ARTIFICIAL INTELLIGENCE IN THE INDIAN LEGAL SYSTEM: CHALLENGES, OPPORTUNITIES AND THE FUTURE OF JUSTICE

[1]V.RAJITHA, [2]Gorantla Udai Deepak
[12]Final year student at Law
[12]Aurora Deemed to be University, Bhongir, Telangana, India

***Abstract*—Artificial intelligence (AI) is increasingly influencing the administration and practice of law in India. Its applications include legal research, document review, translation, transcription, case-information management, scheduling, and assistance in analysing large volumes of legal material. These tools may improve efficiency and access to justice in a system affected by substantial case backlogs, linguistic diversity and unequal access to legal services. At the same time, AI creates serious risks: inaccurate or fabricated legal authorities, algorithmic bias, privacy violations, opacity, cybersecurity threats, unequal access, and the possibility that automated recommendations may improperly influence judicial or professional judgment. This paper examines the opportunities and limits of AI in the Indian legal system through doctrinal legal research. It analyses constitutional principles, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and its phased commencement, the Bharatiya Sakshya Adhiniyam, 2023, and selected judicial and institutional developments. Particular attention is given to the Supreme Court of India's White Paper on Artificial Intelligence and Judiciary (November 2025), and its decision in Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd. (2026), which addressed reliance on AI-generated fictitious authorities. The paper argues that AI should operate as a supervised support system rather than an independent decision-maker. It recommends human oversight, mandatory verification of legal sources, privacy-by-design, bias testing, transparent procurement, audit trails, professional training and accessible grievance mechanisms. The future legitimacy of legal AI in India depends not merely on technological capability, but on its compatibility with constitutional values, procedural fairness and the rule of law.**

***Index Terms*—Artificial Intelligence, Indian Legal System, Judiciary, Access to Justice, Algorithmic Bias, Data Protection, Legal Ethics, Human Oversight**

I. Introduction

Artificial intelligence refers broadly to computational systems capable of performing tasks commonly associated with human cognitive functions, including language processing, pattern recognition, prediction, classification and generation of text or other outputs. Modern generative AI systems can produce fluent legal explanations, summarise documents and draft preliminary text. Their fluency, however, should not be confused with legal accuracy, sound reasoning or authority.

India's justice system operates at an enormous scale and serves people who speak many languages and have widely differing levels of digital access. Technology can help courts and legal professionals manage information, reduce repetitive work and make legal materials easier to navigate. The Government has

reported the use of AI-related technologies, including machine learning, natural language processing and optical character recognition, in e-Courts applications for translation, forecasting, administrative efficiency, filing, scheduling and communication with litigants. It has also described the Legal Research Analysis Assistant (LegRAA) as a research-support tool developed for judicial use. These developments show that AI is no longer a purely theoretical issue.

Yet the use of AI in law raises a fundamental question: how can efficiency be improved without weakening fairness, accountability and judicial independence? A legal system cannot treat a plausible machine-generated answer as a substitute for a verified source, a reasoned judicial finding or professional responsibility. The central argument of this paper is that AI can strengthen the Indian legal system only when its use remains transparent, proportionate, reviewable and subject to meaningful human control.

II. STATEMENT OF THE PROBLEM

The rapid adoption of AI tools has outpaced the development of detailed, uniform safeguards for every legal setting. AI outputs may be inaccurate, incomplete or fabricated; training data may reproduce historical discrimination; and personal or confidential information may be exposed when entered into external systems. Where a tool influences bail, sentencing, case prioritisation, legal aid or other consequential decisions, an error may affect liberty, equality or access to remedies. The problem is therefore not simply whether AI is useful, but who is responsible when it fails, how affected persons can challenge its use, and what safeguards are required before it is deployed.

III. OBJECTIVES OF THE STUDY

- To examine the present and potential applications of AI in Indian courts and legal practice.
- To analyse the constitutional and statutory principles relevant to AI-enabled legal services and decision-support systems.
- To identify risks relating to accuracy, bias, privacy, transparency, cybersecurity and professional ethics.
- To study recent Indian judicial and institutional developments concerning AI in the justice system.
- To propose practical safeguards for responsible, human-centred adoption of AI.

IV. RESEARCH QUESTIONS AND WORKING PROPOSITION

- How can AI improve the efficiency and accessibility of legal services in India?
- Which constitutional and statutory protections constrain the use of AI in legal processes?
- What safeguards are needed to prevent fabricated legal authorities, discriminatory outcomes and misuse of personal data?
- Can AI be used in judicial administration without undermining judicial independence and the duty to give reasons?

Working proposition: AI is constitutionally and institutionally acceptable as an assistive technology where its purpose is legitimate, its use is proportionate, its outputs are independently verified, and a responsible human decision-maker retains authority and accountability.

V. RESEARCH METHODOLOGY

This paper adopts a doctrinal and analytical method of legal research. It examines primary legal materials, including the Constitution of India, parliamentary statutes, delegated legislation, and reported judicial decisions. It also considers official institutional materials published by the Supreme Court of India and the Government of India. Secondary analysis is used to identify recurring themes and evaluate policy choices. The study is qualitative; it does not claim to be based on interviews, surveys, fieldwork or statistical measurement. The legal position is stated as at 6 November 2026. Because the commencement of the Digital Personal Data Protection Act, 2023 is phased, the paper distinguishes between enactment, notified rules and provisions that have not yet commenced on the date of writing.

VI. CONSTITUTIONAL AND STATUTORY FRAMEWORK

6.1 The Constitution of India

Article 14 guarantees equality before the law and equal protection of the laws. An AI system used by a public authority may raise Article 14 concerns if it relies on discriminatory data, produces arbitrary classifications or applies criteria that cannot be justified. A system that appears neutral may still disadvantage groups because of historical patterns in the data on which it was trained. Public authorities should therefore assess disparate impact, explain the purpose of a system and provide a meaningful route to human review.

Article 21 protects life and personal liberty. In Maneka Gandhi v Union of India, the Supreme Court held that a procedure affecting personal liberty must be just, fair and reasonable. Automated tools used in criminal justice, detention, surveillance or access to essential legal services must therefore be assessed against procedural fairness and the consequences for affected persons. The right to privacy recognised in Justice K.S. Puttaswamy (Retd.) v Union of India is also relevant where AI systems collect, infer, process or share personal information. The principles of legality, legitimate aim, necessity and proportionality provide an important constitutional framework for evaluating state use of data-driven systems.

6.2 Information Technology Act, 2000

The Information Technology Act, 2000 provides the foundational statutory framework for electronic records, electronic signatures, specified cyber offences and intermediary-related matters. It gives legal recognition to electronic records and electronic transactions, but it is not a comprehensive AI regulation statute. Its provisions may be relevant where AI deployment involves unauthorised access, damage to computer resources, identity-related offences, privacy breaches or intermediary obligations. The Act must

be read with applicable rules and other laws; it should not be treated as resolving every question about algorithmic accountability or AI-generated content.

6.3 Digital Personal Data Protection Act, 2023 and Rules

The Digital Personal Data Protection Act, 2023 establishes a framework for processing digital personal data, including obligations for data fiduciaries and rights and duties of individuals. It is highly relevant to legal AI because legal systems handle sensitive case files, client information, witness details and other personal data. Principles such as lawful processing, notice, consent where applicable, purpose limitation, security safeguards and accountability should inform the design and procurement of AI tools.

A crucial qualification is necessary. The Act received presidential assent in August 2023, but its provisions were brought into force through a phased notification dated 13 November 2025. As at 6 November 2026, the notification schedules several substantive provisions, including sections 3–17, to commence eighteen months after publication (13 May 2027), while certain other provisions have earlier or different commencement dates. The Digital Personal Data Protection Rules, 2025 also contain staged commencement. Accordingly, it would be inaccurate to state that every substantive duty under the Act and Rules is already fully operational on the date of this paper. Institutions should plan for compliance while checking the precise commencement status of each provision.

6.4 Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), in force from 1 July 2024, recognises electronic and digital records. Sections 61–63 address the legal effect and proof of electronic records, including conditions for admissibility of computer outputs. AI may assist in searching, transcribing or analysing digital evidence, but it does not remove the need to establish authenticity, integrity, provenance and compliance with evidentiary requirements. A machine-generated summary is not automatically a substitute for the underlying record or the statutory proof required for its admission.

6.5 Other relevant legislation

The Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Nyaya Sanhita, 2023 form part of the current criminal law framework and may intersect with technology-enabled investigation and proceedings. The Copyright Act, 1957 may become relevant to training data, reproduction and outputs, while professional duties under the Advocates Act, 1961 and Bar Council of India rules remain important when lawyers use AI in research, drafting or client work. These laws do not create a general licence to delegate professional judgment to software.

VII. APPLICATIONS OF AI IN THE INDIAN LEGAL SYSTEM

7.1 Legal research and document analysis

AI-supported search and language tools can help locate potentially relevant statutes and decisions, classify large document collections, compare versions and generate preliminary summaries. This can reduce the time spent on repetitive tasks. However, search results must be checked against authoritative databases and the full text of the judgment. Lawyers remain responsible for ensuring that a cited case exists, is correctly reported, remains good law and supports the proposition for which it is cited.

7.2 Court administration and case management

AI-assisted scheduling, cause-list management, filing checks, transcription and document classification may reduce administrative burdens. Predictive tools might help identify procedural bottlenecks or estimate workload, but they should not determine the merits of individual cases. Administrative efficiency must not become a justification for opaque prioritisation that disadvantages particular litigants.

7.3 Translation and access to justice

India's linguistic diversity makes translation and speech-to-text tools potentially valuable. AI may help convert judgments, orders and legal information into accessible formats and regional languages. Yet legal translation requires special care: a mistranslated term can change the meaning of a right, obligation or procedural direction. Important documents should be reviewed by qualified human translators, and users should be told when a translation is machine-generated.

7.4 Legal aid and public legal information

Conversational systems can explain basic procedures, identify relevant public services and guide users towards legal aid institutions. These systems should not present themselves as lawyers, promise outcomes or discourage urgent professional assistance. They should provide clear limitations, protect user information and refer complex or high-risk matters to qualified human support.

7.5 Assistance to judges

AI can potentially assist with chronology preparation, summarisation, transcription and locating authorities. It must not replace the judge's independent assessment of evidence, credibility, law or remedy. The judicial function requires reasons that can be understood and reviewed. A system that conceals its sources or effectively determines an outcome risks weakening open justice and judicial accountability.

VIII. RISKS AND CHALLENGES

8.1 Hallucinations and legal accuracy

Generative AI may produce invented case names, incorrect citations, false quotations or inaccurate descriptions of statutes. This is especially dangerous because the output may be expressed confidently. A

fabricated precedent can mislead a court, waste public resources and damage the credibility of counsel. Verification must therefore be mandatory: every authority, quotation, statutory provision and factual assertion generated by AI should be checked against an authoritative source before use.

8.2 Bias and discrimination

AI systems learn patterns from data. If historical data reflects unequal policing, unequal access to representation or social disadvantage, a model may reproduce or amplify those patterns. Risk scores and classification systems can create an appearance of scientific neutrality while embedding contestable assumptions. Before deployment, institutions should test data quality, error rates and disparate impacts, and should periodically reassess performance across relevant groups.

8.3 Privacy and confidentiality

Legal files may contain medical records, financial details, addresses, information about children, trade secrets and privileged communications. Uploading such material to a public or inadequately secured AI service can create confidentiality and data-protection risks. Lawyers and courts should use approved systems, minimise personal data, redact identifiers where possible, assess retention and cross-border processing, and avoid entering privileged information into tools whose terms and security are not understood.

8.4 Opacity and explainability

Some AI systems cannot provide a clear explanation of how a particular output was produced. This is problematic where an output affects rights or access to remedies. A person should not be left unable to challenge a decision because the relevant criteria are secret or unintelligible. Public bodies should document the purpose, data sources, limitations and validation of systems used in consequential settings.

8.5 Accountability and professional responsibility

AI does not hold a practising certificate, owe fiduciary duties or answer to a disciplinary body in the same way as a lawyer. Responsibility must remain with identifiable human and institutional actors. Lawyers must verify work product; judges must independently decide cases; court administrators must oversee procurement and deployment; and vendors must be subject to enforceable contractual and security obligations.

8.6 Digital divide and unequal access

A technology-led justice system may exclude people without reliable internet, devices, digital literacy, accessible interfaces or proficiency in dominant languages. AI should supplement, not eliminate, physical counters, human assistance and offline procedures. Accessibility for persons with disabilities and people in rural areas must be part of system design.

IX. JUDICIAL AND INSTITUTIONAL DEVELOPMENTS

The Supreme Court of India's Centre for Research and Planning published a White Paper on Artificial Intelligence and Judiciary in November 2025. Its publication is an important institutional step towards examining the benefits, risks and governance requirements of AI in courts. The Government has also publicly described AI-related uses in e-Courts applications, including translation, prediction and forecasting, administrative efficiency, automated filing, scheduling and litigant communication. It has referred to LegRAA as a tool intended to assist judicial research and document analysis.

A significant warning appears in Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd., 2026 INSC 668 (2 July 2026). The Supreme Court set aside tribunal decisions that had relied on non-existent or hallucinated AI-generated authorities. The Court emphasised that AI may be used as an aid, but adjudication must remain under human control. It called for a zero-tolerance approach to unverified AI-generated precedents and directed the Bar Council of India to constitute a committee to consider guidance and disciplinary consequences. The decision demonstrates that the central legal risk is not the mere use of AI, but the uncritical treatment of its output as authentic law.

On 3 June 2026, the Supreme Court also published a preliminary draft titled Regulations for Use of Artificial Intelligence (AI) in Courts, 2026, inviting stakeholder comments. The draft identified human primacy, transparency, accountability, data protection and judicial independence as guiding principles. As a draft consultation document, it should not be described as final binding regulations unless and until formally adopted and brought into force. These developments show movement towards structured governance, while leaving a continuing need for clear operational standards.

X. ANALYSIS AND DISCUSSION

The strongest case for AI in Indian justice is its ability to reduce information-processing burdens. Legal professionals routinely handle large records, repeated procedural documents and extensive bodies of precedent. Carefully designed tools can make this work faster and may free human professionals to focus on advocacy, legal reasoning and client interaction. Translation and accessible information tools may also reduce barriers for litigants who cannot easily navigate formal legal language.

However, speed is not the same as justice. The constitutional legitimacy of a decision depends on lawful authority, fair procedure, impartiality and reasons. A system that increases throughput but introduces hidden discrimination, fabricated authorities or unreviewable errors may undermine rather than improve justice. The risk is particularly acute when an AI system is used in criminal proceedings or other matters involving liberty, livelihood, family integrity or access to public benefits.

A distinction should be drawn between low-risk administrative assistance and high-impact decision support. Spell-checking, transcription and document sorting may be suitable for carefully monitored automation. By contrast, tools that rank litigants, predict individual guilt, recommend bail or sentencing, assess witness

credibility, or influence the outcome of a case require much stricter scrutiny and, in some contexts, should not be used. The more consequential the use, the stronger the need for independent validation, disclosure, human review and a right to challenge.

The 2026 Supreme Court decision illustrates the professional dimension of this distinction. AI can help a lawyer discover a possible authority, but the lawyer must verify it. AI can help a judge organise material, but the judge must decide the case. Responsibility cannot be transferred to the software provider or hidden behind an algorithm. This approach preserves the benefits of technological assistance while protecting the institutional role of legal professionals.

XI. RECOMMENDATIONS

1. Adopt a risk-based framework. Classify AI applications according to their impact on rights, liberty, privacy and access to justice. High-impact uses should require prior approval and stronger safeguards.
2. Keep a human decision-maker in control. AI should not independently determine guilt, bail, sentence, credibility, legal entitlement or the outcome of a judicial proceeding.
3. Require source verification. Every AI-generated case citation, statutory reference, quotation and proposition of law must be checked against an authoritative primary source before being filed or relied upon.
4. Create transparent records. Courts and public authorities should maintain an inventory of approved AI tools, record their purpose and limitations, and preserve audit logs for consequential uses.
5. Protect personal and privileged information. Use secure, approved systems; minimise and redact data; set retention limits; restrict access; and assess vendor security and data-processing terms.
6. Test for bias and accuracy. Conduct pre-deployment and periodic independent audits, including tests for error rates, language performance, accessibility and discriminatory impact.
7. Provide notice and review. Where AI materially assists a consequential public decision, affected persons should receive appropriate notice, a meaningful explanation and access to human reconsideration, subject to lawful limits.
8. Train legal professionals. Judges, advocates, court staff and law students should receive practical training in AI limitations, verification, privacy, cybersecurity and professional ethics.
9. Preserve non-digital routes. Maintain human assistance and offline access so that technology does not exclude rural, poor, elderly or disabled users.
10. Strengthen institutional governance. Procurement contracts should specify security, audit access, incident reporting, data ownership, model updates, liability and exit arrangements.

XII. CONCLUSION

Artificial intelligence has the potential to support a more efficient, accessible and responsive Indian legal system. Its applications in legal research, translation, transcription, document management and court administration can help address practical difficulties faced by courts and legal professionals. The Supreme Court's White Paper and the Government's reported e-Courts initiatives demonstrate that institutional engagement with AI is already underway.

At the same time, legal decision-making cannot be reduced to statistical prediction or fluent text generation. The risks of hallucinated authorities, bias, privacy violations, opacity and unequal access are serious because they can affect constitutional rights and public confidence in the justice system. The Supreme Court's decision in Pooja Ramesh Singh reinforces the need for verification and human control. India should therefore pursue a model of responsible and human-centred AI: technology may assist, but accountable human institutions must retain authority over legal judgment.

The future of AI in Indian law should be measured not only by speed or cost savings, but by whether it advances equality, fairness, privacy, transparency and access to justice. AI will strengthen the rule of law only when it remains a tool in service of justice, rather than becoming a substitute for justice.

XIII. AUTHOR DECLARATION AND SUBMISSION CHECKLIST

This manuscript is a draft prepared for the named author. Before submission, the author should independently read and verify every proposition, citation, quotation, statutory commencement date and journal requirement; add any required institutional details; and revise the analysis to reflect her own understanding. The author should not represent that interviews, surveys or empirical research were conducted. The author must also check the journal's originality, plagiarism, AI-use disclosure, formatting and publication-fee policies.

REFERENCES AND BIBLIOGRAPHY

Constitutional and statutory materials

[1] Constitution of India, arts 14 and 21.

[2] Advocates Act 1961.

[3] Copyright Act 1957.

[4] Information Technology Act 2000.

[5] Digital Personal Data Protection Act 2023 (Act 22 of 2023).

[6] Digital Personal Data Protection Rules 2025, notified 14 November 2025, together with the phased commencement notification dated 13 November 2025.

[7] Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023), especially ss 61–63.

[8] Bharatiya Nagarik Suraksha Sanhita 2023.

[9] Bharatiya Nyaya Sanhita 2023.

Cases

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

[11] Maneka Gandhi v Union of India (1978) 1 SCC 248.

[12] Shreya Singhal v Union of India (2015) 5 SCC 1.

[13] Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd., 2026 INSC 668 (Supreme Court of India, 2 July 2026).

Official reports and policy materials

[14] Supreme Court of India, Centre for Research and Planning, White Paper on Artificial Intelligence and Judiciary (November 2025).

[15] Supreme Court of India, Notice inviting comments on the preliminary draft Regulations for Use of Artificial Intelligence (AI) in Courts, 2026 (3 June 2026).

[16] Ministry of Law and Justice, Government of India, ‘Use of Artificial Intelligence in Legal Field’ (Press Information Bureau, 11 December 2025).

[17] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Rules 2025 and enforcement timeline (14 November 2025).

Official online sources

[18] Supreme Court of India, White Paper on AI and Judiciary: https://www.sci.gov.in/reports/

[19] Supreme Court of India, Pooja Ramesh Singh judgment summary: https://www.sci.gov.in/landmark-judgment-summaries/

[20] Information Technology Act, 2000, India Code: https://www.indiacode.nic.in/indiacode/handle/123456789/1999?locale=en

[21] Bharatiya Sakshya Adhiniyam, 2023, India Code: https://www.indiacode.nic.in/indiacode/handle/123456789/20063

[22] Digital Personal Data Protection Rules 2025, MeitY: https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa

[23] PIB, Use of Artificial Intelligence in Legal Field: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2202159&lang=1&reg=6