

# **INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]**

ISSN: 2584-1513 (Online)

Volume 3 | Issue 5 [2025] | Page 123 - 129

© 2025 International Journal of Legal Studies and Social Sciences

Follow this and additional works at: <https://www.ijlsss.com/>

In case of any queries or suggestions, kindly contact [editor@ijlsss.com](mailto:editor@ijlsss.com)

# **FROM CODE TO COURTROOM: FORMULATING AN INDIAN MODEL FOR TRUSTWORTHY AI IN JUSTICE**

**-Akansha Parashar<sup>1</sup>**

## **ABSTRACT**

India is charging ahead into the age of digital justice. The justice ecosystem is being restructured at scale with virtual courts, AI translation of judgments, fully digitized NI Act courts, and a comprehensive modernisation of criminal evidence and procedural law. However, many of the algorithmic services where facial recognition, machine translation, and document summarisation are used in the police and court registries operate under a legal system still grappling with the basics of privacy, explainability, and due process.

This article outlines the India-specific “Trustworthy Judicial AI” architectural framework, which is constitutionally underpinned but takes into consideration the ground realities. The article argues that a governance framework tailored to the India-specific ecosystem can be crafted from the live pilot projects, statutory developments, primary case law, and policy framework to be used not only by judges, but by other stakeholders such as prosecutors, police officers, attorneys, and even technology suppliers.

## **1. THE IMPORTANCE AND NEED OF THE DEBATE**

### **THE JUDICIAL TRANSFORMATION IS UNDERWAY IN INDIA**

The spending plan for the fiscal year 2023-24 includes the setting of a new ₹7,000 crores eCourt project, marking a new phase of state-sponsored technological integration into the judiciary. India is now set to cross modern and technological boundaries with the start of eCourts Phase III. The aim is to bring AI translation for pleadings and judgments, case ranking, virtual hearings with e-

---

<sup>1</sup> 4<sup>th</sup> Year Student at Vivekananda Institute of Professional Studies- Technical Campus, Delhi.

filing, and e-payment. Bringing e-judiciary services is set to reduce case backlogs, improve access, and alter the future dynamics of procedural delays.

## **"DIGITAL COURTS" IN PRACTICE**

In May and June of 2025, 34 complete Digital NI Act Courts for cheque bounce cases were opened at the Delhi High Court. AI scheduling, digital evidence submission, remote witness testimonies, and zero paper filing are just the highlights. The features have been attributed to the NI Act. These courts are not new, but a test to ensure that the technology integrated is responsive to the structural inequities of the system, and how it functions in the face of over 3.5 million cases. Adding more to it, these courts are not just serving a singular end, but a primary purpose of exploring effective automation.

## **SUCAS SYSTEMS AND AI RESEARCH ASSISTANTS IN AI- ENHANCED TRANSLATION INTEGRATE AI INTO JUDICIAL PROCESSES**

SUBAS and SUPACE mechanisms marked the Supreme Court's shift from the use of experimental pilots to operational integration. Further plans, still under Phase III, indicate the forecast AI will predict judicial acts, judge execution of tasks, autonomously manage agenda setup, and perform advanced searches, all under judicial supervision.

## **PROBLEMS OF AI GOVERNANCE IN POLICING LAW ENFORCEMENT**

The use of AI in the judicial and policing domains poses even more interesting problems. When the Delhi police began to extend the use of the facial recognition system in riot and public order investigations, it, for example, raised more governance issues. In an RTI (2024) disclosure, it was found that a match rate of 80% to something was treated as “identification,” something that many groups arguing for civil liberties noted as an accuracy and bias problem. In the absence of a dedicated statute, governance rests precariously on constitutional protections under Articles 14, 19, and 21, and a hodgepodge of MeitY pointers which highlight a lack of AI regulation tailored to specific industries.

## **A MOVING STATUTORY BASELINE FOR DATA PROTECTION: REGULATORY COMPLIANCE ON DATA PROTECTION**

The Digital Personal Data Protection Act of 2023 is India's first multi-sector privacy legislation. It establishes requirements for data fiduciaries regarding lawful processing, data minimization, breach reporting, and data principal rights, enforcing fines of up to ₹250 crore. As of August 2025, Draft Rules containing guidance treat AI deployments in a state of suspended animation governed by the IT Act of 2000 and IT Rules of 2011. Upon the DPDP Act's full enactment, it will play a critical role in the governance of judicial AI training datasets, consent mechanisms, and fairness algorithms.

### **TAKEAWAY: CONCERNS AND COMPLIANCE**

Rather than asking whether AI should be applied in the judicial sphere, India has decisively moved forward with implementation. The primary task now is to safeguard and proactively manage constitutional and legal frameworks to prevent bias and opacity, ensuring core due process standards are not undermined, especially before AI systems are permanently embedded in the judiciary.

## **2. REAL-TIME CASE STUDIES AND INFORMATION: INDIA'S ALGORITHMIC JUSTICE TRIALS**

### **THE THRESHOLD OF PRIVACY AND ARTICLE 21**

In K.S. Puttaswamy v. Union of India (2017), the Supreme Court's nine-judge panel upheld the proportionality test for any State action restricting fundamental rights and constitutionalized the right to privacy under Article 21. In order to evaluate data-intensive judicial technologies like facial recognition tools (FRT) and algorithmic risk scoring in bail or sentencing, the four-limbed test, legitimate aim, rational connection, necessity (least intrusive means), and balancing, has become the standard.

The Court applied proportionality to internet access restrictions in Jammu & Kashmir in Anuradha Bhasin v. Union of India (2020), requiring: Reasoned, reviewable orders for any tech-enabled

restriction; and necessity and minimal impairment of rights. This case indicates that state actions driven by AI that impact digital rights or access to justice must adhere to the same exacting transparency and necessity thresholds.

In order to modernize evidentiary rules, the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the Indian Evidence Act, 1872, affirms electronic records as admissible primary evidence (Sections 61–63) and prescribes comprehensive authentication and integrity verification methods for digital records, which are crucial for evidence that is generated or processed by artificial intelligence. The Bharatiya Nyaya Sanhita, 2023 (BNS) and Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) restructure substantive offenses and criminal procedure, respectively, and foresee: A rise in the use of digital workflows, such as video testimony and e-summons. Integrated data sharing between the police, prosecution, and courts will necessitate careful chain-of-custody and due process protections if AI is enabled.

## **A. SCALING WITH SAFEGUARDS FOR DIGITAL NI ACT COURT**

An estimated 4.5 lakh NI Act cases are still pending in Delhi alone; this is the quintessential "production-line" docket. A remote-first approach was introduced with the opening of 34 fully digital NI Courts in May–June 2025. This model included digital summons service, automated scrutiny, AI-assisted cause-list scheduling, and e-filing. This is a chance to gauge automation's fairness, not just for efficiency. With a particular emphasis on SMEs, the foundation of NI Act litigation, the Delhi High Court's quarterly public dashboards should monitor (i) adjournment rates, (ii) average time-to-disposal, (iii) translation accuracy, and (iv) litigant satisfaction.

## **B. POLICE USE OF FACIAL RECOGNITION TECHNOLOGY (FRT)**

Legality and Proof Requirements: Delhi Police have elevated the risks of error and demographic bias in riot investigations by treating FRT matches at 80% similarity as identification, a figure significantly below thresholds used in other jurisdictions. Puttaswamy's proportionality test should be incorporated into evidentiary gatekeeping by courts in the absence of a specific FRT law. Public SOPs for FRT use, demographic-group-specific accuracy metrics, independent audits, required match corroboration, and stringent retention-deletion procedures with logged oversight are a few

examples of interim safeguards. While still being possible under the current Indian procedural law, such measures are in line with international best practices

### **C. COORDINATED URGENCY**

Deepfakes and Platform Accountability MeitY advisories between 2023 and 2024 called on platforms to label AI-generated content, remove deepfakes quickly, and strengthen due diligence for models that haven't been thoroughly tested. A revised advisory from March 2024 raised accountability standards and added labeling requirements. When drafting bail terms, injunctions, and procedural guidelines in cybercrime cases, courts can, and ought to, refer to these obligations. Even before the DPDP Act is completely implemented, this operationalizes AI governance and improves compliance.

### **3. AJR-INDIA (ACCOUNTABLE JUDICIAL REASONING FOR AI): A CONCRETE GOVERNANCE BLUEPRINT**

The EU AI Act protections, Indian constitutional jurisprudence, and OECD AI principles are all adjusted to judicial realities by the following four-pillar framework:

- **Pillar A: Clearly Defined Use-Cases**

a) Green Zone: Registry automation and translation: Document classification, scheduling assistants, and machine translation are allowed by default as long as there is a human involved, error metrics are made public, and AI outputs are not the only factor used to determine rights.

b) Amber Zone: Evidence handling tools: Fact extraction or ranking from case files is permitted only if audit trails, contestability, non-exclusive reliance, and adherence to BSA electronic-record regulations are followed.

c) Red Zone: Analytics that influence outcomes: It is prohibited to use risk scoring, sentencing, or predictive tools to determine guilt, bail, or sentence unless: Training data and source code are discoverable under protective orders; validation on Indian datasets is published; the tool passes

the Puttaswamy-style proportionality & equality impact review; and the weight assigned is explained in a reasoned judicial order.

- **Pillar B: Rights-First Procedural Protections Explainability & Disclosure**

Any party using algorithmic outputs must provide the other side with meaningful expert access to challenge the model's details, limitations, and confidence scores. Due Process in FRT Cases: No one can be arrested or charged based only on a FRT match; full match reports must be disclosed, human verification is required, and non-FRT alternatives must be documented. Data Protection & Purpose Limitation: Agencies are required to adhere to MeitY deepfake/AI labeling advisories and IT Rules due diligence until the DPDP Act is fully implemented. Data Protection Impact Assessments (DPIAs) for court-facing AI tools should be conducted by key data fiduciaries in the delivery of justice after the Act goes into effect.

- **Pillar C: Institutional Architecture Judicial AI Review Board (J-AIRB)**

An eCommittee Phase III-aligned panel of judges, technologists, statisticians, defense attorneys, and prosecutors led by the Supreme Court that accredits AI tools, publishes model cards, and keeps a public registry of authorized versions. Standards for Evidence Technology Cell: to publish Practice Directions on ensuring minimal disclosure packs for legal proceedings and verifying AI-generated artifacts. Independent Audits: Every year, a third party conducts an audit of court-approved AI, providing public summaries and sunset clauses for noncompliant tools. Open Justice, Open Data (with Privacy) is Pillar D. Release corpora of research orders and judgments that have been anonymized and thoroughly de-identified. For legal-domain LLM evaluation, develop an Indian-language challenge set that measures bias across castes, genders, and regions, as well as translation fidelity and hallucination rates, in relation to NJDG transparency goals.

## **4. THE LEGAL CROSSROADS IN FRONT OF INDIA'S PATH FOR JUDICIAL AI WILL BE SHAPED BY THREE OVERLAPPING LEGAL SYSTEMS**

Constitutional protections of equality, free speech, and privacy (Articles 14, 19, and 21); laws that apply to all sectors, such as the DPDP Act and IT Rules; and procedural codes that apply to specific sectors (CrPC, Evidence Act, NI Act). If there is no harmonization, there is a risk of a patchwork where police AI is controlled by general privacy law, and court AI is not tested until someone appeals it. The governance plan above tries to close that gap before it happens.

## **5. CONCLUSION**

Toward an Indian Theory of Reliable Judicial AI Governance of judicial AI is more than just a technological issue; it is an extension of constitutional design. India has the unique chance to create its own rules before AI becomes an unchangeable "black box" in the delivery of justice. India can make sure that AI strengthens, not weakens, the legitimacy of the courts by making every deployment include contestability, transparency, and proportionality. The system can build trust in digital justice from the ground up by making performance metrics public, opening up anonymized legal datasets, and giving oversight bodies more power.