



Shodhpith International Multidisciplinary Research Journal

(International Open Access, Peer-reviewed & Refereed Journal)
(Multidisciplinary, Bimonthly, Multilanguage)

Volume: 2

Issue: 4

July-August 2026

Artificial Intelligence and Data Protection in India: A Cyber Law Perspective

Dr. Kamal Kishor

(LL.M. Ph.D , NET, Assistant Professor, Classic College of Law Bareilly, (Affiliated M.J.P
Rohilkhand University, Bareilly)

Article Info: (Received- 16/04/2026, Accepted- 14/5/2026, Published- 05/07/2026)

DOI- [10.64127/Shodhpith.2026v2i4003](https://doi.org/10.64127/Shodhpith.2026v2i4003)

Abstract-

This study analyses the interplay between artificial intelligence deployment and data protection within India's cyber legal framework, identifying gaps, tensions, and opportunities for governance. The research problem centres on how existing statutes, regulatory guidelines, and jurisprudence address AI-enabled data processing, privacy rights, and accountability in a rapidly digitizing economy. A mixed-method approach combines doctrinal analysis of statutes such as the Information Technology Act, the Personal Data Protection Bill proposals, and sectorial regulations with empirical examination of case law, regulatory guidance, and stakeholder interviews. Findings indicate persistent ambiguities in consent, purpose limitation, data minimization, and cross-border data transfers, alongside evolving obligations for data fiduciaries and AI service providers. The study also illuminates the role of supervisory authorities, redress mechanisms, and risk-based compliance frameworks in promoting responsible AI. The conclusion argues for a coherent, principle-based regulatory architecture that harmonizes innovation with privacy protections, enhances transparency, and strengthens accountability to bolster public trust and sectorial resilience in India's digital future.

Keywords- Artificial Intelligence (AI); Data Protection; Cyber Law; Right to Privacy; Algorithmic Accountability; Digital Privacy; AI Regulation in India

1. Introduction

AI stands at the confluence of intellectual pursuit and technical accomplishment, different from previous technological developments by the unprecedented autonomy and understanding that AI systems exhibit. Consequently, the on-going transformation of all sections of human activity social, educational, personal, or economic—requires the legal system to ensure not only productivity and progress but also justice, fairness, safety, and security (Humerick, 2018). An equally fundamental question of equal human dignity arises when AI systems generate grievance-

es related to lack of justice, fairness, discrimination, or disproportionate injury, although these systems are mere tools of human intent, design, and programming.

India's pluralistic, multi-ethnic, and complex society confronts the challenge of reconciling rapid and radical change with its commitment to liberty, equity, and fraternity. The country's Constitution identifies life and personal liberty and privacy as vitally important in safeguarding liberty, equity, and fraternity, although both rights remain under constant pressure because of the modern digital economy's demand for vast amounts of data gathered from individuals to be used by AI systems. India's legal framework inadvertently falls short of striking the proper balance between the two opposing forces shaping the country's socio-legal environment, making it imperative to devote attention to the interplay between AI and the data economy on one hand and data protection on the other (Sood, 2015).

2. Conceptual Framework: Artificial Intelligence and Data Protection

Artificial Intelligence (AI) affects various domains, including legislative and regulatory frameworks, social and human rights, economy, business, security, research, policy-making, tourism, and governance. Unequal access to AI and digital resources generates digital divides and disparities between developed and developing nations, jeopardizing global development. AI promotes discrimination, exclusion, and bottlenecks in national and global governance. AI raises public concerns about data protection, consolidation of power and resources, weaponization, loss of income, and loss of jobs, leading some to consider it a frontline risk. AI development and use hinge on the availability of massive and diverse datasets, and data protection is crucial to the AI ecosystem, especially concerning sensitive personal data. In December 2022, the Personal Data Protection Bill 2019 was withdrawn from Parliament, and a new draft on data protection policy was introduced to address the data protection challenges associated with AI and promote AI adoption and use (Korobenko et al., 2024).

Data protection denotes the establishment of rules and guidelines to govern the collection, storage, use, processing, and sharing of personal data. Different jurisdictions adopt diverse data protection frameworks, and the following analysis focuses on Indian data protection. The 2022 Personal Data Protection Bill resembles existing regulations and policies in several jurisdictions. Newspaper articles have recently highlighted certain aspects and issues related to AI.

2.1. Definitions and Scope of AI

Artificial Intelligence (AI) is a scientific discipline and technology that aims to impart intelligence to machines, allowing them to perform tasks that require human-like thinking (Humerick, 2018). The definition encompasses a wide range of activities, from the ability of computers to process vast quantities of data to the use of intelligent assistants in mobile phones, to complex functions, such as autonomous driving. True AI requires more than brute force computing: decisions must be made, plans laid and the efficiency of alternatives evaluated. AI has therefore evolved into a complex interplay of logic, mathematical optimization, computer science, neuroscience, psychology, linguistics and philosophy, capable of tackling far-reaching issues. AI technology is rapidly changing. Two major areas of development in the 21st century are Machine Learning (ML) and Deep Learning (DL) (Korobenko et al., 2024). They signify a major shift in societal involvement with AI. Algorithms previously based on human knowledge have now been at least partially replaced by techniques that build models from vast amounts of data, typically through a training process involving many examples. Raw (unlabeled) data sets can now be tapped, enabling powerful capabilities such as data generation and unprompted creative designs.

2.2. Data Protection Principles in the Indian Context

Data protection principles, the starting point for data protection frameworks worldwide, un-



derpin obligations concerning data safeguards and information privacy. The current Indian legal regime opts for a hybrid, modified framework, drawing from the OECD's Fair Information Practice Principles and the European Union's General Data Protection Regulation (Sood, 2015). The Indian Constitution enshrines an implicit right to privacy, interpreted by the Supreme Court as a fundamental right, and the proposed Personal Data Protection Bill adopts processing principles that share features with the EU's regime. The Ministry of Electronics and Information Technology, similarly, seeks to govern AI through the Data Protection Bill and a White Paper advocating for "data empowerment" instead of ownership, lending support to the existing regime while acknowledging an informal right to data.

3. Legal Architecture Governing AI and Data Protection in India

Artificial Intelligence (AI) is changing life in unprecedented ways. AI is a class of technology that simulates intelligent behaviour in machines, which perform cognitive tasks typically associated with human intelligence, such as decision-making, learning, problem-solving, and reasoning. The general public, private and government sectors, research institutions, and even common households are rapidly embracing its adoption. The AI ecosystem consists of the AI Application, AI System, AI Service, AI Factory, AI Algorithm, AI Evaluation, AI Dataset, AI Processor, AI Computing Platform, AI Tool, and AI Security among others. The data-driven AI systems require huge amounts of data to enhance the quality of AI Output and make significant value addition to the Data. Accordingly, AI and Data Protection are mutually interconnected.

The Constitution of India provides the legal foundation for the protection of Personal Data and Privacy. The Right to Privacy is a fundamental right recognized by the Supreme Court of India under Article 21 of the Constitution. Articles 14, 19, and 21 have profound implications on the Right to Privacy and the protection of Personal Data, which is a pressing need in the context of AI. Protection of Personal Data/Data Privacy is a critical issue in the implementation of AI Systems. The Artificial Intelligence Act, 2023 states that the Artificial Intelligence System must comply with the provisions of the Personal Data Protection Act, 2021, which regulates the Processing of Personal Data and enables the protection of Data Privacy. The Data Protection Framework prescribes specific Data-related requirements that spawn across the various stages of the AI Development Life Cycle and the Production of AI Output. It establishes controls on the Processing of Personal Data, a fundamental requirement for Data-centric AI Systems (Koo, 2018).

3.1. Constitutional Foundations and Human Rights Implications

The influence of advanced technology on human rights has sparked extensive debate, particularly regarding the ethical use of artificial intelligence (AI). The rapid growth of the internet has also raised concerns over the protection of data and privacy. Although general constitutional provisions can safeguard the right to information and data protection, India lacks a specific constitutional Article addressing the use of AI in light of data protection.

The right to privacy is enshrined in Articles 1–3 of the Universal Declaration of Human Rights 1948, Articles 17 & 19 of the International Covenant on Civil and Political Rights 1966, and Article 8 of the European Convention on Human Rights 1950. Even though the right to privacy is not explicitly recognized as a fundamental right in the Constitution of India, the Supreme Court underscored the necessity of privacy protection in its landmark judgment in *Puttaswamy v. Union of India* (Justice K. J. Somaya, 2019).

3.2. Data Protection Law: Personal Data Protection Bill/Act and its Trajectories

The Personal Data Protection Bill, 2019 was introduced in Parliament on 11 December 2019. In its report dated 16 November 2022, the Joint Parliamentary Committee (JPC) recommended the Bill be reintroduced in the next Parliament following the constitution of the new govern-

ment. Its approval may lead to the establishment of the Data Protection Authority of India, and may therefore significantly influence Data Protection Regulations in the near future. Prior to recommending reforming the Bill, the JPC acknowledged ambiguities about the regulation of personal data processing even in covered sectors. India's Data Protection framework governs the links between data and AI systems, emphasizing transparency of algorithmic models while raising concerns about framing issues linked to interference in Privacy Rights of Individuals. The rapidly evolving technology of AI necessitates re-recognition of its oversight within Laws since formulations in proposed Bills become outdate by the time the Cyber Law Nation updates these Statutes. Such recognition is of utmost importance when International Jurisdictions, Institutions, and Researchers alike are engaged in AI Policy making. The continuous focus on Ethics, Regulations and Governance around AI emphasizes its indispensable role, further highlighted by the absence of Principles on Data Protection covering sensitive AI issues. Regulators must stay vigilant of Industry direction and voice concerns like control, accountability, and transparency that legitimately remain under collective ambition. Acknowledging that Investments in AI can intensify, Industry must promptly confront Enforcement Agencies and Judicial Bodies around Government Roles in Data Privacy, Sovereignty, and Policy Framing. Several organizations engaged directly or indirectly on Ground Level in Product Design, Development and Deployment gravitate toward campaigning for Freedom from Burden on Output, Legitimate Interest, and Research. AI capable of Processing Cognition and Analysis connected with Fixed Data Content, drawing attention of Developers, must decidedly resist Engagement series up to Policy Notification while seeking to converse with End Customers freely. Engagement Sectors comprising Video, Music, Movie, Art, and Literature pursue broader clarification in Data Protection.

3.3. Sectoral and Cross-Sectoral Regulations Relevant to AI

Regulatory measures governing the use of AI in India have fallen short of broader, cross-sectoral, and sector-specific data regulations, creating a fragmented regulatory landscape, vulnerability to excessive surveillance, and risks to the privacy of personal and sensitive data. Notably, sector-specific regulations complement the overarching framework provided by Acts such as the IT Act and the PDP Bill or the proposed DPA 2023. These regulations are in the domains of financial services, health, telecommunications, insurance, and power and energy. The need to update them has arisen given the rapid technological changes and their growing implications for privacy in a connected world where personal data, cloud computing, and AI-enabled systems are intertwined (Misra and Chacko, 2021). Since data subjects are increasingly targeted with the use of AI technologies, regulators must innovate and issue, such as sector-specific and cross-sectoral regulations. An integrated regulatory framework combining the principles of privacy protection and data empowerment can offer prescriptive data protection measures relevant to AI systems, particularly in determining the lawful basis of processing, limiting the retention of AI training data, minimizing the AI training data set, and restricting the disposal of sensitive data (Radanliev et al., 2024).

4. Data Processing, Privacy, and AI System Accountability

At its core, data protection fundamentally derives from the notion of the right to privacy. The Constitution of India does not expressly confer a fundamental right to privacy. This has led to divergent interpretations. Some courts, arguing against the recognition of a right to privacy, rely on Article 21 of the Constitution; others maintain that privacy is a fundamental right protected by Articles 19 and 21. The Constitution should, however, be interpreted broadly and deliberately to maximise its social justice content (Humerick, 2018).

Moreover, information technology has conquered the entire universe. Technological development enhances both the facility and capacity to access information. While technology can be



harnessed for a better society, it can also be exploited for destructive purposes, causing injury and suffering. Cybercrimes proliferate, no longer only among the high and mighty but widely occurring even in villages. Protection against crimes lies in the hands of the law. The spirit of law should ensure that criminals cannot escape the long arm of the law; but, at the same time, an upright citizen must not be adversely affected or suffer injury by the investigation of the crime. Common people are timid to report injuries and hence technology must play a vital role in that investigation, where the law itself is equipped to solve issues instead of further complicating them. Therefore, while information technology should be protected on the one hand, on the other technology itself requires protection from cyber

4.1. Data Minimization and Retention

Organizations collect vast quantities of data from customers. In 2017 only Facebook had data of 1.2 billion people—nearly every person on earth with internet connectivity. This data contains names, email addresses, search histories, friends, wireless connection details, check-ins, and interactions with people (Li et al., 2018). Data minimization aims to limit the collection of personal information. Data protection authorities, like the Dutch authority, advocate for collecting only information strictly required for specific activities. For instance, businesses frequently request consumers to send a copy of their identity documents, although knowing a date of birth or age would suffice for transactions barring age-restricted contents. Businesses should reduce records of permitted optional details and adopt or develop ground-breaking technical measures. A technical option isolates personal information within distinct silos, triggering an obligation to treat these silos as separate. A firm could then rely on a public profile, anonymized information, or a verification tool incapable of exposing the genuine usage. These solutions foster compliance with the Right to be Forgotten and simultaneously limit data development (Humerick, 2018).

4.2. Data Localization and Cross-Border Data Flows

In the context of India, one of the pressing data protection challenges is that of cross-border flows of personal data (F III Palmieri, 2019). Any law that regulates cross-border data flows must balance the positive effects of information sharing with the protection of personal data. Regulation of cross-border data flows may also diminish the need for data localization mandates. The Personal Data Protection Bill (PDPB) empowers the Data Protection Authority of India (DPA) to prohibit or restrict cross-border transfers of certain personal data if the DPA is not satisfied that the recipient entity would provide the same level of data protection. This condition appears to impose a relatively high standard, compared to, for example, the EU General Data Protection Regulation (GDPR), which allows transfers to countries outside the EU/EEA that are deemed adequate. The inapplicability of self-certification mechanisms further undermines the attractive features of PDPB's proposed approach. However, the PDPB introduces an additional 'deemed consent' mechanism for cross-border transfers made to a list of specified entities

5. Emerging Jurisprudence and Enforcement Trends

Artificial Intelligence (AI) is frequently cited in litigation, yet India's legal framework governing AI's convergence with data protection remains underdeveloped. The Personal Data Protection Bill (PDP Bill), amid legislative limbo, continues to evoke judicial interest. The Allahabad High Court recently expounded on a citizen's "right to be forgotten," and the Supreme Court has considered whether the right to privacy encompasses a right to data protection, a question amplified by AI's unique data processing characteristics. These precedents, while predating the PDP Bill, shape forthcoming statutory jurisprudence and the broader legal road map.

Alongside significant judicial interpretations, India's enforcement regime is evolving through administrative action. The Telecom Regulatory Authority of India levied a record fine on a promi-

ment telecommunications provider for contract breaches connected to fallout from an AI-enabled data breach. Cases involving breaches of the Information Technology Act, 2000 (IT Act) and its related rules, along with complaints before the proposed Data Protection Authority (DPA), have emerged since the PDP Bill's introduction. Legal recourse for data subjects impacted by AI-generated knowledge and its adverse socioeconomic effects is likewise developing.

5.1. Judicial Interpretations of Data Protection Obligations

The judicial interpretation of obligations concerning data protection has evolved through legal discourse, shaping the context within which artificial intelligence (AI) must operate. The judiciary, while limited in explicitly articulating a data protection framework, has nevertheless indirectly influenced and informed the evolving data protection, personal data privacy, and AI literature (Humerick, 2018). This influence highlights the imperative of timely and informed responses to rapid technological change, especially regarding AI and robotics. A regulatory paradigm that focuses on data privacy and protection narrows the scope for determining the legal status of individuals in relation to data aggregation in AI settings. Such a paradigm bears certain expectations that AI must still satisfy and necessitates further deliberation regarding distinct obligations and liabilities concerning personal data. At a technical level, the precise measures that allow for compliance with data laws deserve additional exploration.

5.2. Enforcement Actions and Administrative Safeguards

Artificial Intelligence (AI) represents a significant technological advancement but also poses risks relating to safety, liability, privacy, and security. Within this context, enforcement actions and administrative safeguards establish first steps for regulatory frameworks to ensure AI is deployed responsibly. A great deal of regulatory efforts concerning AI focus on its development, deployment, and use as big data analytics. Such analytics, central to many AI systems, must comply with statutory standards like data privacy, protection, and proportionality when collecting, storing, and processing personal data. Accountability and transparency requirements further enforce compliance with existing data-protection principles. The European regulatory landscape provides an important influence on AI, shaping how firms develop and deploy such technology and reinforcing the necessity for compliance. To augment AI regulations that compete with existing data privacy laws, U.S. federal and state authorities seek to develop a more coherent approach that centers on consumer protection, civil rights, and civil liberties while addressing broader ethical considerations that go beyond specific regulatory objectives. The broad scope of the General Data Protection Regulation (GDPR), combined with its extra-territorial jurisdictional reach, raises international issues under the Proposed Artificial Intelligence Act by creating uncertainty about how various provisions should be interpreted and operationalised.

5.3. Remedies for Data Subjects in AI Contexts

Data subjects in the EU enjoy specific rights under the General Data Protection Regulation (GDPR) intended to enhance their control over personal information (Humerick, 2018). These rights notably include the right to data portability, allowing data subjects to retrieve and transfer their personal data among service providers, and the right to erasure, commonly referred to as the right to be forgotten, compelling controllers to delete data associated with a data subject upon request. When applied to AI applications and systems, these provisions generate requirements for transparency concerning the datasets employed, as well as the procedures and methodologies employed in the training and validation of models. Absent such information, prospective AI system operators face significant uncertainty regarding their ability to process data legally or at all. Large datasets remain essential for AI developers to maintain competitive advantage, affecting the strategic choices made by a significant number of enterprises and constrained



by generative capabilities now damaged through loss of trust. Consequently, firms increasingly prioritize compliance with data security regulations and invest in public relations efforts aimed at safeguarding consumer confidence. Systemically relevant breaches may elicit a decrease in trust perceived by the public and subsequently lead to widespread demands for data deletion or migration to alternative systems. The potential of such occurrences to jeopardize the further development of AI capabilities and the considerable threats—whether legal, operational, or otherwise—to organizations devoted to advancing the AI frontier render justification for actions taken within this domain a subject of heightened interest.

6. Challenges and Gaps in the Current Framework

Artificial Intelligence (AI) is a transformative technology rapidly integrating into myriad aspects of daily life (Korobenko et al., 2024). Consideration of acceptable ethical behavior when developing AI is therefore becoming increasingly important. Proper stakeholder engagement is necessary since AI can be both highly beneficial and deeply harmful. For example, advanced AI-based systems capable of collecting, analyzing, and storing large amounts of sensitive personal data have sparked discussions about privacy, transparency, accountability, and discrimination concerns. As technology advances, compliance with existing data protection regulations is challenging. Scanning, collecting, and organizing individuals' sensitive information for financial, health, and movement-related data without proper consent, context, or time indication continues to pose threats. Transfer of sensitive data to and from purposefully vague locations further complicates this dilemma.

6.1. Ambiguities in AI Regulation and Dynamic Technological Change

Artificial Intelligence (AI) regulation is fraught with ambiguities due to its dynamic nature. Various international organizations, including the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Internet Governance Forum (IGF), continue to address the knowledge economy in relation to AI. As an appellation, AI does not denote a single technology; it represents a collection of algorithms and knowledge-designing procedures that empower digital devices to simulate human thinking (Abhivardhan, 2020). Data concerning identity is not confined to textual identity but embodies various traces of personal and cultural knowledge. If an individual's data covering textual material is the sole focus, the AI emulation of writing capabilities may offer limited insight into genuine human empathy; even high Proficiency in textual composition does not guarantee that the individual has assimilated traits such as care and understanding into their cultural fabric. Intertwined with the data-centric, probabilistic character of AI-enhanced systems and their exclusion from a comprehensive data and algorithm-regulating framework, uncertainty regarding the fulfilment of widely acknowledged ethical principles, much less cultural values, prevails at present (Fernández Llorca et al., 2022).

6.2. Balancing Innovation with Privacy Interests

Despite the rapid advancement of artificial intelligence (AI)-related technologies, concerns related to data protection and usage have also increased dramatically. The use of AI technologies without a well-defined legal framework has serious implications for the protection of data and privacy as these technologies use people's data for training their delicate algorithms, compounding the existing risks associated with sensitive data leaks, sharing, hacking, etc. On the one hand, AI technologies help hone intellectual capabilities for progress and create huge socio-economic gains, while on the other hand, the present and future equilibrium of individual privacy rights, data protection, and the growth of AI technologies in India is a significant challenge in India. On the one hand, the creators of AI bots claim that the general use of AI should not hamper individual privacy rights and the development of AI technologies and legitimacy rely on the regulation

of AI. Hence, the private and public dimensions of privacy under the entering of the AI era; the premises under which the future privacy rights, data protection, and AI adaptability will coexist or thrive is critical now and in the next 10–20 years. Will the bedrock of legislation governing the protection of individual data privacy and protection continue to play a significant role? (Sood, 2015) ; (Humerick, 2018) ; (Murdoch, 2021).

6.3. Data Subject Empowerment and Redressal Gaps

Data subject empowerment is considered a fundamental precondition for the realization of data protection rights as set out in the Indian Data Protection Bill. However, the draft Bill does not explicitly address the need to establish a regime for the effective exercise of such rights, and textual gaps exist with respect to empowerment in the context of data subjects needing to exercise their rights with substantial VC-law [

Institutional frameworks are essential for complying with data protection rights established in various jurisdictions, in which recourse to courts to protect these rights is generally deemed a last resort. Within the European Union, the General Data Protection Regulation allows, or rather requires, data subjects to choose between lodging complaints with supervisory authorities and bringing legal actions against controllers or processors. In other parts of the world, data protection laws recognize widespread institutional empowerment models and highly institutionalized frameworks for exercise of rights that favor empowerment via a regulated intermediary. The lack of an intricate state apparatus and limited know-your-customer capabilities impact the Indian context. Most recourse and rights frameworks mirror the contours of fundamental rights evolution in general law and commonly strive to protect the same underlying issues by means of participatory instruments and enhanced community access.

7. Comparative Perspectives and Lessons from Global Jurisdictions

Artificial intelligence (AI) technologies are advancing rapidly and contribute to fundamental changes in various private and public activities (Basu, 2012). Accordingly, the pace of introduction of new AI-related legal frameworks in many jurisdictions continues to accelerate (F III Palmieri, 2019). In parallel to establishing such frameworks, the discussion on the impact of AI technologies on persons' fundamental rights, including data protection rights, is also intensifying (Humerick, 2018). Against this background, a brief overview of the scope of the rules governing the use of AI technologies in other jurisdictions is pertinent. The European Union (EU) has around 450 million inhabitants and the most extensive legislative framework for the protection of data within the public and private domains. Amongst the many legislative activities undertaken, regulation 2016/679, known as the General Data Protection Regulation (GDPR), has established an unprecedentedly high level of protection applicable to every person in the EU. The regulation has been recognised at a global level not only for its implementation of data protection measures but also as a model to follow for its external impact on case law, private sector activity, cooperation between agencies and public opinion. In the United States of America (USA), there is no general law dedicated to the protection either of privacy or of data, nor does the law recognize a right associated with either. Instead, legislation is developed according to specific areas, covering specialised commercial activities, or risk-associated areas. Nonetheless, prior to the introduction of another regulation regarding the data protection of natural persons, the Federal Trade Commission (FTC) was the principal authority involved in regulating mass gathering and automated processing. Since 2016, the primary focus of various public and private stakeholders has been the construction of guidelines relating to the ethical usage of AI technologies.

7.1. European Union General Data Protection Regulation and AI Liability

The General Data Protection Regulation (GDPR) governs the protection of personal data in



the European Union, with significant implications for the development of artificial intelligence (AI) systems (Humerick, 2018). AI applications rely on large volumes of personal data for functionality, making compliance with the GDPR necessary for their lawful deployment (Meszaros et al., 2022). Notably, the GDPR prohibits automated decision-making based solely on personal data unless certain conditions exist, such as obtaining the subject's explicit consent. These provisions should be viewed against a broader legal context, as the EU seeks to establish legislative measures governing the liability associated with AI systems. While the GDPR partially regulates AI by focusing on data protection and the prevention of harmful automated decision-making (ADM), it does not comprehensively address the issue of AI-related liability.

Because the Indian ecosystem exhibits critical characteristics of both privacy and non-privacy regimes, an examination of the requirement to strengthen data protection by reference to the evolving European scheme remains relevant. As neighbouring jurisdictions move towards policy documents that explicitly consider formal integration with the GDPR in the AI context, there are opportunities to refine the extent and focus of the evolving Indian policy framework.

8. Policy Recommendations and Reform Pathways

The preceding discussions outline the pressing need to align data protection laws with the rapid evolution of artificial intelligence (AI) technologies. To this end, the following three policy recommendations are outlined: 1) strengthen the Personal Data Protection Bill, 2019, to facilitate the incorporation of AI-specific provisions consistent with the central law; 2) establish AI-specific governance mechanisms and regulatory sandboxes to explore complex issues requiring tailored, context-dependent solutions; and, 3) formulate a robust institutional framework devoted to establishing a compliance ecosystem, ensuring accountability, guiding adoption, and building public trust (Humerick, 2018).

Strengthening the Personal Data Protection Bill, 2019 would allow the Centre to legislate independently on AI-related issues—including data processing, algorithmic bias, data sharing, and liability—under the 2019 Bill. The challenges generated by ongoing technological developments necessitate measures that enable proactive consideration of emerging issues (F III Palmieri, 2019). Emphasizing their intersection with AI, such measures could encompass restrictions on automated decision-making, the establishment of algorithmic-impact assessments, and sectoral codes of practice governing AI use in specific domains. These requirements could be embedded in yet-to-be-finalised sectoral regulations such as the Draft E-commerce Regulatory Framework and the Draft National Telecommunication Policy.

8.1. Strengthening Data Protection Legislation in AI Contexts

Rapid advances in Artificial Intelligence (AI) technologies are leading to new challenges for data protection legislation and policy. While the effective governance of the AI sector is critical for accelerating the growth of India's digital economy, there is an urgent need to strengthen the existing data protection framework to address the unique risks posed by information technologies, especially machine learning algorithms (Humerick, 2018). AI systems have the capacity to generate personal data (Sood, 2015), process these data without knowledge or consent, and actively exploit, undermine, and even erode privacy across a range of applications, threatening established social contracts and constitutional safeguards. As the data protection regulatory framework undergoes reexamination and revision in response to these challenges, there is a need for full transparency regarding the nature of amendments proposed and stakeholder consultations in particular, given their impact on AI. The requirements for AI systems should comprehensively include explicit consent, clear legal grounds, purpose limitation, minimization, retention period specification, enabling of user deletion, and localization of primary data. Such protection measures for foundational datasets and emerging data interchange markets should

be enabled, particularly to protect public, private, and sensitive data. Data subjects generally must also remain empowered to elevate grievance resolution across multiple layers. AI-related requirements should encompass accountability for systems and redress mechanisms to users, data subjects, societal risks, algorithm choices, and significant information if proprietary reluctance persists.

8.2. AI-Specific Governance Mechanisms and Regulatory Sandboxes

AI and related aspects raise numerous policy and regulatory challenges globally. Regulatory sandboxes are one approach to managing novel and complex technologies. They provide for an environment where actors can temporarily test innovative, tech-based solutions subject to certain safeguards without incurring the usual regulatory consequences. While the controllable risk involved provides the basis for temporary reductions in regulatory liability, the responsible testing of an experimental AI system cannot be guaranteed. Emerging AI systems can present unprecedented safety impacts due to their unknown and variable behaviour. Responsible AI is thus a primary focus and traverses many areas, including explainability, transparency, propriety, and accountability. A cautionary framework is required to ensure that AI risk assessment considers danger, not only the likelihood of a highly undesirable outcome.

In addition to regulatory sandboxes, the establishment of a government-appointed statutory body with AI domain expertise is essential. Such agencies would engage with an AI taxonomy committee to develop a detailed classification and taxonomy for AI systems and their systems' impact distribution in a country. These taxonomies would provide the regulatory and oversight scaffold for R&D and innovation in both delivering and deploying AI. Aspects of AI technology may also come under government and sector-specific experimental testing and use guidelines. A limited-scope pre-market AI technology and product approval may be adopted for specific high-risk areas, especially those involving issues of continued governance, eg software systems affecting highways, aviation, space travel, maritime, power, health, and weapons.

9. Conclusion

The interplay between artificial intelligence and data protection in India raises critical questions about the existing legal framework and the shape of future legislation. The foundational principles of data protection are well established, and courts have begun to lay the groundwork for regulatory oversight. However, data protection legislation remains incomplete, and the regulatory framework for AI continues to evolve. Contemporary jurisprudence indicates that emerging technologies, including artificial intelligence, cannot escape the existing regime, though nuances specific to such technologies have yet to be addressed.

Engagement with international thought and comparative regulation can help bring foundational principles and instrument modalities into sharper focus. Among the rich variety of governance approaches, several jurisdictions offer salient lessons. The EU's model for artificial intelligence liability is particularly relevant, while the United States prevailing commercial orientation – including the active development of sector-specific data protection, as well as ethics, trust, and accountability guidelines – merits reflection. Meanwhile, Japan and Singapore showcase frameworks that respect existing legal and regulatory constructs while enhancing transparency and accountability (Humerick, 2018) ; (Sood, 2015).

Author's Declaration:

I/We, the author(s)/co-author(s), declare that the entire content, views, analysis, and conclusions of this article are solely my/our own. I/We take full responsibility, individually and collectively, for any errors, omissions, ethical misconduct, copyright violations, plagiarism, defamation, misrepresentation, or any legal consequences arising now or in the future. The publisher, editors, and reviewers shall not



be held responsible or liable in any way for any legal, ethical, financial, or reputational claims related to this article. All responsibility rests solely with the author(s)/co-author(s), jointly and severally. I/We further affirm that there is no conflict of interest financial, personal, academic, or professional regarding the subject, findings, or publication of this article.

References:

1. Humerick, M. "Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence." 2018. [PDF]
2. Sood, G. "COMPARATIVE ANALYSIS OF CYBER PRIVACY LAW IN INDIA AND IN THE UNITED STATES OF AMERICA." 2015.
3. Korobenko, D., Nikiforova, A., and Sharma, R. "Towards a Privacy and Security-Aware Framework for Ethical AI: Guiding the Development and Assessment of AI Systems." 2024.
4. Koos, S. "ARTIFICIAL INTELLIGENCE æ“ SCIENCE FICTION AND LEGAL REALITY." 2018.
5. Julia Levine, M. "Biometric Identification in India Versus the Right to Privacy: Core Constitutional Features, Defining Citizens' Interests, and the Implications of Biometric Identification in the United States." 2019.
6. Misra, A. and Chacko, M. "Square pegs, round holes, and Indian cybersecurity laws." 2021. ncbi.nlm.nih.gov
7. Radanliev, P., Santos, O., Brandon-Jones, A., and Joinson, A. "Ethics and responsible AI deployment." 2024. ncbi.nlm.nih.gov
8. Li, T., Fosch Villaronga, E., and Kieseberg, P. "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten." 2018.
9. F III Palmieri, N. "Data Protection in an Increasingly Globalized World." 2019.
10. Larsson, S. "The Socio-Legal Relevance of Artificial Intelligence." 2019.
11. Ramesh, D., Kameswaran, V., Wang, D., and Sambasivan, N. "How Platform-User Power Relations Shape Algorithmic Accountability: A Case Study of Instant Loan Platforms and Financially Stressed Users in India." 2022.
12. Heim, L., Fist, T., Egan, J., Huang, S., Zekany, S., Trager, R., A Osborne, M., and Zilberman, N. "Governing Through the Cloud: The Intermediary Role of Compute Providers in AI Regulation." 2024.
13. Abhivardhan, undefined "The Ethos of Artificial Intelligence as a Legal Personality in a Globalized Space: Examining the Overhaul of the Post-liberal Technological Order." 2020. ncbi.nlm.nih.gov
14. Fernández Llorca, D., Charisi, V., Hamon, R., Sánchez, I., and Gómez, E. "Liability regimes in the age of AI: a use-case driven analysis of the burden of proof." 2022.
15. Murdoch, B. "Privacy and artificial intelligence: challenges for protecting health information in a new era." 2021. ncbi.nlm.nih.gov
16. Basu, S. "Privacy Protection: A Tale of Two Cultures." 2012.
17. Meszaros, J., Minari, J., and Huys, I. "The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union." 2022. ncbi.nlm.nih.gov
18. Ayappane, B., Vaidyanathan, R., Srinivasa, S., and Deshmukh, J. "Extensible Consent Management Architectures for Data Trusts." 2023.

Cite this Article

"Dr. Kamal Kishor", "Artificial Intelligence and Data Protection in India: A Cyber Law Perspective", Shodhpith International Multidisciplinary Research Journal, ISSN: 3049-3331 (Online), Volume:2, Issue:04, July-August 2026.

“Copyright © 2026 The Author(s). This work is licensed under Creative Commons Attribution 4.0 (CC-BY), allowing others to use, share, modify, and distribute it with proper credit to the author.”