Journal of Trends and Challenges in Artificial Intelligence

ASPUR PUBLISHING

Vol. 03, No. 02 (2026) 75-84, DOI: 10.61552/JAI.2026.02.002 - http://jai.aspur.rs

PRIVACY AND DATA PROTECTION IN AI-DRIVEN LEGAL SERVICES: AN ANALYSIS OF INDIA'S EMERGING CHALLENGES AND SOLUTIONS

Manindra Singh Hanspal[1]
Bijayananda Behera

Received 28.04.2025.
Revised 25.06.2025.
Accepted 02.07.2025.

Keywords:

Privacy, Data Protection, Artificial Intelligence, Legal Services, India.

Original research

A B S T R A C T

The rapid integration of artificial intelligence (AI) into India's legal sector introduces unprecedented efficiencies, transforming functions such as legal research, predictive analytics, and contract management. However, this integration also presents significant privacy and data protection challenges, especially in India's absence of AI-specific regulations. In contrast, the European Union's Artificial Intelligence Act (AIA) provides a comprehensive framework that establishes stringent privacy, transparency, and accountability standards in AI applications, particularly in high-stakes fields such as law. This paper examines the privacy and ethical risks associated with AI in India's legal services, assesses the gaps in India's regulatory framework compared to the EU's approach, and offers actionable recommendations for implementing AI responsibly within India's legal context. Through a thematic analysis of ethical, technical, and legal concerns, as well as real-world case examples, this paper advocates for an Indian regulatory framework that safeguards privacy, ensures accountability and maintains public trust in AI-augmented legal services. The findings underscore the urgent need for AI-specific guidelines to align with international standards and address the complex privacy challenges posed by AI in the Indian legal sector.

1. INTRODUCTION

Artificial intelligence (AI) is revolutionizing various industries worldwide, offering efficiency, accuracy, and speed advancements. In the legal sector, AI transforms tasks that human professionals traditionally perform, including legal research, case analysis, predictive analytics, and document review (Atrey, 2023). These AI-driven tools are particularly appealing in jurisdictions like India, where the legal system faces substantial challenges due to high caseloads, resource constraints, and a long-standing backlog of cases. By automating routine tasks and providing predictive insights, AI can streamline legal services, improving accessibility and making legal processes faster and more cost-effective for practitioners and clients (Priya, 2025). However, the growing reliance on AI in legal services raises significant concerns about privacy, data protection, and ethics (Renuka et al., 2025). AI models used in legal applications often require access to sensitive personal data, including client information, case histories, and confidential legal communications (Cook & Heinrich

[1] Corresponding author: Manindra Singh Hanspal
Email: mhanspal21@gmail.com

2023). This data could expose clients and legal professionals to unauthorized data access, breaches, and biases embedded within AI algorithms (Banshal, 2025). Moreover, many AI systems function as "black boxes," where the decision-making processes are not easily interpretable, posing risks to accountability and transparency, values fundamental to the legal system (Chaudhary, 2024). In response to these challenges, regulatory frameworks are emerging worldwide to govern the development and deployment of AI systems. The European Union, for instance, has introduced the Artificial Intelligence Act (AIA). This regulatory framework categorizes AI applications by risk level and imposes strict requirements for high-risk applications, including those used in legal and judicial contexts. The AIA mandates compliance with privacy, transparency, and accountability standards to safeguard individuals' rights when interacting with AI technologies (Micklitz & Sartor, 2025). In contrast, India lacks a comprehensive regulatory framework that addresses AI's unique privacy and data protection challenges, instead relying on general data protection laws, such as the Digital Personal Data Protection Act (DPDPA) of 2023 (Sundara & Narendran, 2023).

1.1 Rapid AI Adoption and Technological Advancements in India

As the world's second-most populous country and a rapidly developing nation, India has adopted technological advancements at an unprecedented pace. India is home to one of the largest mobile-using populations, with over a billion mobile users and an expanding digital ecosystem that fosters accessibility to technology (Digital Transformation in India, 2024). The introduction of artificial intelligence (AI) has further accelerated this transformation, as people increasingly rely on AI-powered tools for efficiency, convenience, and innovation across various fields (Dandotiya et al., 2024).

In recent years, AI applications have found diverse uses across sectors in India:

- ***Cinematography:*** AI enhances visual effects, editing processes, and audience analytics in the Indian film industry (Khan et al., 2025).
- ***Medical Field and Robotics:*** AI is used for diagnostics, predictive analytics, robotic surgeries, and patient management, contributing to advancements in healthcare (Zeb et al., 2024).
- ***Education:*** AI-driven platforms support personalized learning, student assessments, and educational management (Yekollu et al., 2024).
- ***Legal Sector:*** AI is revolutionizing case research, contract analysis, predictive analytics, and case management, offering faster, data-driven decision-making tools for legal professionals (Negi Advocate, 2023).

The scope and implementation of AI in India's legal field are particularly noteworthy. Legal professionals utilize AI for tasks such as document review, legal research, and predicting case outcomes, while judicial bodies explore AI for case management and workflow optimization (Kluttz & Mulligan, 2019). Given India's high caseload and backlogs, AI offers promising solutions to streamline judicial processes (Rafiq, 2024). Still, its adoption raises questions about privacy, bias, and accountability, especially in high-stakes environments.

1.2 Privacy and Data Protection in AI-Driven Legal Services: A Global and Indian Perspective

AI-driven applications in legal services present a double-edged sword (Singla et al., 2024). While they promise increased efficiency and can reduce manual labour, they also introduce risks to privacy and data protection. Internationally, the European Union has led by establishing specific privacy protections for high-stakes AI applications through the AIA (Hacker & Passoth 2020). This regulation not only mandates transparency and accountability but also introduces measures to prevent algorithmic bias and safeguard individual privacy. AI systems in high-risk sectors must meet strict data transparency, fairness, and explainability criteria, ensuring that automated decisions can be traced and justified (Hamon et al., 2022). India, however, has yet to implement a comparable regulatory framework specific to AI. While the DPDPA 2023 provides a foundational basis for data protection, it does not address AI's intricacies, such as algorithmic transparency, bias mitigation, or accountability for automated decision-making (Bhattacharjee. 2024). This regulatory gap presents challenges for Indian legal services, as AI algorithms often process sensitive data, raising concerns about privacy, security, and fairness. AI systems have the potential to inadvertently reinforce biases in historical data, leading to discriminatory outcomes, especially in India's socio-culturally diverse landscape (Thakkar, 2024).

1.3 Purpose and Scope

This paper examines the privacy and data protection challenges in AI-driven legal services within India's distinct legal and regulatory framework. By reviewing the privacy risks posed by AI in legal services, assessing the adequacy of India's current regulatory framework, and comparing it with the EU's more stringent AIA, this research seeks to provide actionable insights. Through case examples and an analysis of ethical and technical challenges, the study highlights the importance of AI-specific regulations in upholding privacy and moral standards within India's legal sector.

2. ETHICAL AND TECHNICAL CHALLENGES OF AI IN JUDICIAL PROCESSES

As artificial intelligence becomes increasingly integrated into legal systems, it brings a range of ethical and technical challenges that demand close examination. One particularly controversial issue is whether AI can or should replace human judges.

2.1 The Debate on AI Replacing Judges

The potential for AI to replace human judges in judicial decision-making has sparked considerable debate (Morison & Harkens, 2019). Proponents argue that AI could bring greater consistency and efficiency to the judiciary by automating routine analyses, identifying case patterns, and processing vast amounts of data faster than human judges. AI could theoretically reduce human biases, provide impartial decisions, and address the judicial backlog, a persistent issue in India's legal system where millions of cases remain unresolved for years (Sharma, 2023). However, the counterargument emphasizes the irreplaceable qualities of human judgment. Judicial decisions often require understanding nuanced ethical considerations, empathy, and context, particularly in cases where moral judgment and societal values play a central role (Stępień, 2025). Unlike human judges, AI lacks these cognitive and emotional abilities, making it challenging to apply AI to complex legal issues involving human rights, justice, and fairness (Xu, 2022). This limitation highlights the need for AI to support, rather than replace, judges, assisting with data analysis and procedural tasks while leaving critical judgment and ethical decisions to human professionals (Ejjami, 2024). The European Union's Artificial Intelligence Act (AIA) categorizes AI in judicial applications as "high risk," mandating rigorous standards to ensure AI remains a supportive tool rather than a replacement for human oversight. India, however, lacks AI-specific guidelines on the judiciary's use of AI, raising concerns that unchecked AI usage could compromise justice by prioritizing efficiency over ethics and fairness (Thakur & Kumar, 2024).

2.2 Technical Limitations of AI Algorithms in Legal Contexts

The technical challenges of AI systems—especially in high-stakes environments like the judiciary—include issues with transparency, interpretability, and accuracy. Many AI algorithms, particularly those based on deep learning, operate as "black boxes," meaning their internal decision-making processes are complex and often difficult to understand (Brożek et al., 2024). This lack of interpretability poses a significant issue in judicial settings, where transparency and accountability are paramount. Legal stakeholders, including judges, lawyers, and clients, need to understand how an AI system arrived at a particular decision, significantly if that decision could influence a case outcome (Remus & Levy, 2017).

Another critical technical limitation is the issue of false positives and false negatives, which can have severe consequences in legal proceedings.

- ***False Positives:*** In predictive analytics used for bail decisions, a false positive could result in the erroneous classification of a low-risk individual as high-risk, leading to unjustified detention (Elyounes, 2019).
- ***False Negatives:*** Conversely, a false negative could lead to underestimating the risk posed by an individual, potentially endangering public safety or undermining judicial fairness (Findley, 2017).

False positives and negatives often stem from biases in training data, which may reflect historical inequalities. When AI models are trained on biased or incomplete data, they risk reinforcing these biases, disproportionately affecting marginalized groups. The use of AI in legal systems is particularly problematic in India, where the legal system is embedded in a complex socio-cultural landscape, and even subtle biases in AI could lead to significant injustice for specific communities (Das et al., 2024). Addressing these technical challenges requires rigorous model validation, regular bias audits, and clear explanations for AI-generated decisions. Without these measures, the use of AI in judicial contexts risks perpetuating existing biases and inaccuracies rather than alleviating them, thereby undermining public trust in AI's role within the legal system.

3. PRIVACY CHALLENGES IN AI-DRIVEN LEGAL SERVICES IN INDIA

The deployment of artificial intelligence within India's legal system has prompted serious concerns about the privacy of personal and sensitive data. Before addressing these privacy implications, it is important to understand the nature and scope of AI applications currently being introduced in the Indian judiciary.

3.1 AI Initiatives in the Indian Judiciary

The Indian judiciary has begun leveraging artificial intelligence (AI) to streamline processes, improve accessibility, and enhance the efficiency of legal proceedings (Rajendran et al., 2025). Notable AI applications include:

- ***Translation:*** The Supreme Court utilizes AI to translate judicial documents and orders into vernacular languages, including Hindi, Tamil, Punjabi, Marathi, Malayalam, Bangla, Telugu, Kannada, Nepali, and Urdu. This initiative improves citizens' accessibility by providing essential legal documents in their native languages (Press Information Bureau, 2024).
- ***Legal Research:*** AI tools enhance the efficiency and depth of legal research, enabling quicker and more accurate case law analysis (Nithya et al., 2024).
- ***Process Automation:*** Multiple processes within the Supreme Court of India are now automated using AI, reducing manual workloads and minimizing human error (Prabhavathi & Durai, (2024).
- ***Oral Argument Transcription:*** AI-based transcription tools automatically transcribe oral arguments for Constitution Bench matters,

preserving accurate records and facilitating future references (Nithya et al., 2024).

- **Case Law and Precedent Support**: The Supreme Court Portal for Assistance in Court Efficiency (SUPACE) aids judges by providing relevant case laws and precedents. This tool enables judges to access authoritative references quickly, improving their decision-making accuracy (INDIAI, 2021).
- ***Automated Filing:*** Nyaay AI, developed by Indika AI, automates filing by extracting data directly from case documents, streamlining document processing and saving time (Nigam et al., 2025).
- ***Defect Detection in Filings:*** AI also detects filing defects, reducing delays caused by incomplete or incorrect documentation.
- ***Case Triaging and Bunching:*** AI algorithms triage and categorize cases based on urgency, ensuring that critical matters are addressed promptly.
- **Judgment Research:** AI supports judgment research, enabling judges to review previous judgments and inform their decisions (Mohod et al., 2025).

These initiatives represent significant advancements in the Indian judiciary's operations, and some argue that AI can enhance the fairness of judgments by strictly adhering to precedents, minimizing personal biases, and efficiently processing vast amounts of data. However, AI raises significant ethical and privacy concerns, particularly regarding data protection, transparency, and accountability, despite its benefits. Deploying AI in such sensitive domains requires a robust regulatory framework to address these concerns and protect citizens' rights.

3.2 Data Collection and Consent Management

In AI-driven legal services, data collection is fundamental, as AI systems rely on vast datasets to develop predictive models, assess case histories, and automate routine legal tasks. This data often includes sensitive information, such as client identities, case details, financial information, and private communications (Ejjami, 2024). In India, where privacy is recognized as a fundamental right, obtaining informed consent for the use of data is crucial (Taylor & Paterson, 2020). However, AI tools frequently collect and process data at a scale that makes meaningful consent challenging, as clients may not fully understand how their data is being used. Further complicating matters, AI systems typically require continuous data updates to remain accurate and relevant, which can potentially expose personal information to unauthorized access. In sectors such as healthcare and finance, India's Digital Personal Data Protection Act (DPDPA) 2023 mandates obtaining explicit consent before collecting or processing data; however, it does not address the unique consent challenges associated with AI, including the secondary use of data or the repurposing of data for model training. Without specific guidelines, AI-driven legal services in India may inadvertently infringe upon privacy rights, especially if clients know how these systems utilize their data.

4. COMPARATIVE ANALYSIS OF REGULATORY FRAMEWORKS (INDIA VS. EU)

A meaningful comparison of privacy regulation in AI-driven legal systems requires a detailed examination of how India and the European Union approach data protection and AI governance. This section begins with an overview of India’s regulatory landscape, followed by a discussion of the European Union’s framework.

4.1 Overview of India's Regulatory Landscape

India's current regulatory framework for data protection and privacy primarily relies on the Digital Personal Data Protection Act (DPDPA) 2023, which sets the foundational principles for data protection, including requirements for lawful processing, purpose limitation, and data minimization. The DPDPA establishes general data protection standards for all sectors, covering consent, data processing, and breach notification topics. While this provides a basis for protecting personal data, it is not specifically tailored to address the unique risks posed by AI applications, particularly in high-stakes fields like legal services. In the legal services sector, where AI applications handle sensitive client and case information, India's laws lack clear guidance on AI transparency, accountability, bias mitigation, and explainability. The DPDPA also does not mandate rigorous standards for high-risk applications or address the "black box" nature of many AI models, leaving critical gaps in regulating AI tools that impact judicial and legal processes. Without AI-specific standards, India's legal sector has limited regulatory support to address the nuanced privacy and ethical concerns associated with AI in providing legal services.

4.1.1 Brief Overview of Data Privacy Law in India

India's primary data protection framework, the Digital Personal Data Protection Act (DPDPA) 2023, establishes general principles to safeguard individual privacy rights protected under the Indian Constitution following the landmark case. The DPDPA governs the processing of personal data in both public and private sectors, laying out foundational data protection practices such as:

- ***Lawful Processing and Consent:*** Data processing is allowed only with explicit consent, except in specified circumstances.
- ***Data Minimization and Purpose Limitation:*** The personal data collected should be limited to what is necessary for a specific purpose and should not be repurposed without the individual's consent.
- ***User Rights:*** Data subjects have rights over their data, including the right to access, correct, and delete their information.

- ***Data Security and Breach Notification:*** Organizations must implement appropriate security measures and notify relevant authorities when a data breach occurs.

While the DPDPA establishes fundamental data protection standards, it does not explicitly address AI's unique challenges, such as algorithmic transparency, bias mitigation, or accountability in automated decision-making. This lack of AI-specific regulation leaves critical gaps, particularly in sectors such as law, where AI systems often process sensitive data.

4.2 EU Artificial Intelligence Act (AIA) and Its Provisions for Legal AI Applications

The European Union's Artificial Intelligence Act (AIA), adopted in 2024, provides one of the most comprehensive frameworks for governing AI. The AIA categorizes AI applications into risk-based levels: minimal risk, limited risk, high risk, and unacceptable risk. Applications in legal and judicial contexts are classified as high-risk, which imposes strict requirements for transparency, accountability, and risk mitigation. The AIA mandates that high-risk AI systems comply with specific criteria to safeguard individuals' rights.

4.2.1 Overview of the European Union's AI Act

The European Union's Artificial Intelligence Act (AIA), adopted in 2024, is one of the world's most comprehensive frameworks for regulating AI. The AIA categorizes AI systems based on risk levels. It sets strict requirements for high-risk applications, which include AI tools used in sensitive fields like law, healthcare, and public administration (Directorate-General for Communication, 2024). The AIA covers several key aspects:

- ***Risk-Based Categorization:*** AI systems are classified into four risk categories: minimal, limited, high, and unacceptable. High-risk applications, including those in legal and judicial contexts, are subject to stringent requirements (Schuett, 2023).
- ***Transparency and Explainability:*** High-risk AI systems must be transparent, providing users with information on how they work, their limitations, and potential risks. This requirement ensures that individuals affected by AI decisions can understand and contest them (Felzmann et al., 2019).
- ***Bias Mitigation and Fairness:*** Regular bias audits are required for high-risk AI applications to identify and mitigate potential discriminatory outcomes, safeguarding fairness in AI-driven decisions (Bahangulu & Owusu-Berko, 2025).
- ***Accountability Mechanisms:*** The AIA mandates accountability structures, requiring developers and users of high-risk AI systems to document and monitor their AI operations, ensuring ethical and fair outcomes (Micklitz & Sartor, 2025).
- ***Data Protection and Security:*** The AIA aligns with the EU's General Data Protection Regulation (GDPR), imposing strict data protection standards, including encryption, data minimization, and purpose limitation (Shahlaei & Berente, 2024).

By implementing these standards, the AIA aims to balance AI innovation and ethical and privacy protections, promoting trust in AI systems across the EU. India, in contrast, currently lacks a comparable framework that addresses AI-specific risks, particularly for high-stakes applications such as legal and judicial processes.

4.3 Comparative Analysis and Regulatory Gaps

A comparative analysis of the EU's AIA and India's DPDPA reveals several vital gaps in India's regulatory framework concerning AI in legal services:

- ***Lack of AI-Specific Standards:*** Unlike the AIA, India's DPDPA does not differentiate between general data processing and AI-driven applications. The absence of AI-specific guidelines leaves India's legal sector without regulatory tools to manage issues such as AI transparency, accountability, and bias, which are crucial in judicial contexts (Dhir & Verma, 2024).
- ***Transparency and Explainability Gaps:*** The AIA mandates that high-risk AI systems provide transparency and explainability, ensuring users can understand the AI's decision-making process. In India, no equivalent requirement under the DPDPA or any other regulation enforces explainability for AI in legal services. This gap limits the ability of Indian legal professionals and clients to understand or contest AI-generated decisions, potentially compromising accountability in judicial proceedings.
- ***Insufficient Accountability Mechanisms:*** The AIA enforces accountability measures by requiring comprehensive documentation and monitoring of high-risk AI systems. Establishing accountability mechanisms facilitates oversight and allows users to challenge AI-driven decisions. In contrast, India's DPDPA does not include specific accountability provisions for AI applications, meaning that individuals impacted by AI-driven legal decisions in India may have limited recourse to hold AI developers or users accountable.
- ***Privacy and Data Protection Limitations:*** Although the DPDPA establishes general data protection principles, it lacks the nuanced protections necessary for high-risk AI applications in the legal services sector. The AIA mandates data protection measures aligned with GDPR, including encryption, purpose limitation, and regular audits. The absence of similar requirements in India's framework poses risks to

client confidentiality and privacy, especially in legal contexts where data sensitivity is high.

- ***Risk-Based Categorization:*** The AIA's risk-based approach categorizes AI applications by their potential impact on individuals' rights, mandating stricter oversight for high-risk applications. India's DPDPA, however, applies a blanket approach to data protection without distinguishing between different levels of risk associated with AI applications (Naithani 2024).

Table 1: Comparative Analysis of AI Regulatory Approaches: European Union (AIA) vs. India (DPDPA)

Regulatory Aspect	European Union (AIA)	India (DPDPA)	Gap
AI-Specific Standards	Differentiated by risk level, with high-risk applications regulated	No specific AI standards	Lack of tailored regulations for high-risk applications
Transparency and Explainability	Mandated for high-risk AI systems	No explicit requirement	Limited explainability and accountability
Bias Detection and Mitigation	Required audits for high-risk AI	There are no provisions for bias detection	Risk of perpetuating biases in AI applications
Accountability Mechanisms	Comprehensive documentation and oversight are required	General data accountability provisions	Limited accountability for AI-driven decisions
Data Protection Standards	Strict alignment with GDPR, including regular audits	General data protection lacks AI-specific measures	Insufficient data protection for sensitive legal data
Risk-Based Categorization	Yes, with targeted provisions for high-risk applications	No risk-based differentiation	Blanket regulation, irrespective of application impact

Source: *author elaboration*

This comparison underscores the limitations of India's current approach to AI regulation in the legal sector. The lack of AI-specific standards, transparency requirements, and risk-based differentiation highlights India's need for a robust regulatory framework. Implementing AI-specific guidelines similar to the EU's AIA could help address these gaps, ensuring that AI applications in Indian legal services uphold privacy, fairness, and accountability (Table 1).

5. PROPOSED FRAMEWORK FOR PRIVACY AND DATA PROTECTION IN AI-DRIVEN LEGAL SERVICES IN INDIA

In light of the identified gaps in India's existing regulatory landscape, there is an urgent need to adopt a comprehensive framework that safeguards privacy and ensures accountability in AI-driven legal services. This proposed framework integrates transparency, accountability, bias mitigation, and privacy-by-design principles to promote trust and align India's practices with international benchmarks, such as the European Union's Artificial Intelligence Act (AIA).

5.1 Embedding Privacy-by-Design in Legal AI Systems

Privacy-by-design is a foundational principle that requires privacy considerations to be integrated from the earliest stages of AI system development. In the legal services sector, where highly sensitive information such as client identities, case histories, and legal strategies is routinely processed, embedding these measures is beneficial and imperative for ensuring confidentiality and compliance with emerging privacy norms (Sargiotis, 2024).

Key strategies include:

- **Data Minimization:** AI systems must be designed to collect only the data essential for their specific function, reducing unnecessary exposure to sensitive information.
- **Anonymization and Pseudonymization:** Where feasible, personal data should be anonymized to protect individual identities and mitigate re-identification risks.
- **Purpose Limitation:** Data should be used solely for the explicitly defined purposes for which it was collected. Any repurposing should require renewed consent from data subjects.
- **Regular Privacy Audits:** Periodic audits should be conducted to assess compliance with privacy regulations and identify any emerging vulnerabilities or risks.

By operationalizing privacy-by-design principles, Indian legal services can reduce the likelihood of data breaches and build user trust in AI-enabled systems.

5.2 Fostering Transparency and Explainability

Transparency and explainability are crucial for fostering trust in AI-assisted legal decision-making. Legal practitioners and clients must clearly understand how AI systems function, especially when these systems inform or influence outcomes in high-stakes scenarios.

Recommended practices include:

- **Explainable AI Models:** Prefer interpretable models (e.g., decision trees, rule-based systems) in critical legal applications to ensure understandable and traceable decisions.
- **Comprehensive Documentation and Guidelines:** Provide practitioners with clear, accessible documentation that outlines the AI system's capabilities, limitations, assumptions, and associated risks.
- **Transparency Reports:** Develop and publish detailed reports on the AI system's data sources, decision logic, and performance metrics to enhance accountability and external scrutiny.
- **Client Disclosure and Consent:** Ensure that clients are informed of the AI system's role in the legal process and that they retain the right to

question or contest automated outcomes, which aligns with global norms for informed consent.

Improved transparency enables legal professionals to make more informed decisions and empowers clients by clarifying the role of AI in legal proceedings.

5.3 Institutionalizing Accountability and Ethical Oversight

Establishing precise accountability mechanisms is essential to ensure that the deployment of AI in legal services remains ethical and responsible. It becomes challenging to redress issues such as discriminatory outcomes, privacy breaches, or system errors without accountability (Al-Dulaimi & Mohammed, 2025). Suggested accountability measures include:

- **AI Compliance Officers**: Appoint dedicated officers within legal institutions to monitor AI usage, address compliance concerns, and respond to ethical or legal queries related to system performance.
- **Comprehensive System Documentation:** Maintain detailed records of system architecture, training datasets, decision pathways, and updates to facilitate audits and legal scrutiny.
- **Independent Ethical Review Boards:** Establish boards comprising legal, technical, and ethics experts to review high-risk AI deployments and ensure alignment with principles of fairness, privacy, and legal integrity.
- **Periodic Bias Audits:** Conduct bias audits with inputs from multidisciplinary teams to identify and mitigate discriminatory patterns across different demographic or social groups.

Such mechanisms are vital not only for ensuring regulatory compliance but also for fostering public confidence in the ethical application of AI in justice-related domains.

5.4 Training Legal Professionals in AI and Privacy Governance

Equipping legal professionals with knowledge about AI technologies and privacy frameworks is critical to responsible AI adoption. Informed practitioners are better equipped to deploy AI tools effectively, mitigate legal and ethical risks, and advocate for their clients' rights (Corfmat et al., 2025). A recommended training program should include:

- **Foundations of AI and Machine Learning**: Introduce core concepts, operational mechanisms, and known limitations of AI tools relevant to the legal domain.
- **Data Privacy and Protection**: Educate on key privacy principles, such as data minimization, secure handling, and compliance with India's Digital Personal Data Protection Act (DPDPA).
- **Fairness and Anti-Bias Awareness:** Train professionals to detect and mitigate algorithmic bias, fostering equitable treatment across cases and clients.
- **Interpretation and Communication of AI Outputs**: Develop skills to accurately interpret AI-generated outputs and clearly explain them to clients, including articulating the scope and limitations of AI assistance.

Targeted training initiatives can bridge the knowledge gap and empower legal professionals to integrate AI in a manner that is legally sound, ethically robust, and client-centric.

6. RECOMMENDATIONS FOR A PRIVACY-CENTRIC IMPLEMENTATION OF AI IN INDIAN LEGAL SERVICES

Integrating artificial intelligence into India's legal services offers transformative potential, from streamlining legal research to enhancing judicial efficiency. However, to harness these benefits responsibly, it is essential to prioritize privacy, ethical safeguards, and accountability frameworks tailored to the legal domain. The following recommendations present a roadmap for ensuring that AI implementation in Indian legal services is both privacy-centric and aligned with international standards such as the European Union's Artificial Intelligence Act (AIA).

- **Develop AI-Specific Privacy Regulations**
  India must move beyond generic data protection frameworks and adopt AI-specific regulations, especially for high-stakes legal applications. Key components should include risk-based categorization of AI systems, mandatory transparency disclosures, and the establishment of independent oversight bodies to audit compliance and ensure ethical alignment.
- **Foster Human-AI Collaboration in Judicial Processes**
  AI should be positioned as a supportive tool rather than a replacement for human judgment. Legal professionals, particularly judges, should retain decision-making authority while leveraging AI for data analysis and procedural insights. Explainable AI (XAI) models should be prioritized to ensure that outputs are understandable and interpretable.
- **Institutionalize Regular Audits and Ethical Assessments**
  Routine audits are crucial for detecting algorithmic bias, assessing data security, and ensuring fairness. Ethical assessments conducted by interdisciplinary panels can identify risks pre-emptively and ensure that AI systems align with the values of justice, equity, and transparency.
- **Establish Clear Consent and Data Usage Policies**
  Legal service providers must inform clients about how AI-driven systems use their data. They

should implement transparent consent mechanisms as a standard practice, ensuring clients can opt out or withdraw consent anytime. Providers must also obtain purpose-specific consent, especially when using data for model training or secondary applications.

- **Enhance AI and Privacy Training for Legal Professionals**
  Capacity building is vital to the responsible adoption of AI. Legal practitioners should receive training in AI technologies, data privacy laws (such as India's DPDPA), the ethical use of AI, and strategies for mitigating bias. Such education ensures informed usage, protects client rights, and promotes confidence in AI-assisted legal services.

By integrating these recommendations into policy and practice, India can establish a robust legal AI ecosystem that enhances operational efficiency and safeguards fundamental rights, reinforcing public trust in technology-driven justice.

7. CONCLUSION

Integrating artificial intelligence (AI) into India's legal services promises to improve efficiency, reduce case backlogs, and enhance access to justice. However, this progress also brings critical concerns regarding privacy, accountability, and ethical governance, particularly in the absence of AI-specific regulatory frameworks. While the Digital Personal Data Protection Act (DPDPA) 2023 lays the foundation for data protection, it does not address the unique challenges posed by AI in legal contexts. In comparison, the European Union's Artificial Intelligence Act (AIA) provides a framework for categorizing AI systems by risk and enforces strict safeguards for high-risk applications, including legal technologies. India's current regulatory approach lacks such specificity, leaving gaps in transparency, explainability, and bias mitigation. This paper emphasizes the urgent need for a privacy-centric framework tailored to India's legal sector, including provisions for risk-based AI categorization, privacy-by-design principles, independent oversight, and regular audits. Moreover, training legal professionals in AI ethics, data privacy, and algorithmic fairness is crucial to ensure the responsible implementation of AI. Rather than replacing human judgment, AI should augment legal decision-making in a transparent, fair, and accountable manner. With thoughtful regulation and ethical deployment, India can shape a trustworthy and human-centred future for AI in legal services.

References

Directorate-General for Communication (2024). AI Act enters into force. https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.

Al-Dulaimi, A. O. M., & Mohammed, M. A. A. W. (2025). Legal responsibility for errors caused by artificial intelligence (AI) in the public sector. *International Journal of Law and Management*. ahead-of-print. https://doi.org/10.1108/IJLMA-08-2024-0295

Atrey, I. (2023). Revolutionising the legal industry: The intersection of artificial intelligence and law. *International journal of law management & humanities*,6(3), 1075.

Bahangulu, J. K., & Owusu-Berko, L. (2025). Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency and compliance in AI-powered business analytics applications. *World J Adv Res Rev*, *25*(2), 1746-63.

Banshal, S. K. (2025). Data Security and Ethical Considerations in Embedded AI Systems. In *Embedded Artificial Intelligence* (pp. 279-292). Chapman and Hall/CRC.

Bhattacharjee, B. (2024). Facial Recognition Technology Balancing Ethical Considerations and Privacy Rights. *Available at SSRN 4885585*.

Brożek, B., Furman, M., Jakubiec, M., & Kucharzyk, B. (2024). The black box problem revisited. Real and imaginary challenges for automated legal decision making. *Artificial Intelligence and Law*, *32*(2), 427-440. doi:10.1007/s10506-023-09356-9.

Chaudhary, G. (2024). Unveiling the black box: Bringing algorithmic transparency to AI. *Masaryk University Journal of Law and Technology*, *18*(1), 93-122.

Cook, J. J., & Heinrich, D. R. M. (2023). AI-Ready Attorneys: Ethical Obligations and Privacy Considerations in the Age of Artificial Intelligence. *U. Kan. L. Rev.*, *72*, 313.

Corfmat, M., Martineau, J. T., & Régis, C. (2025). High-reward, high-risk technologies? An ethical and legal account of AI development in healthcare. *BMC Medical Ethics*, *26*(1), 4.

Dandotiya, A. S., Gupta, S. K., Dandotiya, N., & Sharma, M. P. (2024). *AI in everyday life: transforming society*. Navi International Book Publication house.

Das, A., Muschert, G., Dutta, M. J., Aytaç, M. B., Tripathi, P., Khare, A., & Ray, S. (2024). AI Impacts, Concerns, and Perspectives in the Global South A Thought Leadership Round Table. *Социологическое обозрение*, *23*(4), 173-195.

Dhir, M., & Verma, S. (2024). *AI for good: India and beyond: Detailed analysis of AI & laws, policies, ethical frameworks and judgements*. Notion Press.

Digital Transformation in India: (2024). A New Era of Innovation.. https://startup-house.com/blog/digital-transformation-india.

Ejjami, R. (2024). AI-driven justice: Evaluating the impact of artificial intelligence on legal systems. *Int. J. Multidiscip. Res*, *6*(3), 1-29.

Elyounes, D. A. (2019). Bail or jail? Judicial versus algorithmic decision-making in the pretrial system. *CoLuM. SCi. & TECH. L. REv.*, *21*, 376.

INDIAI (2021). Enhancing the efficiency of India's courts using AI, https://indiaai.gov.in/case-study/enhancing-the-efficiency-of-india-s-courts-using-ai.

Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, *6*(1), 2053951719860542.

Findley, K. A. (2017). Reducing error in the criminal justice system. *Seton Hall L. Rev.*, *48*, 1265.

Hacker, P., & Passoth, J. H. (2020, July). Varieties of AI explanations under the law. From the GDPR to the AIA, and beyond. In *International workshop on extending explainable AI beyond deep models and classifiers* (pp. 343-373). Cham: Springer International Publishing.

Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. *IEEE Computational Intelligence Magazine*, *17*(1), 72-85.

Khan, S. U., Khan, S., Ballewar, S. S., Rane, J. P., & Siddiquee, A. Q. (2025). Cinema and Artificial Intelligence: Charting Its Role in the Indian Film Sector. In *Transforming Cinema with Artificial Intelligence* (pp. 143-180). IGI Global Scientific Publishing.

Kluttz, D. N., & Mulligan, D. K. (2019). Automated decision support technologies and the legal profession. *Berkeley technology law journal*, *34*(3), 853-890.

Micklitz, H. W., & Sartor, G. (2025). Compliance and enforcement in the AIA through AI. *Yearbook of European Law*, yeae014.

Mohod, V., Borde, M. P., Rathi, T., More, M., Chintamani, B. G., Waghulkar, S., ... & Mahajan, R. D. (2025). Harnessing Predictive Analytics and AI in Judicial Decisions. In *Exploration of AI in Contemporary Legal Systems* (pp. 187-216). IGI Global Scientific Publishing.

Morison, J., & Harkens, A. (2019). Re-engineering justice? Robot judges, computerised courts and (semi) automated legal decision-making. *Legal Studies*, *39*(4), 618-635.

Naithani, P. (2024). Analysis of India's Digital Personal Data Protection Act, 2023", International Journal of Law and Management, ahead-of-print. DOI: 10.1108/IJLMA-05-2024-0174

Negi Advocate, C. (2023). In the Era of Artificial Intelligence (AI): Analyzing the Transformative Role of Technology in the Legal Arena. *Available at SSRN 4677039*.

Nithya, M., Harini, S., Kavyadharshini, S., & Srinidhi, K. (2024, December). AI-Driven Legal Automation to Enhance Legal Processes with Natural Language Processing. In *2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)* (pp. 1246-1253). IEEE.

Press Information Bureau. (2024). Measures to Translate and Publish Proceedings and Judgments of Supreme Court and High Courts. Government of India.

Priya, K. (2025). The role of legal technology in enhancing judicial efficiency and access to justice. *Холодная наука*, (13), 74-81.

Rafiq, J. (2024). Harnessing the Power of Artificial Intelligence in Indian Justice System: An Empirical Study. *National Journal of Cyber Security Law*, *7*(1), 18-37.

Rajendran, R. K., Vetrivel, S., & NR, W. B. (2025). The Role of AI in Enhancing Access to Justice and Legal Services. In *Exploration of AI in Contemporary Legal Systems* (pp. 139-162). IGI Global Scientific Publishing.

Remus, D., & Levy, F. (2017). Can robots be lawyers: Computers, lawyers, and the practice of law. *Geo. J. Legal Ethics*, *30*, 501.

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data Privacy and Protection: Legal and Ethical Challenges. *Emerging Threats and Countermeasures in Cybersecurity*, 433-465.

Nigam, S. K., Patnaik, B. D., Thomas, A. V., Shallum, N., Ghosh, K., & Bhattacharya, A. (2025). Structured Legal Document Generation in India: A Model-Agnostic Wrapper Approach with VidhikDastaavej. *arXiv preprint arXiv:2504.03486*.

Sargiotis, D. (2024). Data security and privacy: Protecting sensitive information. In *Data governance: a guide* (pp. 217-245). Cham: Springer Nature Switzerland.

Schuett, J. (2023). *Towards risk-based AI regulation* (Doctoral dissertation, Dissertation, Frankfurt am Main, Johann Wolfgang Goethe-Universität, 2025).

Shahlaei, C. A., & Berente, N. (2024). An Analysis of European Data and AI Regulations for Automotive Organizations. *arXiv preprint arXiv:2407.11271*.

Sharma, M. (2023). India's courts and artificial intelligence: A future outlook. *LeXonomica*, *15*(1), 99-120.

Singla, L., preet Kaur, K., & Kaur, N. (2024). AI's Double-Edged Sword: Examining the Dark Side of AI in Human Lives. In *Demystifying the Dark Side of AI in Business* (pp. 44-59). IGI Global.

Stępień, M. (2025). A developmental approach to judicial empathy. In *Judicial Character in Hard Times* (pp. 104-124). Edward Elgar Publishing.

Sundara, K., & Narendran, N. (2023). The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection. *Computer Law Review International*, *24*(5), 129-141.

Taylor, M. J., & Paterson, J. M. (2020). Protecting Privacy in India: The roles of consent and fairness in data protection. *Indian JL & Tech.*, *16*, 71.

Prabhavathi, N., & Durai, K. (2024). Role Of Artificial Intelligence In Access To Justice And Justice Delivery In India. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).

Thakkar, D. (2024). *Towards examining Human-AI collaboration across the AI pipeline* (Doctoral dissertation, City, University of London).

Thakur, A., & Kumar, M. (2024). Right to Privacy vis-a-vis Artificial Intelligence: Indian Scenario. *Issue 2 Int'l JL Mgmt. & Human.*, *7*, 3370.

Xu, Z. (2022). Human judges in the era of artificial intelligence: challenges and opportunities. *Applied Artificial Intelligence*, *36*(1), 2013652. doi:10.1080/08839514.2021.2013652.

Yekollu, R. K., Bhimraj Ghuge, T., Sunil Biradar, S., Haldikar, S. V., & Farook Mohideen Abdul Kader, O. (2024, February). AI-driven personalized learning paths: Enhancing education through adaptive systems. In *International Conference on Smart data intelligence* (pp. 507-517). Singapore: Springer Nature Singapore.

Zeb, S., Nizamullah, F. N. U., Abbasi, N., & Fahad, M. (2024). AI in healthcare: revolutionizing diagnosis and therapy. *International Journal of Multidisciplinary Sciences and Arts*, *3*(3), 118-128.

Manindra Singh Hanspal
Yudhistir Mishra Law College,
Balangir, Odisha, India,
mhanspal21@gmail.com
ORCID: 0009-0002-5973-807X

Bijayananda Behera
Lajpat Rai Law College, Sambalpur,
Odisha, India
drbijayanandabehera@gmail.com