Page 402 - 413 **DOI:** *https://doij.org/10.10000/IJLMH.1111159*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 1

2026

Legal Obligations of AI Developers under Privacy Laws: An Analysis of the Indian Regulatory Framework

DR. NEERA SHUKLA[1] AND MS. LALITA SINGH BAGHEL[2]

ABSTRACT

Artificial Intelligence (AI) has revolutionized numerous industries, transforming the way businesses operate and redefining the contours of innovation. As AI technologies continue to advance, they are increasingly being deployed in various sectors, including healthcare , finance, education, and transportation. However, this rapid growth has also raised critical concerns regarding data privacy, security, and ethical considerations.

In India, the burgeoning AI industry has significant implications for legal professionals, policymakers, and developers. As AI systems increasingly collect, process, and analyze vast amounts of personal data, ensuring compliance with Indian data protection laws becomes paramount. The Indian government has taken steps to regulate data protection and privacy, with the Digital Personal Data Protection Act, 2023 (DPDPA) being a significant development in this regard.

This paper provides an in-depth analysis of the legal obligations of AI developers in India, examining the current regulatory framework, emerging laws, and sector-specific regulations. It highlights the gaps in the current legal framework and the challenges developers face in ensuring compliance, with a focus on fostering trust and ethical AI practices. The paper also offers recommendations for AI developers, policymakers, and regulators to bridge the divide between innovation and legal compliance, ensuring that AI technologies are developed and deployed in a responsible and ethical manner.

Keywords: *AI, Privacy, DPDPA*

I. INTRODUCTION

Artificial Intelligence (AI) has become an indispensable driver of innovation in the modern era, revolutionizing sectors like healthcare, finance, education, and transportation. By enabling predictive analytics, automation, and data-driven decision-making, AI has opened new possibilities for efficiency and precision in these industries.

[1] Author is the Head of Department & Associate Professor at Technocrats Institute of Law, Bhopal, M.P., India.
[2] Author is an Assistant Professor at Technocrats Institute of Law, Bhopal, M.P., India.

 [ISSN 2581-5369]

However, the deployment of AI systems is not without challenges. With their reliance on large volumes of data, including sensitive personal information, concerns about privacy, security, and ethical accountability have become increasingly prominent.

India, as one of the fastest-growing technology markets, has witnessed a surge in AI adoption across various domains. The Indian government has recognized the need for robust data protection measures, introducing laws like the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, to regulate data processing activities.

These laws impose significant responsibilities on AI developers, ranging from ensuring transparency and accountability to adhering to stringent consent and data localization requirements. Yet, the rapid evolution of AI technologies has outpaced legislative efforts, leaving several legal and ethical questions unanswered.

The advent of Artificial Intelligence (AI) has revolutionized numerous industries, transforming the way businesses operate, and redefining the contours of innovation. As AI technologies continue to advance, they are increasingly being deployed in various sectors, including healthcare, finance, education, and transportation.

However, this rapid growth has also raised critical concerns regarding data privacy, security, and ethical considerations. In India, the burgeoning AI industry has significant implications for legal professionals, policymakers, and developers.

As AI systems increasingly collect, process, and analyse vast amounts of personal data, ensuring compliance with Indian data protection laws becomes paramount. The Indian government has taken steps to regulate data protection and privacy, with the Digital Personal Data Protection Act, 2023 (DPDPA) being a significant development in this regard.

II. CURRENT LEGAL FRAMEWORK IN INDIA

The current legal framework for data protection and privacy in India is primarily governed by the Information Technology Act, 2000 (IT Act)[3], and the rules[4] and regulations made thereunder, along with the provisions of the Bharatiya Nyay Sanhita (BNS)[5].

Information Technology (IT) Act, 2000

The IT Act serves as India's foundational legislation for data protection.[6] Section 43A mandates

[3] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[4] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
[5] The Bhartiya Nyay Sanhita, 2023.
[6] Pooja Sharma, Data Protection in India: A Critical Analysis, 10 J. Indian L. & Soc'y 67, 71 (2018)

 [ISSN 2581-5369]

that entities handling sensitive personal data adopt reasonable security practices. This provision, while crucial, is broad and does not cater to the complexities introduced by modern AI systems.[7] Challenges such as algorithmic bias, transparency, and automated decision-making are not explicitly addressed, leaving a regulatory gap that could allow misuse or mishandling of personal data in AI contexts.[8]

Key Provisions:

1. Section 43A: Imposes liability on entities failing to implement reasonable security practices for sensitive personal data.[9]

2. Section 72A: Penalizes unauthorized disclosure of personal information by intermediaries and service providers.[10]

3. Section 79: Provides safe harbour protections for intermediaries, such as online platforms and service providers.[11]

IT Rules, 2011

The IT Rules, framed under the IT Act, define sensitive personal data and prescribe reasonable security practices and procedures. These rules emphasize obtaining consent before collecting personal information and ensuring its protection. However, they fail to consider AI-specific nuances such as predictive analytics, the use of machine learning models, and the ethical accountability of AI systems. For example, while the rules stress data security, they do not mandate developers to explain how AI algorithms can reach decisions, which could have significant implications for transparency and trust.

Key Provisions:

1. Definition of Sensitive Personal Data: Includes personal information such as passwords, financial information, and health records.[12]

2. Reasonable Security Practices: Requires entities to implement reasonable security practices to protect sensitive personal data.[13]

3. Notice Requirements: Requires entities to provide notice to data subjects in the event of a

[7] Information Technology Act, 2000, § 43A.
[8] G. S. Hans, Artificial Intelligence and Law in India: A Critical Analysis, 11 J. Indian L. & Soc'y 35, 41 (2019).
[9] Information Technology Act, 2000, § 43A.
[10] Id. Sec. 72A
[11] Id. Sec. 79
[12] Supra note 5, Rule 3.
[13] Ibid, Rule 8.

 [ISSN 2581-5369]

data breach.[14]

Bharatiya Nyay Sanhita (BNS) Provisions

The BNS includes provisions related to data and privacy, including:

- Section 123: Imprisonment for unauthorized access to computer systems or data.

- Section 124: Imprisonment for unauthorized disclosure of personal information.

- Section 125: Imprisonment for unauthorized use of personal information.

Digital Personal Data Protection Act (DPDP), 2023

. The DPDPA is poised to redefine data privacy in India, introducing significant obligations for entities, including AI developers:

- Consent-centric Processing: AI systems must obtain explicit user consent for data processing activities.[15]

- Transparency and Accountability: Developers must ensure transparency in AI decision-making processes and maintain accountability for data handling.[16]

- Data Principal Rights: Users (data principals) are granted rights to access, correct, or delete their data, and developers must enable mechanisms for exercising these rights.[17]

- Cross-border Data Transfer: AI developers handling sensitive data must comply with stringent rules on data storage and transfer, potentially necessitating data localization.[18]

Personal Data Protection Bill, 2019 (Pending)

The Personal Data Protection Bill, intended to overhaul India's data protection framework, offers promising advancements in safeguarding individual rights. Key highlights include:

- *Mandatory Data Localization*: Sensitive personal data must be stored within India, aiming to enhance data sovereignty and security.[19]
- ***Explicit Consent Requirements***: Entities must obtain unambiguous consent before processing personal data, emphasizing user control over data usage.[20]

[14] Id., Rule 5(8)
[15] Digital Personal Data Protection Act, No. 22 of 2023, Sec. 4, Gazette of India, Part II, § 3(ii) (Aug. 11, 2023).
[16] Id., Sec.10-11.
[17] Id. Sec. 9
[18] Id. Sec. 15-16.
[19] Digital Personal Data Protection Bill, Bill No. 20 of 2023, cl. 15(1), Gazette of India, Part II, § 2 (July 28, 2023)
[20] Id., Cl. 7(1)

 [ISSN 2581-5369]

- ***Data Subject Rights***: Provisions like the right to be forgotten and the right to data portability align with global standards, empowering individuals to manage their data.[21]

Despite its comprehensive approach, the bill has faced delays in enactment. Its pending status creates a legislative vacuum, complicating compliance for AI developers who operate in a rapidly evolving technological and legal landscape. Without clear guidelines, developers may struggle to align their practices with anticipated legal expectations, particularly in areas like automated profiling and cross-border data transfers

Despite its potential, the bill remains pending, leaving a legislative vacuum that complicates compliance for AI developers.

III. SECTOR-SPECIFIC REGULATIONS

The deployment of AI technologies varies significantly across industries, each governed by distinct legal and ethical considerations. Sector-specific regulations add an additional layer of complexity for AI developers, who must ensure that their systems meet the specific requirements of the domains they serve.

Healthcare

AI-driven healthcare applications, such as diagnostic tools and patient management systems, must comply with privacy norms under the **Clinical Establishments Act, 2010**[22], and other relevant sectoral guidelines[23]. These regulations emphasize the protection of patient confidentiality[24], the secure handling of sensitive health data, and adherence to ethical principles in AI deployment.[25] For instance, AI systems analyzing patient data must ensure strict data anonymization[26] and obtain informed consent before processing sensitive information.[27]

Banking and Financial Services

In the financial sector, AI systems are governed by mandates issued by the **Reserve Bank of India (RBI)**,[28] which emphasize data security[29] and ethical data processing.[30] The RBI has

[21]Id., Cls. 9(2), 11.
[22] Clinical Establishments (Registration and Regulation) Act, 2010, § 12.
[23] Ministry of Health and Family Welfare, Guidelines for Healthcare Providers on Electronic Health Records (2016).
[24] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, § 7.14.
[25] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3
[26] Ministry of Health and Family Welfare, National Health Policy (2017).
[27] Supra Note 26, Rule 4.
[28] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, § 7.15.
[29] Reserve Bank of India, Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Security (2016)
[30] Ibid, para., 3.2

introduced guidelines for AI and machine learning applications,[31] requiring developers to implement robust IT frameworks to ensure operational security.[32] Additionally, data localization requirements necessitate that sensitive financial data be stored within India,[33] creating challenges for multinational AI developers.

Telecom

The **Telecom Regulatory Authority of India (TRAI)** sets the standards for AI-powered telecom services,[34] focusing on user consent,[35] data security,[36] and transparency.[37] Developers must align their systems with TRAI guidelines,[38] which aim to protect consumer rights and prevent data misuse in AI-enabled telecom applications.[39] This includes ensuring that AI systems used in customer service, network optimization, and fraud detection[40] operate in compliance with privacy norms.

E-commerce and Retail

AI systems in e-commerce and retail sectors must comply with consumer protection laws, emphasizing transparent data handling and avoiding deceptive practices. Personalized recommendations and targeted advertising powered by AI must align with principles of fairness and consumer consent, ensuring ethical data utilization.

Transportation

Autonomous vehicles and AI-based traffic management systems operate in a regulatory grey area in India, with limited legal guidance on safety and liability issues. Developers must anticipate the need for compliance with broader privacy and cybersecurity laws, while also advocating for clearer sector-specific guidelines to address the unique challenges of AI in transportation.

By tailoring AI systems to meet the specific regulatory requirements of these sectors, developers can mitigate legal risks while fostering trust and ethical AI adoption across industries.

[31] Ibid, para., 3.3
[32] Reserve Bank of India, Guidelines on Artificial Intelligence and Machine Learning for Banks (2020).
[33] Ibid, para 4.2.
[34] Supra Note 30. Para., 3.4.
[35]Telecom Regulatory Authority of India, Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector (2018).
[36]Ibid. Para. 3.2.
[37]Ibid. Para. 3.3
[38]Ibid. Para. 3.4
[39]Supra note 36.
[40]Ibid

 [ISSN 2581-5369]

IV. LEGAL OBLIGATIONS OF AI DEVELOPERS

1. Data Collection and Consent

AI developers must ensure that data collection practices comply with the principles of transparency and consent. This includes:

- *Clearly Informing Users*: Developers must clearly inform users about the purpose of data collection, including the types of data being collected and how it will be used.[41]

- *Obtaining Explicit Consent*: Developers must obtain explicit consent for sensitive personal data, such as financial information or health records.[42]

- *Implementing Age Verification Mechanisms*: Developers must implement age verification mechanisms to ensure that children's data is protected in accordance with applicable laws and regulations.[43]

2. Data Minimization and Purpose Limitation

Developers are obligated to collect only the data necessary for specific purposes and to avoid using data for unrelated activities. This aligns with global best practices, such as the General Data Protection Regulation (GDPR). Key considerations include:

- *Data Minimization*: Developers must collect only the minimum amount of data necessary to achieve the specified purpose.[44]

- *PurposeLimitation*: Developers must ensure that data is used only for the specified purpose and not for unrelated activities.[45]

3. Algorithmic Transparency

AI systems often operate as "black boxes," making it difficult for users to understand how decisions are made. Developers must ensure transparency by:

- *Providing Explanations*: Developers must provide explanations for automated decisions, including the factors that contributed to the decision.[46]

- *Disclosing Data Sources*: Developers must disclose the data sources used for training AI

[41] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, art. 5(1)(a)-(b), 2016 O.J. (L 119) 1 (EU)
[42] Id. art. 7(1)
[43] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2018)
[44] Id. art. 25(1)
[45] See GDPR, supra note 3, art. 12(1)
[46] Artificial Intelligence Act Proposal, European Commission, COM (2021) 206 final (Apr. 21, 2021).

models, including any biases or limitations in the data.[47]

4. Data Security and Anonymization

AI developers must implement robust security measures to protect personal data from breaches. This includes:

- *Encrypting Sensitive Data*: Developers must encrypt sensitive data, both in transit and at rest.[48]

- *Employing Anonymization Techniques*: Developers must employ anonymization techniques to reduce privacy risks, such as pseudonymization or data masking.[49]

5. Accountability and Compliance

Developers must establish mechanisms for accountability, including:

- *Conducting Regular Audits:* Developers must conduct regular audits of AI systems to ensure compliance with legal and ethical standards.

- *Ensuring Compliance with Legal and Ethical Standards*: Developers must ensure that AI systems comply with applicable laws and regulations, as well as ethical standards and industry best practices.

6. Ethical Considerationin AI D: Avoiding Bias and Discrimination

AI systems must be designed to prevent biases that could lead to discriminatory outcomes. Developers must:

- *Regularly Test AI Models for Fairness*: Developers must regularly test AI models for fairness and bias, using techniques such as bias detection and mitigation.

- *Ensure Diversity in Training Data*: Developers must ensure that training data is diverse and representative of the populations that will be affected by the AI system.

7. Ensuring User Autonomy

Developers should empower users to make informed decisions by providing clear information about AI capabilities and limitations. This includes:

- *Providing Transparent Explanations*: Developers must provide transparent explanations of AI

[47] ISO/IEC 27001:2022 – Information Security Management Systems – Requirements, Int'l Org. for Standardization.

[48] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development (OECD), art. 7 (1980). Available at: https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html

[49] U.K. Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR): Accountability and Governance, https://ico.org.uk.

 [ISSN 2581-5369]

decision-making processes, including the factors that contributed to the decision.[50]

- *Disclosing Limitations and Uncertainties*: Developers must disclose the limitations and uncertainties of AI systems, including any potential biases or errors.[51]

8. Balancing Innovation and Privacy

While innovation is essential, it should not come at the cost of privacy. Developers must adopt a privacy-by-design approach, embedding privacy considerations into the development lifecycle. This includes:

- *Conducting Privacy Impact Assessments*: Developers must conduct privacy impact assessments to identify and mitigate potential privacy risks.[52]

- *Implementing Privacy-Enhancing Technologies*: Developers must implement privacy-enhancing technologies, such as encryption and anonymization, to protect personal data.[53]

9. Global Best Practises

India can draw lessons from global regulatory frameworks to strengthen its privacy laws. Key practices include:

1. *GDPR (European Union):* Emphasizes data subject rights, accountability, and transparency.

2. *Children's Online Privacy Protection Act (COPPA) (United States):* Focuses on protecting children's privacy online.

3. *Artificial Intelligence Act (European Union):* Proposes risk-based regulations for AI systems.

V. CHALLENGES FACED BY AI DEVELOPERS IN INDIA

1. **Regulatory Ambiguity:** The absence of AI-specific regulations leaves developers navigating through a fragmented and outdated legal framework. This lack of clarity makes it difficult to align AI practices with existing laws.
2. **Limited Awareness and Expertise:** Many AI developers and organizations are not fully aware of the intricacies of privacy laws or their ethical obligations. This knowledge gap often results in non-compliance, whether intentional or not.

[50] U.N. Office of the High Commissioner for Human Rights (OHCHR), Guiding Principles on Business and Human Rights, princ. 13 (2011). Available at: https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights
[51] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, FTC Report to Congress 11–13 (2012), Available at: https://www.ftc.gov/reports .
[52] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, Jan. 28, 1981, E.T.S. No. 108, art. 6. Available at: https://www.coe.int/en/web/data-protection/convention108-and-protocol
[53] Ibid 14

3. **Enforcement Gaps:** Weak enforcement of existing laws reduces the accountability of AI developers. The inconsistency in regulatory oversight further exacerbates non-compliance issues.
4. **Algorithmic Transparency Challenges:** AI models, particularly complex ones like deep learning networks, often function as "black boxes." Explaining their decision-making processes to regulators, users, or other stakeholders is both technically and legally challenging.
5. **Data Localization Costs:** The DPDPA's requirements for storing sensitive data within India increase operational costs, particularly for developers managing global AI systems. This could deter foreign investments and collaborations.
6. **Bias in Datasets:** Ensuring that training data is unbiased and representative is a persistent challenge. Biased datasets can lead to discriminatory AI outcomes, raising ethical and legal concerns.
7. **Dynamic Nature of AI Systems:** AI models frequently evolve through retraining and updates, making it difficult to ensure continuous compliance with privacy regulations.
8. **Interoperability of Laws:** Balancing Indian data protection requirements with global standards, such as the GDPR, poses challenges for developers with operations spanning multiple jurisdictions.
9. **High Costs of Compliance:** Implementing robust privacy-preserving techniques like encryption, anonymization, and regular audits add significant costs, which may be burdensome for smaller enterprises or startups.
10. **Lack of Ethical Standards:** In the absence of widely accepted ethical guidelines, developers struggle to integrate fairness, accountability, and transparency into their systems.

VI. RECOMMENDATIONS

1. **Establish AI-Specific Regulations:** India should introduce dedicated legislation for AI to address unique challenges like algorithmic transparency, automated decision-making, and ethical considerations. These regulations should also define accountability mechanisms and standards for safe AI deployment.
2. **Strengthen Data Protection Framework:** The government should prioritize passing the Personal Data Protection Bill, ensuring it accommodates AI-specific complexities.

 [ISSN 2581-5369]

Provisions for AI accountability, data minimization, and consent mechanisms should be explicitly included.

3. **Promote Industry Collaboration:** Regulators should work with industry stakeholders, academia, and think tanks to co-develop practical guidelines that balance innovation with privacy and security.
4. **Enhance Awareness and Training:** Conduct training programs and awareness campaigns for AI developers on legal and ethical obligations. Educational institutions can introduce specialized courses on AI ethics and compliance.
5. **Foster Research and Development in Explainable AI (XAI):** Invest in research on explainable AI to address the transparency and accountability challenges associated with "black box" models.
6. **Support Startups and SMEs:** The government can provide incentives, grants, or subsidies to startups and small enterprises to ease the financial burden of implementing data protection measures.
7. **Strengthen Enforcement Mechanisms:** Enhance regulatory oversight through specialized AI compliance bodies that can audit and guide developers effectively. Penalties for violations should be proportionate but significant enough to deter non-compliance.
8. **Adopt Global Best Practices:** India should align its AI and data protection laws with global frameworks, such as the GDPR and the EU's Artificial Intelligence Act, to facilitate international cooperation and ensure cross-border data security.
9. **Encourage Ethical AI Development:** Incorporate ethics-by-design frameworks into AI development processes. Developers should be encouraged to perform fairness tests and actively seek to mitigate biases in AI systems.
10. **Build Data Infrastructure:** Invest in secure and scalable data infrastructure to support compliance with localization and storage requirements while fostering innovation**.**
11. **Continuous Monitoring and Feedback:** Establish a feedback loop between developers, users, and regulators to ensure that laws and guidelines evolve alongside advancements in AI technologies.

VII. CONCLUSION

The legal obligations of AI developers under Indian privacy laws are evolving, reflecting the

complexities of the digital age. While existing frameworks provide a foundation, significant gaps remain in addressing the unique challenges posed by AI systems.

For India to position itself as a global leader in AI innovation, a balanced approach to regulation is crucial—one that supports technological advancement while safeguarding individual privacy rights. Comprehensive legal frameworks should integrate the nuances of AI systems, fostering accountability, transparency, and ethical practices. This will not only ensure compliance but also build trust among users and stakeholders, reinforcing confidence in AI technologies.

Moreover, AI developers must proactively adopt global best practices and ethical guidelines, recognizing that compliance goes beyond mere legal obligations. The focus should be on creating AI systems that respect privacy, promote fairness, and uphold societal values. Collaboration between regulators, developers, and policymakers is essential to establish an ecosystem that bridges the gap between innovation and privacy. Ultimately, a robust regulatory framework, combined with ethical AI practices, can pave the way for sustainable and responsible AI growth in India and beyond.

*****

 [ISSN 2581-5369]