ISSN: 3048-9423(Online)
Naveen International Journal of Multidisciplinary Sciences (NIJMS)
© NIJMS | Vol. 2 | Issue 5 | April-May 2026
Available online at: https://nijms.com/
DOI: https://doi.org/10.71126/nijms.v2i5.128

# Justice in the Age of Algorithms: Artificial Intelligence, Data Privacy, Surveillance, and Digital Evidence in Criminal Adjudication

**Gargi Singh [1] and Dr. Utkarsh Verma[2]**

[1] *Research Scholar, National University of Study and Research in Law (NUSRL), Ranchi*
[2] *Assistant Professor, Law, NUSRL Ranchi*
[1] ***Corresponding Author Email:*** *gargisingh227@gmail.com*
[2]***Author Email:*** *utkarsh.verma@nusrlranchi.ac.in*

***ABSTRACT:***

*The rapid integration of automated and data-driven technologies into criminal justice systems has fundamentally transformed the paradigms of policing, investigation, prosecution, and adjudication. Technologies such as predictive policing tools, facial recognition systems, automated risk assessment instruments, and digital forensics promise efficiency, accuracy, and speed in crime control. However, their deployment raises profound constitutional, legal, and ethical concerns particularly relating to data privacy, structural bias, transparency, and the admissibility and reliability of digitally generated evidence. This research critically examines the governance of artificial intelligence and data-driven technologies in the Indian criminal justice system, focusing on data protection standards, evidentiary challenges, and procedural fairness. Despite significant legislative developments including the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023 India lacks a comprehensive rights-based regulatory framework for data-driven criminal justice technologies. Existing laws remain fragmented and inadequate to address mass surveillance, automated decision-making, structural discrimination in profiling systems, and judicial scrutiny of digitally generated evidence. The study undertakes a comparative analysis of regulatory approaches in the European Union particularly the EU Artificial Intelligence Act, 2024 and the GDPR and the United States' constitutional model. This comparative inquiry highlights significant regulatory lacunae in India, especially regarding accountability, transparency, and constitutional safeguards under Articles 14, 19, and 21 of the Constitution, as interpreted by the Supreme Court in Justice K.S.*

*Puttaswamy (Retd.) v. Union of India. The research concludes by proposing a rights-based regulatory framework for India, emphasising algorithmic transparency, data minimisation, independent audits, and enhanced judicial oversight.*

***Keywords:*** *Artificial Intelligence; Criminal Justice System; Data Privacy; Digital Evidence; Surveillance Technologies; Algorithmic Accountability.*

## 1. INTRODUCTION:

The twenty-first century has witnessed a fundamental transformation in the architecture of criminal justice. Across the world, states deploy an expanding arsenal of data-driven technologies to detect, investigate, prosecute, and adjudicate crime: predictive policing platforms, facial recognition systems, automated biometric databases, and mass surveillance infrastructures capable of aggregating metadata across communications, movement, and financial transactions at a scale unimaginable even a generation ago. India is no exception. If anything, the pace of India's transition to data-driven criminal governance has outrun its legal framework in ways that pose an increasingly urgent constitutional challenge.

The Indian State's investment in technology-assisted criminal justice is substantial and growing. The Crime and Criminal Tracking Network and Systems (CCTNS), now operational across 95 per cent of India's 14,000-plus police stations, serves as the country's primary digitised repository of FIRs and criminal histories. The Interoperable Criminal Justice System (ICJS) 2.0, being upgraded under supervision of the e-Committee of the Supreme Court, integrates CCTNS with e-Courts, e-Prisons, e-Forensics, and e-Prosecution to create a unified data-sharing infrastructure. The National Intelligence Grid (NATGRID), receiving approximately 45,000 queries per month from security agencies, aggregates data across over twenty government and private sources including telecom metadata, immigration records, tax identifiers, and banking transactions. In December 2025, NATGRID launched Gandiva an analytics platform integrating facial recognition with cross-referenced data sources, transforming NATGRID from a passive repository into an active intelligence engine. Predictive policing tools proliferate at the state level: Delhi Police's Crime Mapping, Analytics, and Predictive System (CMAPS); the Smart Prahari platform in Washim, Maharashtra; and AI-enabled drone surveillance for crowd monitoring across Karnataka, Odisha, and Uttar Pradesh.

The breadth of this transformation is matched only by the depth of the regulatory vacuum within which it occurs. India's judicial backlog stands at over 50 million cases as of September 2025, creating institutional pressure to embrace technological acceleration. Yet the legal authority for these deployments rests on a patchwork of statutes the Indian Telegraph Act, 1885, the Information Technology Act, 2000, the Criminal Procedure (Identification) Act, 2022, and the three new criminal laws operative from July 1, 2024 none of which was designed to govern a continuous, population-scale, biometrically-enabled surveillance apparatus. The constitutional dangers are already manifesting: the Delhi High Court issued notice in March 2026 in *Sahibe Alam v. Govt. of NCT of Delhi* arising from coercive biometric collection from un-arrested university students the BNSS, BNS, and BSA operative since July 1, 2024 modernise

criminal procedure without resolving the constitutional standards that must govern digital processes and the Supreme Court's April 2026 Working Sessions on Electronic Evidence signal urgent institutional concern. Comparatively, the EU AI Act (in force August 1, 2024) prohibits real-time biometric identification in public spaces for law enforcement from February 2, 2025, with full high-risk system compliance due August 2, 2026 while *Carpenter v. United States* (2018) marks the US Supreme Court's recognition that digital surveillance is qualitatively different from traditional interception. India, committed to the same constitutional values of dignity and proportionality, has produced no equivalent responses.

This research situates itself at the intersection of criminal law, constitutional law, data protection law, and technology regulation. Three overarching claims animate the analysis: first, India's existing framework is structurally inadequate to govern its operational data-driven criminal justice apparatus; second, the 2023–2025 legislative reforms, while significant, are incomplete modernising procedure without resolving the constitutional standards governing its exercise; third, the EU's proactive, rights-embedding regulatory model provides a more appropriate comparative template for India than the US ex post litigation model, adapted to India's constitutional architecture and the specific vulnerabilities of its marginalised communities. The paper proceeds: Part II (conceptual foundations); Part III (mapping automated technologies across the criminal process); Part IV (constitutional dimensions); Part V (data protection and surveillance); Part VI (comparative analysis); Part VII (structural discrimination); Part VIII (global trends); Part IX (regulatory framework); Part X (conclusion); and Part XI (recommendations).

## 2. CONCEPTUAL AND THEORETICAL FOUNDATIONS

The deployment of automated technologies in criminal justice must be understood through critical conceptual distinctions carrying direct legal significance. 'Narrow' AI specialised systems for facial recognition, predictive policing, and risk assessment is the form currently integrated into criminal justice systems; 'General' AI, involving autonomous reasoning, remains theoretical but has already prompted scholarship on accountability and the limits of algorithmic sovereignty.

Of particular doctrinal importance is the distinction between Automated Decision Systems (ADS) and Decision Support Systems (DSS). ADS operate without meaningful human intervention to produce binding determinations affecting liberty bail recommendations, risk scores feeding judicial decisions. DSS assist but do not supplant human judgment. ADS applications in criminal adjudication implicate heightened constitutional scrutiny because they operationalise state power over individual liberty through processes inherently opaque and immune to ordinary accountability mechanisms.

Algorithmic Governance Theory posits that automated systems do not merely process data but actively construct social order through risk classifications and predictive categorisations. Predictive policing thus creates structural harms: by operationalising historical patterns of over-policing into forward-looking predictions, algorithmic systems encode discrimination into the infrastructure of criminal justice. Surveillance Capitalism, as theorised by Zuboff, provides a socio-legal account of how commodification of personal data reconstitutes citizen-state relations in ways that undermine autonomy

and consent. Digital Constitutionalism offers the normative counter-movement: constitutional rights must be actively applied to digital spaces, and state technological systems must satisfy the same tests of legality, necessity, and proportionality as any other intrusion into fundamental rights.

## 3. MAPPING AUTOMATED TECHNOLOGIES ACROSS THE CRIMINAL JUSTICE PROCESS IN INDIA

### A. Policing and Investigation

In the policing domain, predictive policing tools including CMAPS in Delhi, hotspot policing systems in Hyderabad and Mumbai, and drone surveillance across multiple states rely upon FIR data and historical crime statistics to forecast criminal concentration. The fundamental epistemological flaw is that these systems train on data generated by prior policing practices that themselves reflect structural patterns of over-policing in disadvantaged and minority communities. Predictive models thus construct self-validating feedback loops: algorithmic predictions lead to intensified policing, generating more arrests, reinforcing predictions, justifying further policing. The algorithm does not detect crime; it reproduces and legitimises discriminatory policing practice through the veneer of computational objectivity.

The National Automated Facial Recognition System (AFRS) presents an acute constitutional problem. The Delhi High Court's experience in *Sadhan Haldar v. State (NCT of Delhi)* demonstrated that of 10,617 system matches for missing children, only 3,202 were verified a false positive rate that, if replicated in criminal identification contexts, could cause wrongful arrest at constitutionally unconscionable scale. NIST studies consistently document facial recognition algorithms exhibiting significantly higher error rates for darker-skinned individuals and women, raising specific concerns about discriminatory application against India's marginalised communities. The CPIA 2022 authorises biometric collection from arrested, convicted, and even acquitted persons alike retaining data for seventy-five years compounding these constitutional anxieties. The Act's breadth appears irreconcilable with the *Aadhaar* judgment's requirement that state biometric collection satisfy proportionality and purpose limitation. This confrontation is live: in *Sahibe Alam v. Govt. of NCT of Delhi* (W.P. (Crl.) 672/2026), the Delhi High Court issued notice in March 2026 on precisely these grounds.

### B. Investigation and Digital Forensics

At the investigation stage, digital forensic tools perform device decryption, deleted document reconstruction, facial and voice pattern matching, and large-scale metadata analysis from call detail records and social media platforms. However, the admissibility of such evidence raises unresolved doctrinal questions. The Supreme Court's authoritative rulings in *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* established that strict Section 65B compliance is a prerequisite for electronic records' admission. Section 63 of the BSA 2023 builds upon this by requiring a dual-authentication certificate signed by both the device operator and an independent expert with hash value verification. The Kerala High Court in *Alukas Jewellery v. Anil* (July 17, 2025) reiterated that absence of certification is 'only a curable defect,' reflecting continuing doctrinal uncertainty the Supreme Court must resolve. A critical lacuna is that the BSA leaves 'expert' undefined, creating inconsistent standards across courts. The Supreme Court's April 2026 Working Sessions on Electronic Evidence and

Criminal Justice Reforms, chaired by Justices B.V. Nagarathna and Rajesh Bindal, signal institutional recognition that the digital evidence framework requires authoritative clarification.

When an accused seeks to challenge digitally generated evidence a facial recognition match, a risk score, or a forensic output the inability to access, understand, or cross-examine the underlying system constitutes a structural violation of the fair trial rights guaranteed under Articles 14 and 21. The system cannot be sworn in, cross-examined, or impeached. It cannot account for its training data, error rates in the relevant demographic context, or embedded assumptions. This asymmetry of information is not correctable by the adversarial process without specific legislative intervention.

### C. Prosecution and Adjudication

The American experience with algorithmic risk assessment in sentencing epitomised by the COMPAS system in *State v. Loomis* illustrates the constitutional hazards of algorithmic scores in sentencing without transparency or contestability. In India, the introduction of risk assessment into sentencing would require confrontation with Article 21's guarantee of personal liberty, the presumption of innocence, and the principle of individualised sentencing. Risk scores derived from group-level statistics would violate Indian criminal jurisprudence's constitutional core.

## 4. CONSTITUTIONAL DIMENSIONS OF AUTOMATED TECHNOLOGIES IN CRIMINAL JUSTICE

The constitutional framework is structured around Articles 14, 19, and 21. The landmark *Puttaswamy* judgment overruled *M.P. Sharma* and *Kharak Singh*, establishing privacy as a fundamental constitutional right and articulating the four-part proportionality test legality, legitimate aim, necessity, and proportionality for any state intrusion into personal information.

Article 14's guarantee of non-arbitrariness is directly implicated by automated decision-making that lacks transparency and intelligibility. Where a bail decision or investigative determination is produced by a system whose logic cannot be understood, explained, or scrutinised, the state's action is inherently arbitrary in the constitutional sense not the product of reason and law but of computational process that substitutes for reason without being reason. Article 19's protection of fundamental freedoms is threatened by mass automated surveillance producing a 'chilling effect.' The Supreme Court's reasoning in *Shreya Singhal v. Union of India* that digital expression laws must be narrowly drawn to avoid chilling constitutional freedoms applies equally to surveillance systems tracking, profiling, and predicting citizens exercising Article 19 rights. *Anuradha Bhasin v. Union of India* anchors internet access as a fundamental right. Most recently, *Kunal Kamra v. Union of India* demonstrates the chilling effect doctrine's continuing vitality as a constitutional constraint on digital governance.

## 5. DATA PROTECTION AND THE SURVEILLANCE FRAMEWORK

The DPDP Act, 2023 represents India's first comprehensive statutory framework for personal data regulation, establishing data fiduciary obligations encompassing purpose limitation, data minimisation, storage limitation, and security requirements. However, Section 17's sweeping exemptions for state processing covering sovereignty, national security, and law enforcement create a regulatory regime structurally incapable of providing meaningful protection against data-driven criminal justice

surveillance. The constitutional challenge filed in February 2026 by the Reporters' Collective highlights a structural paradox at the core of India's data governance architecture: a statute nominally enacted to protect privacy simultaneously enables surveillance and erodes transparency by amending RTI disclosure provisions.

The surveillance framework resting on Section 5(2) of the Telegraph Act, 1885 and Section 69 of the IT Act, 2000 was designed for point-in-time communications interception and is wholly inadequate to govern continuous, population-scale digital surveillance aggregating metadata across communications, location data, biometric records, and behavioural patterns. The DPDP Rules 2025, notified November 14, 2025, introduce DPIA obligations for Significant Data Fiduciaries, algorithmic fairness assessments, and 72-hour breach notification requirements. However, their broad state exemptions mean law enforcement agencies engaged in mass biometric surveillance remain substantially outside accountability architecture. A critical gap compared to the EU GDPR is the absence of any DPIA requirement for high-risk processing or equivalent algorithmic impact assessment for criminal justice contexts. The GDPR provides, under Article 22, for the right not to be subject to solely automated decisions with significant legal effects. No equivalent provision exists in Indian law.

## 6. COMPARATIVE REGULATORY APPROACHES: EU AND UNITED STATES

### A. The European Union Framework

The EU AI Act, in force August 1, 2024, establishes the world's first comprehensive horizontal regulatory framework for AI. Its Annex III classifies AI systems used in law enforcement including risk assessments, predictive policing, criminal profiling, and judicial decision support as 'high-risk,' subjecting them to mandatory fundamental rights impact assessments, transparency and explainability obligations, human oversight requirements, and EU-wide database registration. Article 5 prohibits certain practices inherently incompatible with fundamental rights, including real-time remote biometric identification in public spaces for law enforcement and social scoring. These prohibitions were enforceable from February 2, 2025; full high-risk system compliance obligations apply from August 2, 2026. The EU framework is complemented by GDPR Articles 22 and 35, creating an algorithmic accountability regime that India's DPDP Act conspicuously lacks.

### B. The United States Framework

The United States lacks a federal AI governance framework, relying on constitutional principles and sectoral statutes. In *Carpenter v. United States*, the Supreme Court's holding that warrantless acquisition of comprehensive digital location data violates the Fourth Amendment marked a decisive doctrinal shift the Court rejected the third-party doctrine as applied to digital data enabling 'near perfect surveillance' of a person's entire life. *State v. Loomis* represents the American system's most prominent encounter with algorithmic criminal adjudication: the Wisconsin Supreme Court's permission of a proprietary risk score while cautioning against sole reliance has been widely criticised for failing to resolve the fundamental due process deficiency. The comparative analysis reveals a divergence with direct implications for India: the EU's precautionary, ex ante regulatory framework contrasts with the US ex

post constitutional litigation model. India should draw from the EU's proactive approach while adapting it to India's constitutional architecture.

## 7. ALGORITHMIC BIAS, STRUCTURAL DISCRIMINATION, AND EQUAL PROTECTION

Algorithmic bias in criminal justice is not incidental but structural, rooted in the data on which systems train. NIST's comprehensive facial recognition study documented false positive rates for darker-skinned individuals at 10 to 100 times those for lighter-skinned individuals, with particularly acute disparities for women. In India, where marginalised communities Dalits, Adivasis, minorities, lower-income populations have historically been subject to disproportionate policing and criminalisation, the risk of algorithmic systems reproducing and amplifying structural inequalities is not hypothetical but demonstrable. Predictive policing models are particularly susceptible to feedback loop dynamics: systems trained on historical arrest data, which reflects prior policing deployment rather than objective criminal activity, perpetually predict high crime in already-over-policed areas, justifying further intensified policing.

Under the transformative reading of Article 14 in *Navtej Singh Johar v. Union of India*, algorithmic systems that reproduce structural discrimination even without discriminatory intent may constitute a violation of the equality guarantee. The principle that facially neutral practices systematically disadvantaging marginalised groups may be unconstitutional under Article 14 extends naturally to algorithmic systems achieving the same effect through mathematically sophisticated classifications. The Supreme Court's bail guidelines in *Satender Kumar Antil v. Central Bureau of Investigation* emphasise the constitutional imperative of individualised bail determinations a principle directly subverted by algorithmic risk scores substituting group-level statistical generalisations for individualised assessment.

## 8. EMERGING GLOBAL TRENDS AND INTERNATIONAL OBLIGATIONS

At the international level, the governance of automated technologies in criminal justice is increasingly shaped by normative frameworks from the UN, OECD, and specialised bodies addressing cross-border criminal justice cooperation. These frameworks converge on common principles human oversight, accountability, transparency, non-discrimination, and data protection that India has endorsed in diplomatic fora but not systematically incorporated into domestic legal architecture. Where a system deployed by the state causes harm wrongful arrest, discriminatory profiling, false conviction the question of civil and constitutional liability between developer, deploying agency, and state has not been resolved in Indian law. Article 300 of the Constitution and the doctrine of tortious state liability provide a foundation for constitutional tort claims arising from automated system-induced harm, but legislative clarity is urgently needed. AI regulatory sandboxes pre-deployment controlled testing environments have been adopted in the UK and are under EU consideration as mechanisms for bias testing, accuracy validation, and human rights impact assessment. A similar framework in India would provide structured pre-deployment validation before automated systems affect the liberty of any individual.

## 9. TOWARDS A RIGHTS-BASED REGULATORY FRAMEWORK FOR INDIA

Drawing upon the constitutional analysis, comparative review, and doctrinal critique undertaken above, this Part proposes a five-pillar framework. First, constitutional anchoring: all automated systems deployed in criminal justice must be governed by statutory authorisation satisfying the *Puttaswamy* proportionality test. Judicial warrants must be required for activation of surveillance tools targeting individuals; no automated system should impose any liberty-restricting measure without human authorisation subject to review. Second, evidentiary reform: Section 63 of the BSA should be extended by parliamentary enactment to require (i) disclosure of system architecture, training data characteristics, and validated error rates; (ii) demographic performance data across the accused's population characteristics; (iii) an explanation of the output contestable by the accused and court; and (iv) independent expert certification by a body designated by the judiciary rather than the investigating agency. Third, algorithmic accountability legislation: Parliament must enact a dedicated Digital Criminal Justice Regulation Act mandating impact assessments, independent bias audits with published results, and enforceable rights for individuals adversely affected. Fourth, independent regulatory oversight: a Digital Criminal Justice Regulatory Authority, independent of the Ministry of Home Affairs, should conduct pre-deployment approvals, compliance audits, transparency reporting, and adjudication of complaints. Fifth, parliamentary oversight and periodic review: the regulatory framework must incorporate built-in parliamentary review at minimum every three years, with mandatory sunset clauses and active reauthorisation requirements, drawing upon OECD and UN normative frameworks to ensure consonance with international human rights standards.

## 10. CONCLUSION

The data-driven state is no longer a distant prospect; it is an entrenched reality in India's criminal justice system. The legislative developments of 2023–2025 represent a pivotal moment. The BNSS, BNS, and BSA operative from July 1, 2024 constitute the most significant restructuring of India's criminal procedure and evidence law in a generation. The DPDP Act and DPDP Rules 2025, operationalised on November 14, 2025, establish India's first comprehensive data governance framework. The Supreme Court Criminal Procedure Rules 2026 advance procedural digitisation. Yet each of these reforms embeds structural weaknesses: the DPDP Act's Section 17 exemptions insulate the most consequential surveillance power from accountability; the BSA's undefined 'expert' creates inconsistent evidentiary standards; and the BNSS authorises digital processes without specifying their constitutional standards. The CPIA 2022's 75-year retention period for biometric data from acquitted persons and DPDP Rules' broad state exemptions compound these concerns. The EU AI Act's phased enforcement prohibitions from February 2025, full high-risk compliance from August 2026 presents an imminent international benchmark against which India's governance gaps are becoming conspicuous. The constitutional challenges now before India's courts *Sahibe Alam* at the Delhi High Court and the Reporters' Collective challenge at the Supreme Court represent opportunities for the judiciary to lay down the constitutional standards that legislation has not yet provided. Without the legislative and institutional reforms proposed in this paper, India's technological revolution in criminal justice risks becoming an engine for the

reproduction of inequality, the entrenchment of surveillance, and the systematic erosion of rights the Constitution mandates be protected. A constitutional state that claims to enforce the rule of law must, above all, be bound by it.

## 11. RECOMMENDATIONS

### A. Legislative Recommendations

1. Enact a Digital Surveillance Oversight Act. Parliament must enact a comprehensive statute governing automated surveillance technologies in law enforcement, requiring prior judicial authorisation for targeting individuals, mandatory fundamental rights impact assessments, and sunset clauses requiring periodic reauthorisation. This legislation must supersede the inadequate framework constituted by the Telegraph Act, 1885 and IT Act, 2000.

2. Amend the CPIA 2022. The Act must be amended to restrict biometric collection to convicted persons, prohibit collection from acquitted or un-arrested individuals, reduce retention to a proportionate period, establish an independent NCRB audit body, and create a statutory right to erasure upon acquittal. Pending amendment, interim administrative guidelines should restrict biometric collection to situations of formal arrest under the BNSS, as evidenced as necessary by *Sahibe Alam*.

3. Amend DPDP Act, 2023 and DPDP Rules, 2025. Section 17 exemptions for state data processing must be narrowed to satisfy the *Puttaswamy* proportionality test. Rules must extend DPIA obligations explicitly to law enforcement agencies, require fairness assessments as preconditions for automated profiling tools, and guarantee individuals a statutory right to be informed when an automated system contributed to a liberty-affecting decision. The RTI-weakening provisions must be reversed.

4. Strengthen the Section 63 BSA Framework. Parliament must define 'expert' for Part B certification, empower courts to appoint independent forensic experts at state expense, and accompany the hash value requirement with standardised protocols for the forensic tools used so that non-standardised methods do not defeat legitimate evidentiary challenges.

5. Enact a Facial Recognition and Biometric Surveillance Regulation Act. Given that more than twenty state police forces have deployed facial recognition without legislative authorisation or judicial oversight, Parliament must urgently enact a standalone statute requiring: legislative authorisation and mandatory rights impact assessments before any system deployment; prohibition on real-time mass identification in public spaces absent a specific judicial order; minimum accuracy and bias-testing standards disaggregated by demographic group; and civil liability for false matches resulting in wrongful detention.

### B. Judicial Recommendations

6. Supreme Court Guidelines on Digital Evidence. Building on the April 2026 Working Sessions, the Supreme Court should issue comprehensive guidelines on the standards of admissibility, authentication, and contestability of digital evidence in criminal proceedings specifying expert witness

qualifications, minimum disclosure obligations where prosecution relies on automated outputs, and chain of custody standards for biometric or metadata-sourced evidence.

7. Establish a Digital Forensics Reference Panel. The Supreme Court's E-Committee should constitute a permanent Panel comprising forensic scientists, data protection specialists, and civil society technologists to advise courts on technical dimensions of digital evidence disputes, review accuracy and bias characteristics of law enforcement tools, and publish annual reports on digital evidence standards.

8. Comprehensive CPIA Constitutional Adjudication. The Delhi High Court's notice in *Sahibe Alam* (W.P. (Crl.) 672/2026) should be treated as an occasion for comprehensive constitutional adjudication, laying down enforceable standards grounded in *Puttaswamy* proportionality and Article 20(3) governing every stage of biometric data collection, storage, sharing, and deletion in the criminal justice context.

**C. Executive and Institutional Recommendations**

9. Establish an Independent Technology Audit Authority with powers to review and certify bias-testing results before deployment, conduct annual NAFRS audits with published demographic accuracy statistics, and receive and investigate complaints from individuals whose liberty has been affected by inaccurate or discriminatory automated systems.

10. Mandate Training for Investigating Officers and Prosecutors on Section 63 BSA certification and hash value protocols, lawful limits on biometric collection under the CPIA and constitutional standards, chain of custody obligations under the Supreme Court Criminal Procedure Rules 2026, and the constitutional right to privacy as applied to investigative data gathering.

11. Adopt a Pre-Deployment Regulatory Sandbox for automated criminal justice tools modelled on the UK ICO sandbox programme including independent demographic bias testing, a Fundamental Rights Impact Assessment with civil society participation, and judicial notification prior to first operational use. No automated tool should affect the liberty of any individual without clearing this pre-deployment validation framework.

12. Pursue International Cooperation to domestically incorporate accountability standards from the OECD AI Principles, the UN Special Rapporteur's guidelines on surveillance and privacy, and the Council of Europe Framework Convention on Artificial Intelligence. The DPDP Rules' restrictions on cross-border data transfers provide a starting point, but law enforcement data flows require separate and more stringent treatment given the liberty interests at stake.

# REFERENCES

[1] Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India), §§ 61–65 (electronic records framework); Ministry of Law and Justice, Notification No. S.O. 2116(E) (June 26, 2024) (notifying July 1, 2024 as date of commencement).

[2] Digital Personal Data Protection Act, No. 22 of 2023 (India) [hereinafter DPDP Act]; Ministry of Electronics and Information Technology, The Digital Personal Data Protection Rules, 2025, G.S.R. 747(E) (Nov. 14, 2025) [hereinafter DPDP Rules 2025].

[3] See Reporters' Collective v. Union of India, W.P. (C) No. 130/2026 (S.C. India) (constitutional challenge to DPDP Act §§ 8(1)(j) and 44(3) for curtailing RTI transparency disclosures and enabling mass surveillance).

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter Puttaswamy] (nine-judge bench unanimously recognising privacy as a fundamental right under Article 21 and articulating a four-part proportionality test).

[5] Ministry of Law and Justice, Press Release: Integration of AI in Crime Detection, Surveillance and Criminal Investigations (Feb. 25, 2025); National Crime Records Bureau, Annual Report on CCTNS Implementation 2024–25 (2025) (noting 95% operational coverage across 14,000+ police stations).

[6] Ministry of Home Affairs, NATGRID: Capability Overview (2025); Software Freedom Law Centre India, Artificial Intelligence and Surveillance in India: 2025 Roundup (Jan. 15, 2026) [hereinafter SFLC 2025 Roundup] (documenting NATGRID's 45,000 monthly queries and the December 2025 Gandiva launch).

[7] SFLC 2025 Roundup, supra note 6; Shailendra Kumar & Priya Nair, Predictive Policing, AI Surveillance, and Privacy in India: A Legal Analysis Under the DPDP Act 2023, 4 Int'l J. Trends Emerging Rsch. & Dev. 112, 118–20 (2025) (documenting Smart Prahari in Washim, Maharashtra and CMAPS deployment in Delhi).

[8] Oxford Institute of Technology and Justice, India: Increasing Use of AI Across the Justice System (Sept. 2025) (noting judicial backlog exceeding 50 million cases as of September 2025).

[9] Sahibe Alam v. Govt. of NCT of Delhi, W.P. (Crl.) 672/2026 (Del. H.C. 2026) (Delhi High Court issued notice in March 2026 on constitutional challenge to Criminal Procedure (Identification) Act, 2022, arising from coercive biometric collection from un-arrested university students).

[10] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023 (India) [hereinafter BNSS]; Bharatiya Nyaya Sanhita, No. 45 of 2023 (India) [hereinafter BNS]; Ministry of Home Affairs, Inter-Operable Criminal Justice System (ICJS) 2.0: Project Overview (2024) (describing ICJS integration architecture under e-Committee of the Supreme Court's Data Sharing Matrix).

[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1 [hereinafter EU AI Act]; art. 5(1)(d) (prohibiting real-time remote biometric identification in public spaces for law enforcement); arts. 6(2), Annex III (classifying law-enforcement risk tools as high-risk).

[12] Carpenter v. United States, 585 U.S. 296, 138 S. Ct. 2206, 2217–18 (2018) (holding that warrantless acquisition of seven days of CSLI data violates the Fourth Amendment; rejecting third-party doctrine as applied to 'near perfect surveillance').

[13] Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, 51 U.C. Davis L. Rev. 399, 421–23 (2017); Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 14–15 (2015) (theorising algorithmic governance as construction rather than mere processing of social order).

[14] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 7–9 (2018); Bernard Harcourt, Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age 190–94 (2007) (documenting self-validating feedback loops in predictive policing).

[15] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 93–95 (2019); Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society 45–48 (2022).

[16] SFLC 2025 Roundup, supra note 6, at 4–5; Tracing the Rise of Predictive Policing in India, SFLC India (Feb. 26, 2026) (documenting hotspot policing in Delhi, Hyderabad, and Mumbai; AI-enabled drone surveillance in Karnataka, Odisha, and Uttar Pradesh; and twenty state-level AFRS deployments).

[17] Sadhan Haldar v. State (NCT of Delhi), W.P. (Crl.) 1/2016 (Del. H.C. 2016) (out of 10,617 AFRS matches for missing children, only 3,202 verified); Patrick Grother et al., Nat'l Inst. of Standards & Tech., NISTIR 8280: Face Recognition Vendor Testing (FRVT) Part 3: Demographic Effects 8–11 (2019) [hereinafter NIST FRVT] (documenting false-positive rates 10–100× higher for darker-skinned individuals and women).

[18] Criminal Procedure (Identification) Act, No. 11 of 2022 (India) [hereinafter CPIA], § 3 (authorising biometric collection from arrested, convicted, and acquitted persons); § 8 (75-year retention period).

[19] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2018) 16 SCC 409 [hereinafter Aadhaar Judgment] (holding that biometric data collection must satisfy purpose limitation and data minimisation as conditions of constitutional proportionality).

[20] Sahibe Alam v. Govt. of NCT of Delhi, W.P. (Crl.) 672/2026 (Del. H.C.) (noting that police officers at Nehru Place Cyber Cell coerced biometric submissions from Jamia Millia students who had not been arrested; court issued notice Mar. 2026).

[21] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India) (holding electronic records inadmissible without strict compliance with § 65B certificate requirement); Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 3 SCC 216 (India) [hereinafter Arjun Panditrao] (reaffirming Anvar and overruling Shafhi Mohammad on necessity exception).

[22] Bharatiya Sakshya Adhiniyam § 63(4) (requiring certificate signed by (a) person in charge of device and (b) an independent expert, in the prescribed schedule format); § 61 (providing that no electronic record shall be denied admissibility solely by virtue of being digital).

[23] Alukas Jewellery v. Anil, Crl. Rev. Pet. No. 512/2025 (Ker. H.C. July 17, 2025) (reiterating that absence of § 63 certificate is 'only a curable defect' relating to mode of proof, not admissibility per se; tension with Arjun Panditrao noted by commentators).

[24] Sathya Narayanan Subramanian, From Section 65B to Section 63(4)(c): The Evolution of Electronic Evidence in Indian Law (2024); Evidence in the Digital Era: Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, 4 Int'l J. Hum. Rts. L. Rev. 206, 212–13 (2025) (noting absence of definition of 'expert' and need for standardised hash-value verification protocols).

[25] Supreme Court of India, Working Session III on Electronic Evidence and Criminal Justice Reforms (Apr. 11, 2026) (chaired by Justice B.V. Nagarathna; Working Session IV on Electronic Records and Judicial Reforms chaired by Justice Rajesh Bindal, Apr. 12, 2026).

[26] State v. Loomis, 881 N.W.2d 749, 768–70 (Wis. 2016) (permitting COMPAS risk score in sentencing while cautioning against sole reliance; widely criticised for failing to resolve due process deficiencies in proprietary algorithm disclosure).

[27] India CONST. art. 21 (right to life and personal liberty, interpreted to include privacy, dignity, and fair trial rights); see also Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (holding 'procedure established by law' requires fairness, not mere legality).

[28] India CONST. art. 14 (equality before law and equal protection); E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 (establishing non-arbitrariness as the core content of Article 14 in administrative and quasi-judicial action).

[29] India CONST. art. 19(1)(a)–(d) (freedoms of expression, assembly, association, and movement); M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (earlier decision declining to recognise privacy as fundamental right, subsequently overruled by Puttaswamy); Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (same).

[30] Puttaswamy, supra note 4, ¶¶ 180–85 (Chandrachud, J.) (articulating four-part test: (i) legality—law in force; (ii) legitimate state aim; (iii) necessity—least intrusive means; (iv) proportionality—balance between restriction and object).

[31] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India) (striking down § 66A of the IT Act as unconstitutional; holding digital communication laws must be narrowly drawn to avoid chilling constitutionally protected expression).

[32] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India) (recognising access to internet and freedom of press through internet as fundamental rights under Articles 19(1)(a) and (g); proportionality review required for internet shutdowns).

[33] Kunal Kamra v. Union of India, W.P. (C) 220/2023 (Bom. H.C. 2024) (striking down Information Technology (Intermediary Guidelines) Amendment Rules, 2023 establishing government Fact Check Unit as violative of Article 19(1)(a); demonstrating ongoing vitality of chilling effect doctrine in digital governance).

[34] DPDP Act § 17(2)(a)–(b) (exempting state processing of personal data for security of state, public order, prevention of offences, and related purposes from data principal rights and fiduciary obligations); § 17(3) (Central Government may exempt specified data fiduciaries by notification).

[35] Reporters' Collective v. Union of India, W.P. (C) No. 130/2026 (S.C.) (challenging DPDP Act § 44(3), which amends § 8(1)(j) of the Right to Information Act, 2005 to restrict disclosure of personal information, thereby reducing RTI transparency).

[36] Indian Telegraph Act, 1885, § 5(2) (authorising interception of communications on grounds of public emergency or public safety); Information Technology Act, 2000, § 69 (empowering state to intercept, monitor, or decrypt information); People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301 (laying down procedural safeguards for telephone tapping).

[37] Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data, 2016 O.J. (L 119) 1 [hereinafter GDPR], art. 22 (right not to be subject to solely automated decisions producing significant legal effects); art. 35 (mandatory data protection impact assessments for high-risk processing).

[38] EU AI Act, supra note 11, art. 5(1)(a) (prohibition on subliminal manipulation); art. 5(1)(b) (prohibition on exploitation of vulnerabilities); art. 5(1)(d) (prohibition on real-time remote biometric identification for law

enforcement in public spaces, subject to exhaustive exceptions); art. 5(1)(e) (prohibition on emotion recognition in law enforcement contexts).

[39] EU AI Act arts. 9–17 (risk management, data governance, technical documentation, transparency, human oversight obligations for providers of high-risk AI systems); art. 49 (EU database registration); EU AI Act compliance obligations for high-risk systems fully enforceable from August 2, 2026.

[40] European Commission, Proposal for a Regulation on Artificial Intelligence Liability, COM (2022) 496 final (Sept. 28, 2022); EU AI Act Omnibus proposal (Nov. 2025) (proposing extended compliance timelines for certain high-risk systems to late 2027, not yet enacted into law as of June 2026).

[41] Carpenter, supra note 12, at 2218–19 (Roberts, C.J.) (holding that 'seismic shifts in digital technology' require rethinking third-party doctrine; CSLI data enabling 'near perfect surveillance' of entire life distinguishable from records voluntarily conveyed to third parties).

[42] State v. Loomis, 881 N.W.2d at 767–70 (finding no due process violation in use of COMPAS score where court stated it was not sole basis for sentence; scholars argue this fails to address asymmetry of access to methodology). See also Julia Dressel & Hany Farid, The Accuracy, Fairness, and Limits of Predicting Recidivism, 4 Sci. Advances 1, 3–4 (2018).

[43] NIST FRVT, supra note 17, at 8–11 (documenting false-positive rates 10–100× higher for darker-skinned individuals; highest error rates for Black and Asian females); see also Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Mach. Learning Rsch. 1, 7–9 (2018).

[44] Harcourt, supra note 14, at 200–05 (explaining ratchet effect: predictive deployment generates more enforcement in already-over-policed areas, reinforcing algorithmic predictions); see also Rashida Richardson et al., Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. Online 192, 202–08 (2019).

[45] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, ¶¶ 234–37 (India) (Chandrachud, J., concurring) (articulating transformative constitutionalism under Article 14; holding that facially neutral state action that entrenches structural discrimination against marginalised groups may violate equality guarantee even absent discriminatory intent).

[46] Satender Kumar Antil v. Central Bureau of Investigation, (2022) 10 SCC 51 (India) (Supreme Court issuing comprehensive bail guidelines; emphasising individualised assessment and constitutional imperative against mechanical application of risk criteria; directing Courts and investigating agencies to follow prescribed procedures).

[47] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019) (establishing principles of transparency, accountability, robustness, security, and human-centred values); United Nations Human Rights Council, Report of the Special Rapporteur on the Right to Privacy, A/HRC/46/37 (Jan. 19, 2021) (addressing surveillance and privacy in the digital age).

[48] India CONST. art. 300 (suits by and against Government of India); State of Rajasthan v. Mst. Vidhyawati, AIR 1962 SC 933 (establishing vicarious state liability in tort); see also Common Cause (A Registered Society) v. Union of India, (2018) 5 SCC 1 (right to die with dignity as incident of Article 21; expanding scope of constitutional tort).

[49] Puttaswamy, supra note 4, ¶¶ 325–30 (Kaul, J., concurring) (proposing warrant requirement for state surveillance targeting individuals; criticising absence of independent judicial oversight for mass data collection programs); see also Selvi v. State of Karnataka, (2010) 7 SCC 263 (holding narco-analysis, polygraph, and brain-mapping on non-consenting subjects unconstitutional under Articles 20(3) and 21).

[50] Bharatiya Sakshya Adhiniyam §§ 61, 63(4) (combined reading); Supreme Court Working Sessions, supra note 25; National Forensic Sciences University Act, No. 32 of 2020 (India) (establishing NFSU as apex body for forensic science education and research; relevant to definition of 'expert' for § 63(4) certification purposes).

[51] Arjun Panditrao, supra note 21, ¶¶ 23–26 (emphasising that certificate under § 65B/§ 63(4) must be filed at the time of production of electronic evidence, not as an afterthought; right of accused to contest certificate is an incident of fair trial under Articles 14 and 21).

[52] Delhi High Court, Launch of Mobile App, e-HRMS Portal, and Digital Preservation of Judicial Records (Sept. 5, 2025) (Chief Justice Devendra Kumar Upadhyaya and Justice Vikram Nath presiding; part of e-Courts Phase III initiatives); Supreme Court E-Committee, Report on Phase III of e-Courts Project (2024).

[53] Supreme Court Criminal Procedure Rules 2026 (introducing mandatory e-filing, video-conference hearings, digital evidence submission protocols, and victim-identity protection; promulgated under Article 145 of the Constitution).

[54] CPIA, supra note 18, § 4(1) (permitting collection from 'any person' who has been arrested in connection with any offence punishable with imprisonment for one year or more); § 8 (retention up to 75 years or until date of death); contrast Aadhaar Judgment, supra note 19 (requiring purpose limitation and proportionality for state biometric collection).

[55] DPDP Act § 17(2); DPDP Rules 2025, Rule 3(1)(b); see Arindrajit Basu & Elonnai Hickok, The Surveillance State: A Comparative Analysis of the Chinese and Indian Personal Data Protection Frameworks 45 (2019) (critiquing structural exemptions that reproduce surveillance capacity within rights-protection frameworks).

[56] EU AI Act art. 5(1)(d); see also Information Commissioner's Office (UK), Regulatory Sandbox: Annual Report 2024–25 (2025) (documenting sandbox programme for pre-deployment testing of high-risk AI tools including law enforcement applications); European Commission, AI Regulatory Sandbox Guidelines (Aug. 2025).

[57] Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225, 2024) [hereinafter CoE AI Convention]; OECD AI Principles, supra note 48; UN Human Rights Council Res. 51/27, Right to Privacy in the Digital Age, U.N. Doc. A/HRC/RES/51/27 (Oct. 7, 2022).

## *Cite this Article:*

***Gargi Singh and Dr. Utkarsh Verma*,"*Justice in the Age of Algorithms: Artificial Intelligence, Data Privacy, Surveillance, and Digital Evidence in Criminal Adjudication*", *Naveen International Journal of Multidisciplinary Sciences (NIJMS), ISSN: 3048-9423 (Online), Volume 2, Issue 5, pp. 31-45, April-May 2026.***

*Journal URL: https://nijms.com/*

***DOI:*** *https://doi.org/10.71126/nijms.v2i5.128*