scope of this study is limited to an examination of the rights of data principals under the Digital Personal Data Protection Act, 2023 in the context of Artificial Intelligence. The research focuses on AI-related issues such as automated decision-making, algorithmic profiling, transparency, accountability, and privacy protection.

The study does not undertake an empirical investigation involving surveys, interviews, or field-based data collection. Further, since AI regulation is an evolving area of law, the analysis is confined to existing legal frameworks, policy developments, and available scholarly literature up to the time of writing. The study primarily examines legal and regulatory dimensions and does not address technical aspects of AI architecture in detail.[8]

2. CONCEPTUAL FRAMEWORK OF ARTIFICIAL INTELLIGENCE AND DATA PROTECTION

2.1 Meaning and Evolution of Artificial Intelligence

Artificial Intelligence (AI) refers to the capability of machines and computer systems to perform tasks that ordinarily require human intelligence, including learning, reasoning, problem-solving, decision-making, language processing, and pattern recognition.[9]AI has evolved from a theoretical concept into a transformative technology that influences nearly every aspect of modern society. Early AI research during the mid-twentieth century focused on developing machines capable of simulating human reasoning. Over time, advances in computational power, data availability, and algorithmic innovation have

[8] Terry Hutchinson & Nigel Duncan, *Defining and Describing What We Do: Doctrinal Legal Research*, 17 Deakin L. Rev. 83, 84–87 (2012).
[9] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1 (4th ed. 2021).

enabled the development of sophisticated AI systems capable of autonomous learning and decision-making.[10]

The emergence of machine learning and deep learning technologies has significantly accelerated the adoption of AI across sectors such as healthcare, finance, education, transportation, governance, and digital commerce. More recently, generative AI models have demonstrated the ability to create text, images, audio, and other forms of content, further expanding the role of AI in everyday life.[11] The growing dependence of these systems on large datasets has intensified concerns regarding the protection of personal data and individual privacy.

2.2 Types of AI Systems

AI systems may be categorized based on their functionality and methods of operation.

2.2.1 Machine Learning

Machine Learning (ML) is a subset of AI that enables systems to learn from data and improve their performance without explicit programming. ML algorithms identify patterns within datasets and generate predictions or recommendations based on those patterns.[12] Common applications include fraud detection, recommendation systems, and predictive analytics.

2.2.2 Deep Learning

Deep Learning is an advanced form of machine learning that utilizes artificial neural networks with multiple layers to process complex data. These systems are capable of recognizing speech, identifying images, translating languages, and performing sophisticated analytical tasks.[13]

2.2.3 Generative Artificial Intelligence

Generative AI refers to systems capable of producing new content, including text, images, videos, and software code. These models are trained on extensive datasets and generate outputs by identifying patterns within the training data.[14] The widespread

[10] Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* 13–25 (2010).
[11] World Economic Forum, *The Presidio Recommendations on Responsible Generative AI* (2023).
[12] Ethem Alpaydin, *Machine Learning* 2–5 (MIT Press, 2021).
[13] Ian Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning* 1–8 (2016).
[14] UNESCO, *Guidance for Generative AI in Education and Research* (2023).

adoption of generative AI has raised significant questions concerning consent, copyright, privacy, and data governance.

2.2.4 Predictive Analytics Systems

Predictive AI systems analyze historical and real-time data to forecast future outcomes or behaviors. Such technologies are commonly used in credit scoring, employment screening, healthcare diagnostics, and targeted advertising.[15]While these applications may enhance efficiency, they also create risks of profiling and discriminatory outcomes.

2.3 AI and Personal Data Processing

Personal data serves as a critical resource for the functioning of AI systems. Machine learning models require extensive datasets to train algorithms, improve accuracy, and generate meaningful outputs. Consequently, AI systems frequently collect, analyze, store, and process large volumes of personal information, including demographic details, online activities, biometric information, location data, and behavioral patterns.[16]

The processing of personal data through AI differs from conventional data processing in several respects. First, AI systems often operate continuously and autonomously, allowing them to process information at an unprecedented scale. Second, advanced algorithms may infer new information about individuals that was not explicitly provided by them. Third, AI systems may combine data from multiple sources, creating comprehensive profiles of individuals and increasing the likelihood of privacy intrusions.[17]

The extensive reliance on personal data has led to growing concerns regarding the legality, fairness, and transparency of AI-driven processing activities. As a result, data protection laws increasingly seek to regulate how personal data is collected, utilized, and retained by organizations employing AI technologies.

2.4 Privacy Concerns in AI Systems

The integration of AI into data-driven decision-making processes has generated several privacy-related challenges.

[15] Cathy O'Neil, *Weapons of Math Destruction* 15–29 (2016).
[16] Digital Personal Data Protection Act, No. 22 of 2023, § 2(t) (India).
[17] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences*, 2019 Colum. Bus. L. Rev. 494, 499–506 (2019).

2.4.1 Mass Data Collection

AI systems require large datasets for training and operation. Organizations often collect extensive personal information from users, sometimes exceeding what is necessary for a specific purpose. Such practices may undermine the principle of data minimization and increase the risk of misuse.[18]

2.4.2 Profiling and Behavioral Tracking

AI technologies enable organizations to monitor individual behavior, preferences, and activities across digital platforms. Through profiling techniques, organizations can predict consumer behavior, political preferences, and purchasing patterns, potentially affecting individual autonomy and freedom of choice.[19]

2.4.3 Automated Decision-Making

Many AI systems make decisions without meaningful human involvement. Automated decisions relating to employment, lending, insurance, and public services may significantly affect individuals while offering limited opportunities for review or challenge.[20]

2.4.4 Algorithmic Bias and Discrimination

AI systems may produce biased outcomes when trained on incomplete, inaccurate, or historically discriminatory datasets. Such biases can result in unfair treatment of individuals based on gender, race, ethnicity, socioeconomic status, or other protected characteristics.[21]

2.4.5 Lack of Transparency

Complex AI models often function as "black boxes," making it difficult for individuals to understand how decisions are reached. This lack of explainability undermines accountability and restricts the ability of affected individuals to exercise their rights effectively.[22]

[18] OECD, *OECD Privacy Guidelines* (2013).
[19] Shoshana Zuboff, *The Age of Surveillance Capitalism* 93–120 (2019).
[20] Regulation (EU) 2016/679 (General Data Protection Regulation), art. 22.
[21] Cathy O'Neil, *Weapons of Math Destruction* 108–130 (2016).
[22] Frank Pasquale, *The Black Box Society* 3–18 (2015).

2.5 AI Governance and Ethical Principles

The rapid development of AI has prompted governments and international organizations to formulate ethical and regulatory principles aimed at ensuring responsible innovation. Common principles include transparency, accountability, fairness, privacy protection, human oversight, and respect for fundamental rights.[23]

The OECD AI Principles emphasize inclusive growth, transparency, robustness, security, and accountability in AI development and deployment.[24] Similarly, the European Union's AI regulatory framework adopts a risk-based approach that seeks to regulate AI systems according to the potential risks they pose to individuals and society.

In India, discussions regarding AI governance have increasingly focused on balancing technological innovation with privacy protection and individual rights. The effectiveness of the DPDP Act, 2023 in addressing AI-related challenges therefore depends on its ability to incorporate these emerging principles of responsible AI governance. Understanding the interaction between AI technologies and data protection rights is essential for evaluating the adequacy of the existing legal framework.

3. Rights of Data Principals under the Digital Personal Data Protection Act, 2023

3.1 Overview of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive legislation specifically governing the processing of digital personal data. The Act seeks to balance the individual's right to protect personal data with the legitimate need of organizations and the State to process such data for lawful purposes.[25] It establishes obligations for data fiduciaries, recognizes rights of data principals, prescribes penalties for non-compliance, and creates the Data Protection Board of India as the primary enforcement authority.

The Act adopts a consent-centric framework, requiring data fiduciaries to obtain free, specific, informed, unconditional, and unambiguous consent before processing personal data, except in certain legitimate uses recognized by the legislation.[26] By conferring statutory rights upon data

[23] UNESCO Recommendation on the Ethics of Artificial Intelligence, UNESCO Gen. Conf., 41st Sess. (2021).
[24] OECD, *OECD Principles on Artificial Intelligence* (2019).
[25] Digital Personal Data Protection Act, No. 22 of 2023, pmbl. (India).
[26] Id. § 6.

principals, the Act aims to enhance transparency, accountability, and individual control over personal information.

However, while the Act provides a general framework for data protection, its applicability to AI-driven environments remains a subject of debate due to the increasing use of automated systems, predictive analytics, and algorithmic decision-making.

3.2 Concept of Data Principal

The DPDP Act defines a data principal as the individual to whom the personal data relates. In the case of a child or a person with a disability, the parent, lawful guardian, or legal representative may exercise rights on behalf of the concerned individual.

The concept of a data principal lies at the heart of the Act's rights-based framework. The legislation recognizes that individuals should retain control over the collection, use, storage, and disclosure of their personal information. Accordingly, various rights have been provided to ensure meaningful participation in decisions affecting personal data.

3.3 Right to Access Information about Personal Data

One of the most significant rights granted under the DPDP Act is the right to obtain information regarding the processing of personal data. Upon request, a data principal may seek details concerning:

- The personal data being processed.
- Processing activities undertaken by the data fiduciary.
- Identities of data fiduciaries and data processors with whom data has been shared.
- Any other information prescribed by law.

This right promotes transparency and enables individuals to understand how their information is being utilized. In AI-driven systems, access to information becomes particularly important because personal data is often processed through complex algorithms that operate beyond the direct knowledge of users.

Nevertheless, the Act does not explicitly require disclosure of algorithmic logic or AI decision-making mechanisms, which may limit the practical effectiveness of this right in certain contexts.

3.4 Right to Correction, Completion, Updating and Erasure

The DPDP Act grants data principals the right to request correction, completion, updating, and erasure of their personal data.

This right serves several objectives:

- Ensuring accuracy of personal information.
- Preventing adverse decisions based on incorrect data.
- Maintaining data quality.
- Enhancing individual control over personal information.

The right assumes particular significance in AI systems where inaccurate data may lead to erroneous predictions, profiling, or automated decisions. However, practical challenges arise where AI systems derive inferred data or predictive conclusions that are not directly supplied by individuals but generated through algorithmic processing.

3.5 Right to Grievance Redressal

The Act provides data principals with the right to seek redress against grievances arising from violations of their rights or obligations imposed upon data fiduciaries.

A data principal may:

1. Submit a complaint to the concerned data fiduciary.
2. Approach the Data Protection Board of India if dissatisfied with the response.

This mechanism seeks to ensure accountability and provide remedies against unlawful processing practices. However, AI-related disputes involving algorithmic bias, automated decision-making, or opaque processing systems may require specialized expertise beyond traditional grievance mechanisms.

3.6 Right to Nominate

The DPDP Act introduces a novel right enabling a data principal to nominate another individual who may exercise rights on their behalf in the event of death or incapacity.

This provision reflects the growing importance of digital identities and digital assets. It also ensures continuity in the management and

protection of personal data where the data principal is unable to exercise rights independently.

3.7 Right to Withdraw Consent

The right to withdraw consent constitutes a fundamental component of informational self-determination under the DPDP Act.

A data principal may withdraw previously granted consent at any time, and the process for withdrawal must be as simple as the process through which consent was originally provided.

This right reinforces individual autonomy by ensuring that data processing remains subject to ongoing control by the individual concerned. However, AI systems often rely on historical datasets that may have already been incorporated into machine learning models. Consequently, the practical implementation of consent withdrawal presents significant challenges in AI environments where data has already contributed to algorithmic training.

3.8 Duties of Data Principals

Unlike many international data protection frameworks, the DPDP Act also imposes certain duties upon data principals. These include:

- Compliance with applicable laws.
- Avoidance of false or frivolous complaints.
- Provision of authentic information while exercising rights.

The inclusion of duties reflects the legislative intention to balance individual rights with responsible participation in the digital ecosystem.

3.9 Critical Evaluation of Data Principal Rights in the Context of Artificial Intelligence

The rights recognized under the DPDP Act provide an important foundation for data protection and individual autonomy. They promote transparency, accountability, and user control over personal information. Nevertheless, the effectiveness of these rights becomes uncertain when applied to AI-driven processing activities.

Several limitations become evident:

- Absence of a specific right against solely automated decision-making.

- No statutory right to explanation of algorithmic decisions.
- Limited safeguards against profiling.
- Lack of transparency obligations regarding AI systems.
- No mandatory algorithmic impact assessments.

Consequently, while the DPDP Act strengthens the protection of personal data, it may not adequately address emerging risks associated with AI technologies. These shortcomings become more apparent when compared with international frameworks such as the GDPR, which expressly provides safeguards relating to automated decision-making and profiling.[27]

The next chapter therefore examines the specific challenges posed by Artificial Intelligence to data principal rights and evaluates whether the existing legal framework is capable of responding to these emerging concerns.

4. Challenges to Data Principal Rights in AI-Driven Ecosystems

4.1 Introduction

Artificial Intelligence has transformed the manner in which personal data is collected, processed, analyzed, and utilized. Unlike traditional data processing systems, AI technologies continuously learn from large datasets and often operate with minimal human intervention. While such systems enhance efficiency and innovation, they also create significant challenges for the protection of data principal rights. The increasing use of algorithmic decision-making, predictive analytics, and machine learning has exposed limitations within existing legal frameworks, particularly concerning transparency, accountability, and individual autonomy.[28]

The rights granted under the Digital Personal Data Protection Act, 2023 are intended to empower individuals and ensure responsible data governance. However, the unique characteristics of AI systems often make it difficult for data principals to effectively exercise these rights. This chapter examines the major challenges posed by AI-driven ecosystems and their implications for data protection.

[27] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 15, 21 & 22, 2016 O.J. (L 119) 1.
[28] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–18 (Harvard Univ. Press 2015).

4.2 Automated Decision-Making and Loss of Human Oversight

One of the defining characteristics of AI systems is their ability to make decisions without direct human involvement. Automated decision-making refers to decisions generated through algorithms based on predefined rules, statistical models, or machine learning techniques.[29]

Such systems are increasingly used in:

- Recruitment and hiring processes.
- Credit scoring and loan approvals.
- Insurance underwriting.
- Healthcare diagnostics.
- Public welfare distribution.

While automated systems may improve efficiency and consistency, they can significantly affect individual rights. Data principals may be denied employment opportunities, financial services, or public benefits based solely on algorithmic assessments. The absence of meaningful human review creates concerns regarding fairness and accountability.

Unlike the GDPR, which provides safeguards against decisions based solely on automated processing, the DPDP Act, 2023 does not expressly recognize such protections. [30]Consequently, affected individuals may face difficulties challenging adverse decisions generated by AI systems.

4.3 Algorithmic Profiling and Behavioral Prediction

AI systems frequently engage in profiling, which involves analyzing personal data to evaluate or predict aspects of an individual's behavior, preferences, interests, economic status, health, or reliability.[31]

Modern organizations employ profiling techniques for:

- Personalized advertising.
- Consumer behavior analysis.

[29] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L. 76, 77–81 (2017).
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.
[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 4(4), 2016 O.J. (L 119) 1.

- Creditworthiness assessment.
- Political campaigning.
- Risk evaluation.

While profiling may improve service delivery, it also raises concerns regarding privacy and autonomy. Individuals are often unaware of how profiles are created or utilized. Furthermore, extensive profiling can result in digital surveillance and manipulation of individual choices.

The DPDP Act grants rights relating to access and correction of personal data but does not specifically regulate profiling activities or provide safeguards against excessive behavioral monitoring.

4.4 Challenges of Informed Consent in AI Systems

Consent forms the foundation of the DPDP Act's regulatory framework.[32] However, obtaining meaningful consent becomes increasingly difficult in AI-driven environments.

Several factors contribute to this challenge:

4.4.1 Complexity of AI Systems

AI models often involve highly technical processes that are difficult for ordinary individuals to understand. As a result, users may provide consent without fully appreciating how their data will be processed.

4.4.2 Future and Secondary Uses of Data

AI systems frequently use data for purposes that were not foreseeable at the time of collection. Data initially collected for one purpose may later be utilized for algorithm training, research, or predictive analytics.

4.4.3 Consent Fatigue

Individuals are routinely presented with lengthy privacy notices and consent requests. Repeated exposure often results in users accepting terms without meaningful review, thereby undermining genuine informed consent.[33]

[32] Digital Personal Data Protection Act, No. 22 of 2023, § 6 (India).
[33] Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1882–88 (2013).

These challenges weaken the effectiveness of consent as a mechanism for protecting data principal rights.

4.5 Data Scraping and AI Training Models

The development of advanced AI systems often requires access to massive datasets obtained from websites, social media platforms, online repositories, and publicly accessible sources.^7

Many AI developers engage in large-scale data scraping to collect information used for training machine learning models. Such practices raise important legal and ethical questions:

- Whether publicly available information can be freely used for AI training.
- Whether individuals have consented to such processing.
- Whether personal data embedded in training datasets can later be removed.

The DPDP Act does not specifically regulate the use of scraped data for AI training purposes. Consequently, uncertainty remains regarding the rights of data principals whose information forms part of AI training datasets.

4.6 Algorithmic Bias and Discrimination

AI systems are often perceived as objective and neutral. However, research demonstrates that algorithms can replicate and amplify existing social biases when trained on inaccurate or historically discriminatory datasets.[34]

Examples include:

- Gender bias in recruitment systems.
- Racial or ethnic bias in facial recognition technologies.
- Discriminatory credit scoring mechanisms.
- Unequal access to public services.

Such outcomes may adversely affect fundamental principles of equality and fairness. Data principals subjected to biased decisions may

[34] UNESCO, Guidance for Generative AI in Education and Research (2023).

experience significant harm without understanding the source of discrimination.

The DPDP Act does not contain explicit provisions addressing algorithmic fairness or bias mitigation, creating a significant regulatory gap.

4.7 Explainability and Transparency Challenges

Transparency is essential for ensuring accountability in data processing activities. However, many AI systems operate as "black box" models whose internal decision-making processes are difficult to understand even for their developers.[35]

Lack of explainability creates several concerns:

- Individuals cannot understand why a decision was made.
- Errors become difficult to identify and correct.
- Accountability mechanisms become ineffective.
- Regulatory oversight becomes more challenging.

The DPDP Act provides a right to access information regarding data processing but does not establish a specific right to explanation of AI-generated decisions. Consequently, data principals may remain unaware of the factors influencing decisions that affect their rights and interests.

4.8 Re-identification Risks and Data Security Concerns

Organizations frequently rely upon anonymization and pseudonymization techniques to protect privacy while utilizing data for AI development. However, advancements in AI have increased the possibility of re-identifying individuals from datasets that were previously considered anonymous.[36]

AI systems can combine information from multiple sources and infer identities through sophisticated analytical techniques. Such capabilities create risks including:

- Unauthorized disclosure of personal information.
- Identity theft.

[35] Cathy O'Neil, *Weapons of Math Destruction* 108–130 (Crown Publ'g Group 2016).
[36] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–18 (Harvard Univ. Press 2015).

- Data breaches.
- Loss of privacy.

Although the DPDP Act imposes obligations relating to data security and breach notification, evolving AI capabilities present new challenges that may require stronger safeguards and technical standards.

4.9 Critical Analysis

The foregoing discussion demonstrates that AI technologies challenge several assumptions underlying traditional data protection frameworks. While the DPDP Act, 2023 provides important protections through consent requirements and data principal rights, it does not comprehensively address issues such as automated decision-making, profiling, explainability, algorithmic bias, and AI training datasets.

The absence of AI-specific safeguards may limit the practical effectiveness of rights granted to data principals. Consequently, there is a growing need to evaluate whether existing legal protections remain adequate in increasingly automated digital environments. These concerns become more evident when India's framework is compared with international regulatory models that explicitly address AI-related risks.

5. Evaluating the Adequacy of the Digital Personal Data Protection Act, 2023 in the Age of Artificial Intelligence

5.1 Introduction

The Digital Personal Data Protection Act, 2023 represents a significant milestone in India's data protection landscape. By establishing a rights-based framework for personal data governance, the Act seeks to balance innovation, economic development, and individual privacy interests. However, the rapid evolution of Artificial Intelligence (AI) has introduced novel challenges that extend beyond conventional data processing activities. AI systems rely heavily on large-scale data collection, automated decision-making, profiling, and predictive analytics, raising concerns regarding transparency, accountability, fairness, and individual autonomy.[37]

This chapter critically evaluates whether the rights granted to data principals under the DPDP Act, 2023 are sufficient to address these emerging challenges. It identifies the strengths of the existing framework, examines its limitations in the context of AI, and highlights

[37] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–18 (Harvard Univ. Press 2015).

regulatory gaps that may undermine the effective protection of data principal rights.

5.2 Strengths of the DPDP Act, 2023

5.2.1 Recognition of Data Principal Rights

One of the major strengths of the DPDP Act is its explicit recognition of rights available to data principals.[38]These rights promote transparency and enable individuals to exercise greater control over their personal information. The rights relating to access, correction, erasure, grievance redressal, and withdrawal of consent provide an important foundation for protecting privacy in digital environments.

5.2.2 Consent-Centric Framework

The Act adopts consent as the primary legal basis for personal data processing.[39] By requiring consent to be free, informed, specific, unconditional, and unambiguous, the legislation seeks to ensure that individuals participate meaningfully in decisions affecting their personal information.

5.2.3 Accountability of Data Fiduciaries

The Act imposes obligations upon data fiduciaries to process data responsibly, implement security safeguards, and prevent unauthorized disclosures.[40]These obligations contribute to greater organizational accountability and strengthen trust in digital ecosystems.

5.2.4 Establishment of the Data Protection Board

The creation of the Data Protection Board of India provides an institutional mechanism for grievance redressal, compliance monitoring, and enforcement.^5 This framework enhances the practical enforceability of rights granted under the Act.

5.3 Regulatory Gaps in the Context of Artificial Intelligence

Despite these strengths, several limitations become apparent when the Act is examined through the lens of AI-driven data processing.

[38] Digital Personal Data Protection Act, No. 22 of 2023, §§ 11–15 (India).
[39] Digital Personal Data Protection Act, No. 22 of 2023, § 6 (India).
[40] Digital Personal Data Protection Act, No. 22 of 2023, §§ 8–10 (India).

5.3.1 Absence of a Right Against Automated Decision-Making

AI systems increasingly make decisions that significantly affect individuals, including decisions relating to employment, lending, insurance, healthcare, and access to public services.[41]

Unlike the GDPR, which grants individuals protection against decisions based solely on automated processing, the DPDP Act contains no equivalent provision.[42]As a result, data principals may be subjected to consequential algorithmic decisions without meaningful human review.

The absence of such protection represents one of the most significant shortcomings of the Indian framework.

5.3.2 Lack of a Right to Explanation

Transparency is essential for meaningful exercise of data protection rights. Individuals must be able to understand why a decision affecting them was made.

However, the DPDP Act does not recognize a specific right to explanation concerning AI-generated outcomes.[43]Although data principals may seek information regarding processing activities, they cannot compel disclosure of algorithmic logic or decision-making criteria.

This limitation weakens accountability and restricts the ability of individuals to challenge unfair or inaccurate decisions.

5.3.3 Inadequate Regulation of Profiling Activities

Profiling enables organizations to analyze personal data and predict behavior, preferences, or future actions.[44]

AI-driven profiling is extensively used in:

- Digital advertising.

[41] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L. 76, 77–81 (2017).
[42] Digital Personal Data Protection Act, No. 22 of 2023, §§ 18–28 (India).
[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.
[44] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 186–205 (Harvard Univ. Press 2015).

- Consumer analytics.
- Credit assessment.
- Political campaigning.
- Risk prediction systems.

Despite the potential impact of profiling on privacy and autonomy, the DPDP Act contains no dedicated provisions governing profiling practices. Consequently, data principals may remain vulnerable to intrusive monitoring and behavioral manipulation.

5.3.4 Absence of Algorithmic Accountability Mechanisms

Modern AI systems often operate through complex algorithms whose functioning is difficult to evaluate or audit. Effective governance requires mechanisms ensuring that organizations remain accountable for algorithmic outcomes.

The DPDP Act does not mandate:

- Algorithmic audits.
- Fairness assessments.
- Bias testing.
- Independent verification procedures.

The absence of these safeguards limits the ability of regulators to detect discriminatory or harmful AI practices.

5.3.5 Lack of AI Impact Assessments

Many jurisdictions increasingly require organizations to conduct impact assessments before deploying high-risk AI systems.[45]

Such assessments typically evaluate:

- Privacy risks.
- Discrimination risks.
- Security vulnerabilities.

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 4(4), 2016 O.J. (L 119) 1.

- Potential harm to individuals.

The DPDP Act does not impose a mandatory requirement for AI-specific impact assessments. Consequently, organizations may deploy high-risk systems without systematically evaluating their impact on data principal rights.

5.4 Gap Analysis

AI-Related Issue	Position under DPDP Act, 2023	Regulatory Gap
Automated Decision-Making	No specific provision	Significant
Right to Explanation	Not expressly recognized	Significant
Algorithmic Profiling	Limited regulation	Significant
AI Transparency	General transparency obligations only	Moderate to Significant
Algorithmic Accountability	No explicit requirement	Significant
Bias and Discrimination	Not specifically addressed	Significant
AI Impact Assessments	No mandatory requirement	Significant
Human Oversight	Not mandated	Significant

The above analysis demonstrates that while the DPDP Act establishes a general framework for data protection, it does not sufficiently address many challenges unique to AI-driven processing activities.

5.5 Comparative Perspective

International regulatory frameworks provide useful insights into addressing AI-related risks.

The GDPR recognizes safeguards against solely automated decision-making and profiling through Article 22.[46]Individuals are entitled to

[46] OECD, OECD Framework for the Classification of AI Systems (2022).

obtain human intervention and challenge decisions that significantly affect them.

Similarly, the European Union AI Act adopts a risk-based regulatory model that imposes enhanced obligations on high-risk AI systems, including transparency requirements, human oversight mechanisms, and conformity assessments.[47]

Compared to these frameworks, the DPDP Act adopts a broader and technology-neutral approach. While this approach offers flexibility, it may be inadequate in addressing the unique challenges presented by rapidly evolving AI technologies.

5.6 Key Findings of the Study

The analysis undertaken in this research reveals several important findings:

1. The DPDP Act establishes a robust foundation for personal data protection through a rights-based framework.

2. Existing rights are primarily designed for conventional forms of data processing rather than AI-driven environments.

3. Significant regulatory gaps exist regarding automated decision-making, profiling, explainability, and algorithmic accountability.

4. The consent-centric model may not adequately protect individuals where AI systems engage in complex and opaque processing activities.

5. International frameworks provide stronger safeguards for individuals affected by AI-driven decisions.

6. Additional regulatory measures are necessary to ensure meaningful protection of data principal rights in the era of Artificial Intelligence.

5.7 Conclusion

The DPDP Act, 2023 marks a significant advancement in India's data protection regime and establishes important rights for data principals. Nevertheless, the growing use of AI technologies exposes limitations within the current framework. The absence of safeguards relating to automated decision-making, explainability, profiling, and algorithmic

[47] European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, arts. 8–27 (2024).

accountability raises concerns regarding the effectiveness of existing protections.

Although the Act provides a valuable foundation for data governance, its long-term effectiveness will depend upon its ability to adapt to emerging technological realities. Addressing AI-specific risks through targeted legal reforms will be essential to ensure that data principal rights remain meaningful and enforceable in increasingly automated digital ecosystems.

6. COMPARATIVE ANALYSIS OF INTERNATIONAL FRAMEWORKS

6.1 Introduction

The increasing integration of Artificial Intelligence into governance, commerce, healthcare, finance, and other sectors has compelled jurisdictions across the world to develop legal frameworks addressing the challenges posed by AI-driven data processing. Since AI systems rely extensively on personal data, modern regulatory approaches increasingly combine data protection principles with AI-specific governance mechanisms. Comparative analysis of international frameworks provides valuable insights into the strengths and limitations of India's Digital Personal Data Protection Act, 2023 and helps identify best practices that may be adopted to enhance the protection of data principal rights.

This chapter examines key international regulatory models, including the European Union General Data Protection Regulation (GDPR), the European Union Artificial Intelligence Act (EU AI Act), the United Kingdom's AI Governance Framework, and the OECD AI Principles. The objective is to assess how these frameworks address concerns relating to automated decision-making, profiling, transparency, accountability, and individual rights.

6.2 European Union General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is widely regarded as the most comprehensive data protection framework in the world.[48] It establishes extensive rights for data subjects and imposes significant obligations upon organizations processing personal data.

[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

6.2.1 Rights of Data Subjects under GDPR

The GDPR grants individuals several rights, including:

- Right to access personal data.
- Right to rectification.
- Right to erasure ("Right to be Forgotten").
- Right to data portability.
- Right to object to processing.
- Right to restriction of processing.[49]

These rights provide stronger protections than those currently available under the DPDP Act, particularly in relation to AI-driven processing activities.

6.2.2 Protection Against Automated Decision-Making

Article 22 of the GDPR provides that individuals have the right not to be subject to decisions based solely on automated processing when such decisions produce legal or similarly significant effects.[50]

The GDPR further requires:

- Human intervention.
- Opportunity to contest decisions.
- Meaningful explanation regarding outcomes.

This safeguard directly addresses concerns associated with algorithmic decision-making and represents a major protection absent from the DPDP Act, 2023.

6.2.3 Profiling and Transparency

The GDPR expressly regulates profiling activities and requires organizations to inform individuals when profiling is undertaken.

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), arts. 15–21, 2016 O.J. (L 119) 1.
[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.

Data subjects may object to profiling in certain circumstances and seek redress against unfair outcomes.

6.2.4 Relevance for India

The GDPR demonstrates how data protection legislation can incorporate specific safeguards addressing AI-related risks. Provisions concerning automated decision-making, profiling, and transparency offer valuable lessons for strengthening India's legal framework.

6.3 European Union Artificial Intelligence Act

Recognizing that traditional data protection laws alone may not adequately regulate AI technologies, the European Union adopted the Artificial Intelligence Act (EU AI Act) in 2024.

The EU AI Act is the world's first comprehensive AI-specific legislation and adopts a risk-based regulatory approach.

6.3.1 Risk-Based Classification

The Act categorizes AI systems into four levels:

1. Unacceptable Risk AI.
2. High-Risk AI.
3. Limited-Risk AI.
4. Minimal-Risk AI.

Systems posing greater risks are subject to stricter regulatory obligations.

6.3.2 High-Risk AI Systems

High-risk AI systems include technologies used in:

- Employment decisions.
- Education.
- Law enforcement.
- Healthcare.
- Critical infrastructure.

Organizations deploying such systems must comply with requirements relating to:

- Risk management.
- Data governance.
- Human oversight.
- Technical documentation.
- Transparency obligations.

6.3.3 Human Oversight Requirements

The EU AI Act mandates human supervision of high-risk AI systems to prevent harmful or discriminatory outcomes. Such safeguards help ensure that automated systems remain subject to meaningful human control.

6.3.4 Lessons for India

India currently lacks AI-specific legislation comparable to the EU AI Act. The adoption of a risk-based framework could help address challenges associated with high-risk AI applications while preserving opportunities for innovation.

6.4 United Kingdom AI Governance Framework

The United Kingdom has adopted a principles-based and sector-specific approach to AI regulation rather than enacting a comprehensive AI statute.[51]

The UK framework is based upon five core principles:

- Safety, security, and robustness.
- Transparency and explainability.
- Fairness.
- Accountability and governance.
- Contestability and redress.

[51] European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, 2024 O.J. (L) 1.

These principles are implemented through existing sectoral regulators, including authorities responsible for financial services, healthcare, competition, and data protection.

6.4.1 Explainability and Accountability

Particular emphasis is placed upon transparency and explainability. Organizations are encouraged to provide meaningful explanations regarding AI-assisted decisions affecting individuals.[52]

6.4.2 Regulatory Flexibility

The UK's approach seeks to balance innovation with regulatory oversight by allowing regulators to adapt governance measures according to sector-specific needs.

6.4.3 Relevance for India

The UK model demonstrates that effective AI governance may be achieved through flexible regulatory mechanisms while still safeguarding individual rights. Such an approach may be particularly relevant for India's rapidly expanding digital economy.

6.5 OECD AI Principles

The Organisation for Economic Co-operation and Development (OECD) adopted the OECD AI Principles in 2019, establishing globally recognized standards for responsible AI development.[53]

The principles emphasize:

- Inclusive growth and sustainable development.
- Human-centered values.
- Transparency and explainability.
- Robustness and security.
- Accountability.

[52] Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation* (U.K. Gov't, 2023).
[53] Id.

Although not legally binding, these principles have significantly influenced national AI governance frameworks worldwide.

6.5.1 Human-Centered AI

The OECD framework stresses that AI systems should respect human rights, democratic values, and the rule of law.

6.5.2 Transparency and Accountability

Organizations should provide sufficient information regarding AI systems to ensure that individuals understand how decisions affecting them are made.

6.5.3 Significance for India

The OECD principles provide a normative foundation for future AI regulation in India and reinforce the importance of protecting individual rights in AI-driven environments.

6.6 Conclusion

The comparative analysis demonstrates that international frameworks increasingly recognize the unique challenges posed by Artificial Intelligence and have responded by introducing targeted safeguards relating to automated decision-making, profiling, transparency, explainability, and accountability. The GDPR provides strong protections against solely automated decisions, while the EU AI Act establishes a comprehensive risk-based regulatory framework for AI systems. The United Kingdom and OECD frameworks similarly emphasize transparency, fairness, and human oversight.

In contrast, India's DPDP Act, 2023 remains primarily focused on conventional data protection principles and does not comprehensively address AI-specific concerns. While the Act provides an important foundation for safeguarding personal data, significant regulatory gaps remain. Lessons derived from international frameworks can assist policymakers in developing reforms that strengthen the protection of data principal rights and ensure responsible AI governance in India.

7. RECOMMENDATIONS AND CONCLUSION

7.1 Introduction

The preceding chapters have demonstrated that while the Digital Personal Data Protection Act, 2023 establishes a significant legal framework for protecting personal data in India, it does not comprehensively address several challenges arising from the increasing

deployment of Artificial Intelligence (AI). The rapid growth of AI technologies has transformed the nature of data processing, creating risks associated with automated decision-making, algorithmic profiling, opacity, bias, and large-scale data analytics. These developments necessitate a re-evaluation of existing legal safeguards to ensure that data principal rights remain effective in an AI-driven environment.

This chapter proposes legislative, regulatory, and institutional reforms aimed at strengthening the protection of data principals while fostering responsible AI innovation.

7.2 Legislative Recommendations

7.2.1 Introduction of a Right Against Automated Decision-Making

The DPDP Act should be amended to provide data principals with protection against decisions based solely on automated processing that significantly affect their rights and interests.[54]

Such a provision should ensure:

- Human review of significant automated decisions.
- Opportunity to contest decisions.
- Access to effective remedies.

Incorporating such safeguards would align India's framework with internationally recognized standards, particularly those reflected in the GDPR.

7.2.2 Recognition of a Right to Explanation

The law should expressly recognize a right to explanation in cases where AI systems generate decisions affecting individuals.[55]

Data principals should be entitled to:

- Understand the basis of decisions.

[54] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation), art. 22, 2016 O.J. (L 119) 1.
[55] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L. 76, 77–81 (2017).

- Receive meaningful information regarding factors influencing outcomes.
- Challenge inaccurate or discriminatory decisions.

This measure would enhance transparency and accountability in AI-driven processing activities.

7.2.3 Regulation of Profiling Activities

Specific statutory provisions should govern algorithmic profiling and behavioral prediction systems.

Organizations should be required to:

- Disclose profiling practices.
- Inform individuals of the consequences of profiling.
- Provide opt-out mechanisms where appropriate.

Such safeguards would strengthen informational autonomy and reduce risks associated with excessive surveillance.

7.2.4 Mandatory AI Impact Assessments

The DPDP Act should require organizations deploying high-risk AI systems to conduct AI Impact Assessments before implementation.[56]

These assessments should evaluate:

- Privacy implications.
- Discrimination risks.
- Security vulnerabilities.
- Potential societal impacts.

Mandatory assessments would encourage proactive risk management and responsible AI deployment.

[56] OECD, OECD Framework for the Classification of AI Systems (2022).

7.3 Regulatory Recommendations

7.3.1 Development of AI-Specific Guidelines

The Government of India, in collaboration with regulatory authorities, should formulate AI-specific guidelines clarifying obligations relating to:

- Transparency.
- Accountability.
- Data governance.
- Human oversight.

Such guidance would assist organizations in complying with legal requirements while promoting innovation.

7.3.2 Establishment of Algorithmic Audit Requirements

Organizations utilizing high-risk AI systems should be required to conduct periodic independent audits.[57]

These audits should assess:

- Accuracy.
- Fairness.
- Bias mitigation.
- Compliance with data protection obligations.

Regular auditing would strengthen public confidence in AI systems and improve accountability.

7.3.3 Enhanced Transparency Standards

Organizations should provide clear information regarding:

- Data sources used by AI systems.
- Purpose of processing.
- Categories of automated decisions.

[57] European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, arts. 8–27 (2024).

- Potential consequences for individuals.

Transparency obligations would facilitate informed decision-making and strengthen the exercise of data principal rights.

7.4 Institutional Recommendations

7.4.1 Strengthening the Data Protection Board of India

The Data Protection Board should be equipped with specialized expertise relating to Artificial Intelligence and emerging technologies.[58]

Capacity-building initiatives should include:

- Technical experts.
- Data scientists.
- AI governance specialists.

Enhanced institutional expertise would improve the Board's ability to address complex AI-related disputes.

7.4.2 Creation of a Dedicated AI Regulatory Authority

India may consider establishing a specialized AI regulatory authority responsible for:

- Monitoring AI deployment.
- Developing technical standards.
- Conducting compliance assessments.
- Coordinating with sectoral regulators.

Such an institution could provide focused oversight while complementing the role of the Data Protection Board.

7.4.3 Promotion of Interdisciplinary Governance

AI governance requires collaboration among legal experts, technologists, policymakers, ethicists, and industry stakeholders.

[58] Digital Personal Data Protection Act, No. 22 of 2023, §§ 18–28 (India).

Interdisciplinary engagement would facilitate the development of balanced regulatory solutions that protect rights without impeding technological progress.

7.5 Policy Recommendations

7.5.1 Adoption of a Risk-Based Regulatory Framework

India should consider adopting a risk-based approach similar to the European Union AI Act.[59]

AI systems may be categorized according to the level of risk they pose, with stricter obligations imposed upon high-risk applications.

7.5.2 Promotion of Ethical AI Principles

National AI policies should incorporate principles relating to:

- Fairness.
- Transparency.
- Accountability.
- Privacy.
- Human-centered innovation.

Embedding ethical considerations within governance frameworks would contribute to responsible technological development.

7.5.3 Public Awareness and Digital Literacy

Effective protection of data principal rights requires informed and empowered citizens.

Government agencies, educational institutions, and civil society organizations should promote awareness regarding:

- Privacy rights.
- AI technologies.
- Data protection obligations.

[59] European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, arts. 5–7 (2024).

- Available grievance mechanisms.

Improved digital literacy would enable individuals to exercise their rights more effectively.

7.6 Future Research Directions

Artificial Intelligence is a rapidly evolving field, and numerous issues remain underexplored within the Indian legal context. Future research may focus on:

- Regulation of generative AI systems.
- AI and biometric data protection.
- AI governance in healthcare and education.
- Cross-border data transfers and AI.
- Ethical implications of autonomous systems.
- Interaction between AI regulation and competition law.

Further scholarly inquiry will contribute to the development of robust and adaptive regulatory frameworks.

7.7 Conclusion

Artificial Intelligence has fundamentally transformed contemporary data processing practices, creating unprecedented opportunities for innovation while simultaneously generating significant risks for privacy, autonomy, and individual rights. The Digital Personal Data Protection Act, 2023 represents a major advancement in India's data protection regime by establishing statutory rights for data principals and imposing obligations upon data fiduciaries.

However, the findings of this study indicate that the existing framework was primarily designed for conventional forms of data processing and does not adequately address several challenges associated with AI-driven ecosystems. Significant regulatory gaps exist in relation to automated decision-making, algorithmic profiling, explainability, transparency, and accountability. The absence of AI-specific safeguards may limit the practical effectiveness of rights granted under the Act and expose individuals to new forms of harm.

Comparative analysis of international frameworks demonstrates that jurisdictions such as the European Union and the United Kingdom have increasingly adopted targeted measures to address AI-related risks.

These developments offer valuable lessons for India as it seeks to balance technological innovation with the protection of fundamental rights.

The study concludes that while the DPDP Act, 2023 provides a strong foundation for data protection, meaningful protection of data principal rights in the era of Artificial Intelligence requires further legislative refinement, regulatory innovation, and institutional strengthening. The adoption of AI-specific safeguards, enhanced transparency obligations, and robust accountability mechanisms would ensure that India's data protection framework remains responsive to emerging technological realities and capable of safeguarding individual rights in an increasingly data-driven society.

REFERENCES

A. Statutes and Legislative Instruments

1. Digital Personal Data Protection Act, No. 22 of 2023 (India).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.
3. European Union Artificial Intelligence Act, Regulation (EU) 2024/1689, 2024 O.J. (L) 1.

B. Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

C. Books

1. Alpaydin, Ethem. *Machine Learning*. MIT Press, 2021.
2. Goodfellow, Ian, Yoshua Bengio & Aaron Courville. *Deep Learning*. MIT Press, 2016.
3. Nilsson, Nils J. *The Quest for Artificial Intelligence: A History of Ideas and Achievements*. Cambridge University Press, 2010.
4. O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group, 2016.

5. Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015.

6. Russell, Stuart & Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed., Pearson, 2021.

7. Solove, Daniel J. *Understanding Privacy*. Harvard University Press, 2008.

8. Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.

D. Journal Articles

1. Hutchinson, Terry & Nigel Duncan, Defining and Describing What We Do: Doctrinal Legal Research, 17 Deakin L. Rev. 83 (2012).

2. Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010).

3. Solove, Daniel J., Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

4. Wachter, Sandra, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L. 76 (2017).

5. Wachter, Sandra & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, 2019 Colum. Bus. L. Rev. 494 (2019).

E. International Reports, Guidelines and Policy Documents

1. Department for Science, Innovation and Technology (United Kingdom), *A Pro-Innovation Approach to AI Regulation* (2023).

2. Information Commissioner's Office (ICO), *Explaining Decisions Made with AI* (2023).

3. Organisation for Economic Co-operation and Development (OECD), *OECD Privacy Guidelines* (2013).

4. Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (2019).

5. Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2019).

6. Organisation for Economic Co-operation and Development (OECD), *OECD Framework for the Classification of AI Systems* (2022).

7. UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

8. UNESCO, *Guidance for Generative AI in Education and Research* (2023).

9. World Economic Forum, *The Presidio Recommendations on Responsible Generative AI* (2023).

F. Additional Authorities

1. European Data Protection Board (EDPB), *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* (2018).

2. NITI Aayog, *Responsible AI for All: Approach Document for India* (2021).

3. Ministry of Electronics and Information Technology (MeitY), Government of India, *Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna* (2018).

4. United Nations Educational, Scientific and Cultural Organization (UNESCO), *Ethics of Artificial Intelligence Recommendation* (2021).

5. Alan F. Westin, *Privacy and Freedom* (Atheneum, 1967).

6. Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019).

7. Luciano Floridi et al., AI4People—An Ethical Framework for a Good AI Society, 28 Minds & Machines 689 (2018).