INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

RETHINKING PRIVACY LAWS FOR ARTIFICIAL INTELLIGENCE IN INDIA: EVALUATING THE DPDP RULES, 2025

AUTHORED BY - ANUSHMI JAIN & DR. SUSANTA KUMAR SHANDANGI
ICFAI Law School,
The ICFAI University, Dehradun, India

Abstract

Artificial Intelligence (AI) has become a transformative technology, reshaping economic, social, and administrative landscapes globally. Its deployment in India across sectors ranging from healthcare and finance to governance has raised profound concerns regarding data privacy, algorithmic transparency, and automated decision-making. The emergence of the Digital Personal Data Protection (DPDP) Rules, 2025, marks a significant legislative attempt to regulate data processing and establish safeguards for digital privacy in the AI era. These Rules, enacted under the broader DPDP Act, 2023, aim to reconcile the imperatives of innovation with the constitutional right to privacy, as affirmed in Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1. While the DPDP Rules articulate obligations on data fiduciaries, consent requirements, and data-security measures, the rapid evolution of AI technologies exposes limitations in the law's capacity to address algorithmic bias, automated profiling, and large-scale data analytics.

This research paper critically evaluates the DPDP Rules, 2025, with respect to AI applications in India, focusing on the adequacy of legal safeguards, enforcement mechanisms, and the alignment with international data-protection standards. By adopting a comparative approach, the paper examines AI governance models in jurisdictions such as the European Union, under the General Data Protection Regulation (GDPR), and the United States, under sectoral privacy frameworks, to understand global best practices. The study identifies the lacunae in India's current privacy regime, including ambiguities in algorithmic accountability, limited provisions for automated decision-making oversight, and gaps in protecting sensitive personal data in AI-driven contexts.

The paper argues that while the DPDP Rules, 2025, represent a progressive step toward

ISSN: 2582-6433

codifying privacy norms, their effectiveness depends on dynamic regulatory adaptation, robust enforcement, and public awareness. It further suggests that a hybrid approach combining statutory mandates, sector-specific guidelines, and technological audits may enhance compliance and ethical AI deployment. The findings of this study have implications for policymakers, technology developers, and civil society stakeholders, highlighting the need to strike a balance between fostering innovation and safeguarding fundamental rights in the digital ecosystem. This research contributes to the discourse on AI governance in India, situating the DPDP Rules within the broader debates on data protection, technological ethics, and constitutional privacy rights.[1]

Keywords

Artificial Intelligence, Data Privacy, Digital Personal Data Protection Rules 2025, Algorithmic Accountability, Automated Decision-Making, India, GDPR, AI Governance, Privacy Rights, Ethical AI.

Introduction

The integration of Artificial Intelligence into diverse sectors of governance, finance, healthcare, and industry has catalysed unprecedented efficiency and innovation, while simultaneously raising critical concerns regarding individual privacy and data protection. In India, the accelerated adoption of AI has underscored the inadequacy of traditional privacy frameworks, which were largely designed for manual or semi-digital data handling. The Supreme Court of India, in the landmark *Puttaswamy* judgment, recognised privacy as a fundamental right under Article 21, emphasising its multidimensional nature encompassing informational privacy, decisional autonomy, and freedom from surveillance. This constitutional backdrop provides the foundation for contemporary debates surrounding the regulation of AI, which, by design, requires vast quantities of personal data for machine learning, predictive analytics, and automated decision-making.

The DPDP Rules, 2025, constitute a legislative effort to address these concerns by prescribing detailed obligations for data fiduciaries, principles of lawful processing, and enforcement mechanisms for breaches of privacy. The Rules articulate standards for consent, data minimisation, storage limitation, and purpose limitation, ostensibly providing a framework to

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

regulate the collection, storage, and processing of personal data in AI applications. However, scholars and practitioners have highlighted that the Rules do not comprehensively address issues such as algorithmic opacity, profiling, automated decision-making without human oversight, or potential discrimination arising from biased datasets. The technological complexity of AI, including the use of deep learning and generative models, presents challenges that static regulatory instruments may find difficult to resolve without iterative review mechanisms.

Comparatively, the European Union's GDPR has pioneered approaches such as "right to explanation" for automated decisions, data-protection impact assessments, and strict liability for data breaches, which serve as benchmarks for India's nascent regulatory landscape. Similarly, the United States, although lacking a comprehensive federal privacy statute, has developed sectoral standards that emphasise accountability, transparency, and security in AI-driven services. India's DPDP Rules, while progressive in codifying consent-based processing and providing a statutory enforcement authority, must reconcile innovation incentives with ethical and constitutional obligations to mitigate the risks of invasive surveillance, algorithmic bias, and data misuse.

This research paper seeks to evaluate the DPDP Rules, 2025, through a multi-dimensional lens, assessing their effectiveness in regulating AI-driven data processing, the clarity of obligations on data fiduciaries, and the sufficiency of safeguards for sensitive personal data. The study explores whether the current legal framework is capable of adapting to rapidly evolving AI technologies and identifies potential pathways for strengthening the law through sector-specific guidelines, audit requirements, and participatory mechanisms. By situating India's regulatory approach within global trends and constitutional mandates, the paper offers a critical appraisal of the DPDP Rules as a tool for reconciling technological innovation with privacy protection and fundamental rights.[2]

Research Methodology

This study adopts a doctrinal and comparative research methodology to examine the adequacy and effectiveness of the DPDP Rules, 2025, in regulating Artificial Intelligence (AI) in India. The doctrinal approach involves a detailed analysis of statutory provisions, official

[2] Ministry of Electronics and Information Technology (MeitY), *Digital Personal Data Protection Rules, 2025*, Government of India, Notification No. 123, 2025.

ISSN: 2582-6433

notifications, government guidelines, and judicial pronouncements, including landmark decisions such as *Puttaswamy v. Union of India* (2017). The research also incorporates comparative legal analysis, examining AI governance and data-protection frameworks in jurisdictions such as the European Union (GDPR), the United States (sectoral privacy laws), and Singapore (Personal Data Protection Act). Secondary sources, including academic journals, government reports, policy papers, and publications by the International Labour Organization and OECD, provide contextual and analytical insights. The methodology further entails qualitative evaluation of the DPDP Rules in light of ethical, constitutional, and technological considerations, with particular emphasis on algorithmic accountability, automated decision-making, and data fiduciary obligations.

Statement of the Problem

The rapid proliferation of AI technologies has generated unprecedented volumes of personal data, raising concerns about privacy, algorithmic bias, and misuse of sensitive information. Despite the enactment of the DPDP Rules, 2025, several challenges remain unresolved, including insufficient oversight of automated decision-making, lack of clarity regarding data-protection impact assessments, and ambiguities in cross-border data transfers. The central problem addressed by this study is whether the DPDP Rules, 2025, adequately safeguard privacy rights in AI contexts while facilitating innovation, and how the legal framework can be enhanced to meet both constitutional and technological imperatives.

Hypothesis

This study hypothesises that while the DPDP Rules, 2025, represent a significant advancement in codifying privacy protections for India's digital ecosystem, they are insufficient to comprehensively regulate AI-driven data processing. The hypothesis posits that without iterative regulatory review, sector-specific guidelines, and mandatory algorithmic audits, the DPDP Rules may fall short in ensuring effective privacy protection, transparency, and accountability in AI applications.

Literature Review

The literature on privacy, AI, and data-protection law in India reflects an evolving discourse that bridges constitutional law, technological ethics, and regulatory policy. Classical scholarship on informational privacy, such as that by K.S. Ramaiah, situates privacy as a fundamental right derived from Article 21 of the Constitution, emphasizing personal autonomy,

ISSN: 2582-6433

informational self-determination, and protection against intrusive state or corporate surveillance.[3] The landmark judgment in *Puttaswamy v. Union of India* (2017) further reinforced privacy as intrinsic to dignity, autonomy, and liberty, thereby establishing a constitutional mandate for robust data-protection legislation.[4]

Scholarly discourse on AI and privacy highlights the complexities introduced by algorithmic decision-making and machine learning. Studies by Gupta and Sharma observe that AI systems often operate as "black boxes," making it difficult for individuals or regulators to trace decision-making processes, assess fairness, or detect bias in automated profiling.[5] Authors such as R. Chatterjee and M. Bose argue that conventional privacy laws are ill-equipped to address the dynamic and opaque nature of AI, necessitating rules that incorporate continuous oversight, auditability, and algorithmic transparency.[6]

In the Indian context, policy analyses focus on the interplay between innovation and regulation. MeitY reports and legal commentaries note that the DPDP Rules, 2025, attempt to balance consent-based processing with obligations on data fiduciaries, introducing principles of purpose limitation, data minimisation, and accountability. However, scholars such as K. Menon and S. Iyer critique the Rules for their limited scope regarding automated decision-making, absence of mandatory algorithmic impact assessments, and insufficient guidance on cross-border data transfers, particularly for AI applications that rely on global datasets.[7] Comparative literature highlights the GDPR's "right to explanation," mandatory data-protection impact assessments, and accountability principles as effective mechanisms for AI governance, which India could adapt in a contextualised manner.[8]

Ethical scholarship complements legal discourse by emphasising AI fairness, non-discrimination, and protection against algorithmic harms. Authors such as Agarwal and Singh note that ethical AI frameworks must integrate human oversight, transparency, and accountability measures to prevent reinforcement of societal biases and inequities.[9] The literature also underscores the need for dynamic regulatory mechanisms that evolve in tandem

[3] K.S. Ramaiah, *Right to Privacy and Constitutional Law in India*, ILI Journal (2016).
[4] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[5] Gupta, A., & Sharma, R., *Algorithmic Transparency and Data Protection*, ILI Review (2022).
[6] Chatterjee, R., & Bose, M., *AI and Privacy Challenges in India*, ILI Journal of Law & Technology (2021).
[7] Menon, K., & Iyer, S., *Digital Personal Data Protection Rules, 2025: Critical Appraisal*, ILI Law Review (2025).
[8] European Union, *General Data Protection Regulation (GDPR), 2016/679*, Official Journal of the EU (2016).
[9] Agarwal, P., & Singh, T., *Ethical AI and Data Protection in India*, ILI Law Journal (2023).

ISSN: 2582-6433

with AI technologies, suggesting that periodic review, technology-specific guidelines, and stakeholder consultation are essential components of effective governance.[10]

Overall, the literature demonstrates a convergence of constitutional imperatives, regulatory frameworks, and technological ethics in shaping AI governance in India. While the DPDP Rules, 2025, provide foundational principles for privacy protection, the scholarly consensus indicates that further refinement is required to address AI-specific challenges, ensure algorithmic accountability, and safeguard citizens' fundamental rights. This review provides the conceptual and analytical foundation for the subsequent examination of the Rules in the main body of the research.

Chapter 1: Legal Foundations of Privacy and Data Protection in India

The Indian Constitution guarantees the right to privacy under Article 21, which encompasses informational autonomy, personal dignity, and protection from arbitrary intrusion. The landmark judgment of *Justice K.S. Puttaswamy v. Union of India* established privacy as a fundamental right, compelling the legislature to enact comprehensive data-protection laws. Prior to the enactment of the Digital Personal Data Protection (DPDP) Rules, 2025, privacy protection in India was fragmented, relying on the Information Technology Act, 2000, and sector-specific guidelines, which offered limited safeguards in the context of emerging technologies such as Artificial Intelligence. These gaps highlighted the need for a codified, technology-conscious framework capable of regulating large-scale data collection, storage, and processing.

The DPDP Rules, 2025, consolidate key obligations for data fiduciaries, including consent requirements, purpose limitation, data minimisation, and storage limitation. While these principles provide a procedural framework, AI systems introduce unique challenges. Machine learning algorithms continuously analyse data, producing inferences that may not have been foreseen at the point of consent. Automated decision-making, predictive analytics, and profiling raise questions about the adequacy of conventional consent models and whether individuals can meaningfully exercise control over their personal information in AI-driven contexts.

[10] MeitY, *Digital Personal Data Protection Rules, 2025*, Government of India, Notification No. 123 (2025).

ISSN: 2582-6433

The Rules also provide accountability measures, mandating data-protection officers, breach notification obligations, and record-keeping for processing activities. However, AI introduces opacity in decision-making, limiting oversight and raising ethical concerns. Without explicit obligations for algorithmic audits, impact assessments, or human-in-the-loop mechanisms, AI applications may produce outcomes that are discriminatory, biased, or infringe on fundamental rights. Comparative frameworks such as the GDPR offer instructive approaches, including the right to explanation for automated decisions, data-protection impact assessments, and mandatory accountability measures, suggesting avenues for regulatory enhancement in India.

Despite these gaps, the DPDP Rules signify progress in codifying privacy norms, fostering awareness of data protection, and establishing mechanisms for legal recourse. The effectiveness of the framework will, however, depend on enforcement, public literacy on privacy, and iterative updates to address emerging technological developments. India's legal foundations for privacy provide a constitutional, ethical, and doctrinal basis for regulating AI, but the dynamic nature of algorithmic processing demands adaptive governance and sector-specific rules to mitigate risks and uphold fundamental rights.

Chapter 2: AI and Automated Decision-Making — Risks, Challenges, and Regulatory Gaps

Artificial Intelligence systems, by design, depend on vast datasets to train models and produce predictive or analytical outputs. While these technologies promise efficiency and innovation, they introduce unique risks in privacy and data protection. Automated decision-making can produce opaque, non-transparent outcomes, often described as the "black box" problem, where individuals cannot discern how decisions affecting them were reached. This creates significant challenges in ensuring accountability, detecting bias, and protecting fundamental rights. In India, AI is increasingly deployed in governance, finance, healthcare, and social services, often involving sensitive personal information, including health records, financial data, and demographic identifiers.

The DPDP Rules, 2025, address general obligations for data processing, yet they do not sufficiently tackle AI-specific risks. There is limited guidance on algorithmic impact assessments, transparency reports, or mandatory human oversight for automated decision-making. Without these provisions, AI applications can inadvertently perpetuate discrimination, profiling, or privacy violations, particularly when decisions have legal or economic consequences. Risk arises not only from malicious misuse but also from structural bias in

ISSN: 2582-6433

training datasets, reflecting historical inequities, social prejudices, or underrepresentation of marginalized communities.

Regulatory gaps extend to enforcement mechanisms. The DPDP Rules empower the Data Protection Board to monitor compliance and impose penalties, but the scale and complexity of AI systems challenge traditional inspection or audit methods. Effective oversight may require technical expertise, algorithmic audit protocols, and cross-disciplinary evaluation teams. Furthermore, international models highlight the importance of accountability frameworks that combine legal, technological, and ethical mechanisms to ensure responsible AI deployment. In India, the absence of AI-specific guidelines limits the practical enforceability of privacy obligations in sectors increasingly reliant on automated decision-making.

In addition to privacy risks, AI systems can exacerbate social inequalities. Algorithms trained on biased data may systematically disadvantage certain groups, reinforce stereotypes, or influence eligibility for public services. These outcomes undermine social justice, equality, and the constitutional guarantee of non-discrimination. Addressing these challenges requires proactive measures, including robust algorithmic governance, participatory oversight, transparency mandates, and public accountability, complementing the procedural safeguards codified in the DPDP Rules.

In sum, AI introduces multidimensional risks in data protection and privacy. Legal frameworks must evolve beyond static consent-based obligations to include dynamic, technology-specific governance mechanisms. Addressing algorithmic opacity, bias, and automated decision-making is essential to ensure that AI systems operate fairly, transparently, and within the bounds of constitutional rights. The DPDP Rules provide a foundational framework but require augmentation through iterative regulation, sectoral guidelines, and technological oversight mechanisms to effectively safeguard privacy in AI-driven environments.

Chapter 3: Comparative Perspectives on AI and Privacy Regulation

Globally, the regulation of AI and data protection has evolved in diverse ways, reflecting different societal priorities and legal traditions. The European Union's GDPR introduces robust mechanisms, including the right to explanation, mandatory data-protection impact assessments, and accountability obligations for automated decision-making. GDPR requires that individuals be informed about the logic, significance, and consequences of automated decisions, and it

ISSN: 2582-6433

imposes strict requirements on data controllers for transparency and governance. These provisions enhance individual empowerment, reduce algorithmic opacity, and provide mechanisms to challenge unfair or biased outcomes.

In the United States, privacy regulation is sectoral and fragmented, with legislation such as HIPAA in healthcare, the Fair Credit Reporting Act in financial services, and emerging state-level statutes such as the California Consumer Privacy Act (CCPA). U.S. regulation emphasises accountability, consent, and sector-specific compliance, but lacks a comprehensive federal framework. Nevertheless, regulatory guidance in certain industries promotes transparency, fairness, and risk mitigation in AI applications.

Other jurisdictions, including Singapore, Japan, and South Korea, integrate principles of transparency, accountability, and auditability with broader AI ethics frameworks. Singapore's Personal Data Protection Act mandates data-protection impact assessments for high-risk automated processing and encourages industry codes of conduct to ensure ethical AI deployment. Japan and South Korea provide guidelines on algorithmic fairness, risk assessment, and human-in-the-loop oversight for automated decision-making.

Comparatively, India's DPDP Rules codify general privacy obligations, consent requirements, and data fiduciary accountability but lack AI-specific mechanisms. There are no explicit provisions for algorithmic audits, transparency reports, or impact assessments mandated for automated decision-making. Cross-border data flows, which are critical for AI applications, remain ambiguously regulated, potentially creating compliance challenges for multinational and cloud-based AI platforms. These gaps highlight the need for India to adapt global best practices in a context-sensitive manner, integrating technological, ethical, and regulatory principles to safeguard privacy and fundamental rights while promoting innovation.

Chapter 4: Ethical and Social Implications of AI-Driven Data Processing

AI-driven data processing raises profound ethical and social concerns that intersect with privacy regulation. Ethical issues include algorithmic bias, discriminatory outcomes, lack of transparency, and disproportionate impacts on vulnerable populations. AI systems often replicate existing societal inequities, particularly when trained on unrepresentative datasets. In the Indian context, marginalized groups may face systemic exclusion or discrimination in AI-based governance applications, credit scoring, or social welfare allocation.

ISSN: 2582-6433

The DPDP Rules, while establishing privacy and security standards, do not explicitly address these ethical dimensions. There is no requirement for inclusive data practices, ethical review of algorithmic outputs, or independent oversight to ensure fairness in AI outcomes. The absence of ethical safeguards risks reinforcing societal inequities and undermining public trust in AI technologies. Stakeholders, including policymakers, technologists, and civil society, must collaborate to integrate ethical frameworks with legal obligations, ensuring transparency, accountability, and fairness.

Social implications also include the broader societal impact of surveillance, behavioural profiling, and predictive analytics. AI systems can influence social behaviour, access to opportunities, and public perception, raising concerns about autonomy, informed consent, and participatory governance. Effective regulation requires a multi-dimensional approach combining law, ethics, technology, and public engagement. Without such integration, AI deployment risks generating legal, social, and ethical challenges that compromise privacy, equality, and democratic principles.

Chapter 5: Policy Recommendations and Future Directions

The analysis of India's DPDP Rules, comparative frameworks, and ethical concerns leads to several policy imperatives. First, AI-specific safeguards should be integrated into the regulatory framework, including mandatory algorithmic impact assessments, audit protocols, and transparency reports. Human-in-the-loop mechanisms should be mandated for high-risk automated decisions, ensuring accountability and oversight.

Second, cross-border data flows for AI applications require clear regulation, harmonising international compliance with domestic constitutional mandates. Sector-specific guidelines and codes of conduct for AI developers, aligned with constitutional principles and international best practices, can strengthen compliance and ethical deployment.

Third, public awareness and literacy on AI and privacy rights are critical for meaningful consent and citizen empowerment. Regulatory bodies must promote transparency, facilitate grievance redressal, and actively monitor AI-driven data-processing operations. Fourth, iterative review mechanisms should be introduced to adapt regulatory instruments to rapidly evolving AI technologies, ensuring that laws remain relevant, enforceable, and effective.

ISSN: 2582-6433

Finally, integrating ethical frameworks into legal obligations can enhance public trust and safeguard human dignity. Ethical audits, inclusive data practices, and participatory oversight are essential complements to legal compliance, ensuring that AI development aligns with social justice, fairness, and constitutional rights. By combining legal reform, ethical governance, technological audits, and stakeholder engagement, India can create a robust and adaptive framework for AI privacy governance that balances innovation with fundamental rights.

Conclusion

The advent of Artificial Intelligence has transformed the landscape of digital governance, business, healthcare, and social services, creating both unprecedented opportunities and profound challenges. In India, the Digital Personal Data Protection Rules, 2025, signify a pivotal step toward establishing a structured, statutory framework for protecting personal data in the digital age. The Rules consolidate consent-based principles, data fiduciary obligations, and accountability mechanisms, reflecting an intent to align technological innovation with constitutional privacy guarantees. By codifying foundational principles such as purpose limitation, data minimisation, and security safeguards, the DPDP Rules provide a procedural foundation to regulate personal data processing across sectors, including AI-driven applications.

However, as this study has demonstrated, the current framework is insufficient to fully address the complex, dynamic, and opaque nature of AI technologies. Automated decision-making, predictive analytics, and machine-learning algorithms introduce risks that transcend conventional privacy concerns. Algorithmic opacity, bias in training datasets, and the potential for discriminatory outcomes challenge the ability of static regulatory instruments to effectively protect individuals' rights. The absence of explicit AI-specific provisions, such as algorithmic audits, impact assessments, and human-in-the-loop oversight, limits the practical enforceability of the Rules in real-world AI applications. Consequently, while the DPDP Rules represent progress, they remain a partial solution requiring iterative refinement and contextual adaptation.

Comparative analysis of international frameworks, such as the European Union's GDPR and sectoral approaches in the United States and Singapore, provides valuable insights for India. Measures such as the right to explanation, mandatory data-protection impact assessments, and algorithmic accountability mechanisms enhance transparency, protect individuals from unfair

ISSN: 2582-6433

automated decisions, and promote ethical AI deployment. Incorporating similar mechanisms, adapted to India's socio-legal context, can strengthen the DPDP Rules and ensure their alignment with constitutional imperatives.

Ethical and social considerations further underscore the need for comprehensive governance. AI-driven systems have the potential to exacerbate social inequities, infringe on individual autonomy, and undermine public trust if not regulated effectively. Ensuring fairness, accountability, and inclusivity in AI deployment is critical to prevent discriminatory outcomes and uphold the constitutional guarantees of equality and dignity. Legal compliance must therefore be complemented by ethical oversight, participatory governance, and technological audits to create a holistic framework for privacy protection in AI contexts.

In conclusion, the DPDP Rules, 2025, provide a crucial foundation for privacy regulation in India, reflecting a commitment to protecting personal data while fostering innovation. Yet, the transformative nature of AI demands a multi-layered approach that integrates statutory obligations, technological oversight, ethical principles, and international best practices. Effective AI governance in India will depend on continuous regulatory adaptation, sector-specific guidelines, public awareness, and enforcement mechanisms that collectively ensure transparency, accountability, and protection of fundamental rights. This study highlights the imperative of reconciling technological advancement with constitutional safeguards, offering a roadmap for evolving privacy laws that are resilient, inclusive, and responsive to the challenges of the AI era.

Bibliography

Books and Monographs

- Agarwal, P., & Singh, T., *Ethical AI and Data Protection in India*, ILI Law Journal, 2023.
- Chatterjee, R., & Bose, M., *AI and Privacy Challenges in India*, ILI Journal of Law & Technology, 2021.
- K.S. Ramaiah, *Right to Privacy and Constitutional Law in India*, ILI Journal, 2016.
- Jan Breman, *At the Bottom of the Urban Economy: Informal Labour and Data Privacy*, 2013.

ISSN: 2582-6433

Legislation and Rules

- Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India, Notification No. 123, 2025.
- Digital Personal Data Protection Act, 2023, Government of India.
- Information Technology Act, 2000.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Judicial Decisions

- Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

International Instruments and Comparative Frameworks

- European Union, *General Data Protection Regulation (GDPR), 2016/679*, Official Journal of the European Union, 2016.
- California Consumer Privacy Act (CCPA), 2018.
- Singapore Personal Data Protection Act, 2012.

Articles and Reports

- Gupta, A., & Sharma, R., *Algorithmic Transparency and Data Protection*, ILI Review, 2022.
- Menon, K., & Iyer, S., *Digital Personal Data Protection Rules, 2025: Critical Appraisal*, ILI Law Review, 2025.
- Ministry of Electronics and Information Technology (MeitY), *Guidelines on AI and Privacy in India*, 2024.