

Brief on

**DRAFT REGULATIONS  
FOR USE OF  
ARTIFICIAL INTELLIGENCE  
IN COURTS, 2026**



## **Brief: Draft Regulations for Use of Artificial Intelligence in Courts, 2026**

On June 3, 2026, the Supreme Court released a preliminary draft titled “[Regulations for Use of Artificial Intelligence \(AI\) in Courts, 2026](#)” (Draft Regulations). The Draft Regulations aim to establish a comprehensive governance framework for the adoption, deployment, and oversight of AI across the Indian judicial system, and seek to balance innovation and efficiency with judicial independence, constitutional values, accountability, transparency, and data protection.

The Supreme Court has invited public comments and suggestions on the Draft Regulations until June 20, 2026.

### **Chapter I: Preliminary Provisions**

#### **Scope and Applicability**

The Draft Regulations apply to the use, deployment, or integration of AI in any judicial, adjudicatory, or administrative function carried out by the Supreme Court of India, High Courts, Subordinate Courts, Tribunals, and Statutory Commissions exercising adjudicatory functions.

#### **Definition of AI**

The Draft Regulations define AI as “any machine-based system that generates decisions, predictions, recommendations, or outputs with varying degrees of autonomy through algorithms, computational processes, or software.” This includes AI tools used in court processes but excludes ordinary software unless it incorporates AI capabilities.

#### **Key Concepts Introduced**

- **AI System:** Includes any software, platform, application, device, or process that employs Artificial Intelligence to perform tasks in connection with any Court process.
- **Anonymization:** The process of irreversibly altering or removing personal information from a dataset such that an individual cannot be identified, directly or indirectly.
- **Black Box Systems:** An AI whose internal reasoning cannot be explained or understood by users; subject to heightened restrictions.
- **Data Minimization:** The principle that an AI System shall collect, process, and retain only such personal data as is strictly necessary for that specific purpose for which it is deployed.
- **Generative AI (GenAI):** AI that generates text, images, audio, or code. Any GenAI content used in court proceedings must be disclosed and verified.
- **Hallucinations:** The Draft Regulations formally recognize AI hallucinations as outputs that are fabricated, misleading, unsupported by evidence, or legally incorrect, including false precedents, statutes, facts, or legal principles.
- **Human-in-the-Loop (HITL):** A Governance process ensuring all AI outputs are subject to mandatory human review; final authority always rests with a human.
- **Risk Scoring:** The Draft Regulations define risk scoring as the use of AI to estimate the likelihood of future conduct, including recidivism, flight risk, or failure to appear before court. Such systems are later prohibited under the regulations.
- **Sensitive Judicial Data:** Personal data of parties, witnesses, or representatives whose unauthorised disclosure may cause harm. Such data is afforded the highest protection.

## Chapter II: General Principles Governing AI in Courts

The Draft Regulations establish the following principles-based framework that governs every AI system deployed within the judiciary:

14 General Principles for AI Adoption in the Indian Judiciary

<p><b>1. Human Primacy and Judicial Independence</b> AI may assist judicial functions, but it cannot replace judicial decision-making; final authority over law, facts, and justice remains with judges.</p> <p><b>2. Rule of Law</b> All AI deployment must remain consistent with the Constitution of India, principles of natural justice, due process, equality before law, access to justice, and fair trial rights.</p> <p><b>3. Fairness and Non-Discrimination</b> AI systems must not create or reinforce bias and must protect the rights of vulnerable and disadvantaged groups.</p> <p><b>4. Transparency and Explainability</b> AI systems should be understandable and capable of explaining how their outputs are generated, especially in contexts affecting legal rights.</p> <p><b>5. Accountability</b> Judicial officers remain fully responsible for decisions made with AI assistance; AI errors or hallucinations cannot excuse incorrect outcomes.</p> <p><b>6. Auditability and Continuous Oversight</b> All AI systems must be subject to continuous monitoring and periodic technical, legal, and ethical audits throughout their lifecycle.</p> <p><b>7. Data Protection and Privacy</b> Systems must comply with the DPDP Act (2023), the IT Act (2000), and cybersecurity standards, affording the highest protection to sensitive judicial data.</p>	<p><b>8. Purpose Limitation</b> AI systems may only be used for approved purposes; any expanded use requires fresh written approval from the Appropriate Authority.</p> <p><b>9. Proportionality</b> AI use must match the risk profile of each task, with high-risk applications affecting liberty requiring heightened Human-in-the-Loop (HITL) safeguards.</p> <p><b>10. Inclusivity and Accessibility</b> AI deployment must expand access to justice equitably for rural, economically disadvantaged, and linguistically diverse communities.</p> <p><b>11. Data Integrity</b> AI must be trained on accurate, representative, and lawfully obtained data; systems trained on biased or unlawfully collected datasets are prohibited.</p> <p><b>12. Cyber Security</b> Court data must be protected by robust, layered, and continuously updated technical and organizational security measures.</p> <p><b>13. Presumption in Favor of Responsible AI Adoption</b> Courts are encouraged to adopt AI where it improves efficiency, reduces delays, or enhances access to justice, subject to appropriate safeguards.</p> <p><b>14. Innovation Over Restraint</b> The framework supports responsible innovation and encourages the development of AI that strengthens judicial administration and service delivery.</p>
---	---

NotebookLM

\*The above infographic is generated by AI

## Chapter III: Permissible and Prohibited Uses

Area	Permissible Uses of AI	Prohibited Uses of AI
<b>Court Administration and Operations</b>	Case management, scheduling, cause-list preparation, filing scrutiny, resource allocation, anonymization of judgements, court performance assessment, transcription, and translation; subject to human oversight.	AI cannot independently determine judicial outcomes, findings of fact or law, or sentencing decisions.
<b>Legal Research and Adjudicatory Support</b>	Legal research, precedent retrieval, citation verification, and document summarisation, with outputs remaining advisory and subject to judicial verification.	AI cannot be used for risk scoring, including recidivism prediction, flight-risk assessment, bail eligibility, or witness credibility evaluation. No submission of AI-generated evidence should be made in court without full and transparent disclosure.
<b>Litigant Services and Accessibility</b>	Chatbots for court services and procedural guidance, along with speech-to-text, text-to-speech, braille conversion, and language assistance tools.	AI cannot predict, profile, or infer the future conduct of litigants, witnesses, accused persons, or lawyers.
<b>Document Review and Verification</b>	Fraud detection, authenticity verification, and administrative document review are subject to human validation before action is taken.	Black Box AI Systems cannot be used where personal liberty or legal rights may be affected.

<b>Governance and Judicial Integrity</b>	AI may assist court processes only under human supervision and accountability.	AI-based surveillance of judges, lawyers, or litigants, and any use that compromises judicial deliberations, confidentiality, or judicial independence, is prohibited.
--	--	--

## Chapter IV: Institutional Framework

- Apex Body: A permanent national AI governance body at the Supreme Court, established by the Draft Regulations. It includes 2 judges of the Supreme Court, 2 Chief Justices of the High Court, 2 High Court judges, a representative from the Ministry of Electronics and Information Technology (not below the rank of Joint Secretary), experts in finance, cyber security, technology law or data privacy, and academic representatives.
  - Its role is to establish minimum national standards and oversee AI governance across all courts.
  - Five specialist committees support the Apex Body: the Judicial Committee, Technical Committee, Infrastructure and Finance Committee, Case and Data Management Committee, and Cyber Security Committee. Together, they oversee policy, technology, infrastructure, research, and security.
- Centre of Research and Excellence (CoRE-AI): Serves as the judiciary's dedicated research and policy institution. Its functions include conducting AI research, evaluating tools, tracking global developments, publishing studies and white papers, and advising the Apex Body.
  - Each High Court must establish an AI Committee to oversee governance and approvals, and an AI Secretariat to manage operations, audits, incident reporting, and implementation. The AI Secretariat may fast-track approval of low-risk administrative tools.

## Chapter V: Oversight, Audits and Incident Management

Mechanism	Trigger	Key Requirements
<b>Technical and Ethical Impact Assessment</b>	Before every deployment	Covers: purpose, training data, bias risks, hallucination risks, explainability, cyber security, HITL compliance, redress mechanisms
<b>Controlled Environment Testing</b>	Before full-scale deployment	Time-bound, isolated environment; must not affect live operations or influence actual judicial decisions
<b>AI Register</b>	Ongoing	Must document AI Systems used in Courts, purposes and scope of approved system, identity of AI Service Provider, records of Technical and Ethical Impact Assessments, and record of audits and their outcomes
<b>Technical / Legal / Ethical Audit</b>	At least annually; or shorter as directed	Conducted in-house only. Source code, algorithms, and datasets must NOT be shared with any external party.
<b>Cyber security Audit</b>	At least annually	Outcomes reported to Appropriate Authority and recorded in the AI Register
<b>AI Incident Reporting</b>	Upon any malfunction, bias, or error	Immediate report to AI Secretariat; shared across all High Courts; remedial action without delay
<b>Fall-back Protocol Activation</b>	Upon failure or suspension	Continuity via manual or alternative means; AI Committee notified within 24 hours

<b>Review of AI Systems Already in Use</b>	Within 1 year of commencement	AI Secretariat reviews compliance; Appropriate Authority determines action for non-compliant systems
<b>Annual Transparency Report</b>	Every year	Submitted to Apex Body and published on the court's official website; covers AI in use, audit outcomes, incidents

## Chapter VI: Procurement and Private Sector Engagement

Private entities<sup>1</sup> may provide AI solutions only after approval and rigorous evaluation. This includes:

- **Mandatory contractual protections:** Court retains ownership of all Court data and AI outputs, prohibition on use of judicial data beyond the scope of engagement, full audit and inspection rights for the AI Secretariat, mandatory indemnity clauses protecting courts from vendor defects, on-premise or sovereign cloud for sensitive data processing, prohibition on retraining AI models using court data without AI Committee approval, clear liability allocation for AI incidents and data breaches, and explainability documentation for all high-risk AI tools.
- **Intellectual Property and Data Ownership:** Where court data is used to develop AI tools, courts must retain ownership or a perpetual royalty-free license, and private vendors cannot claim exclusive ownership rights over tools built primarily using judicial data.

## Chapter VII: Data Protection and Cyber Security

The Draft Regulations impose strict data governance requirements, including compliance with the DPDPA 2023 and the IT Act 2000, data minimization, anonymization wherever feasible, restrictions on transfers of sensitive judicial data, sovereign cloud or on-premises deployment for sensitive systems, and annual cyber security audits. Sensitive judicial data cannot be transferred externally without express authorisation.

## Chapter VIII: Capacity Building and Training

The Draft Regulations require mandatory AI training for judges, advocates, and court staff, accessible to district courts and delivered in multiple languages. Training must cover AI capabilities and limitations, bias detection, hallucinations, data protection, cyber security, ethical obligations, and incident reporting. Programmes are to be reviewed by the AI Committee every two years, with each High Court preparing an annual training calendar in coordination with the Apex Body and judicial training institutions. A continuously updated repository of best practices, case studies, and lessons from AI incidents must also be maintained.

## Chapter IX: Grievance Redressal and Remedies

Any party harmed by prohibited AI use may file an application before the relevant court at the earliest opportunity, and the court must provide a reasonable opportunity to be heard before issuing appropriate orders. High Courts may prescribe simplified formats for AI-related grievances to improve accessibility, particularly for individuals with limited legal literacy. The Draft Regulations preserve all other legal remedies

---

<sup>1</sup> "Private entity" means any company, firm, partnership, trust, society, or other legal entity, whether incorporated or not, that is not owned, controlled, or managed by the Central Government or any State Government, and includes foreign entities and their subsidiaries or representatives operating in India.

available under existing law and require parties submitting AI-assisted filings to disclose such use through a prescribed declaration or certificate.

## Chapter X: Miscellaneous

These Draft Regulations operate alongside, and do not override, existing laws such as the IT Act, DPDP Act, and other applicable laws governing courts, data protection, and AI. Where a conflict arises, the applicable law prevails. The Draft Regulations also do not diminish constitutional, statutory, or court-imposed obligations on courts and judicial officers. However, if the Draft Regulations provide stronger protections than administrative instructions or directions, the regulations will prevail to that extent.

The Chief Justice or Institutional Head may issue directions to implement the regulations, provided they are consistent with them. The Chief Justice may also relax or modify any provision, except those relating to the prohibited use of AI, so long as the changes do not violate the core principles in Chapter II of the Draft Regulations (General Principles Governing AI in Courts), and any such modification must be reported to the Apex Body within two weeks. The Supreme Court AI Committee<sup>2</sup> is responsible for periodically reviewing regulations in light of technological, legal, or practical developments, with High Courts regularly contributing data, feedback, and recommendations to support continuous improvement in AI governance within the judiciary.

## Conclusion

The Draft Regulations adopt a human-led, AI-assisted model for the judiciary. They encourage AI deployment to improve efficiency, accessibility, and court administration, while establishing strict safeguards against automated adjudication, predictive justice, surveillance, and unaccountable AI systems. The Draft Regulations combine institutional oversight, mandatory impact assessments, audit obligations, transparency requirements, and strong data governance protections to ensure that AI supports rather than replaces the judicial function.

---

<sup>2</sup> The Supreme Court and each High Court shall constitute an AI Committee, chaired by a senior judge and supported by other judges and members of the AI Secretariat, to oversee AI adoption in courts. The Committee is responsible for approving AI systems, monitoring compliance, issuing supplementary directions, overseeing audits and incident reviews, preparing annual reports, coordinating with the Apex Body, and supporting AI governance in courts, tribunals, and adjudicatory commissions within its jurisdiction. It may also engage with academia, researchers, and industry on AI-related matters.