

From Human Judgement To Algorithmic Decision Making: A Comparative Analysis of AI, Criminal Justice And Rule of Law

Original Research Article | Volume 1 | Issue 4 | 2026 | Article Number: 072

Accepted: 05 September 2026 | Published: 10 September 2026 | ISSN: 2979-8582 (Online)



Crossref : <https://doi.org/10.67693/BJCR-UEZZNMYL>



Pooja Hrishikesh Deo

Deccan Education Society, Shri Navalmal Firodia Law College Pune, India

Correspondence: Pooja Hrishikesh Deo, vaidyapoo@gmail.com

Abstract

Artificial intelligence is progressively reshaping how criminal justice systems function, supporting police forces, prosecutors and courts through tools such as predictive policing, facial recognition, evidence review, risk scoring and judicial decision-support. While these algorithmic tools offer the promise of speed, uniformity and evidence-driven outcomes, their expanding role in decisions that affect personal freedom raises core concerns about lawfulness, equal treatment, fair process, openness, accountability and adherence to the rule of law. The shift away from purely human judgment toward machine-assisted decision-making is thus more than a technical upgrade; it signals a deeper change in how public authority is exercised and distributed. This paper undertakes a comparative study of AI's place in criminal justice by analyzing the legal and regulatory frameworks of India, the European Union, the United States and the United Kingdom. It asks whether algorithm-based decisions can meet established rule-of-law standards, given that such systems are often opaque, probabilistic in nature, shielded by commercial confidentiality, or built on datasets carrying historical bias. The analysis focuses closely on predictive policing, algorithmic risk assessment tools, facial recognition technology, AI-supported evidence analysis and judicial decision-support systems. The central argument advanced here is that the deeper legal risk is not simply machines displacing human decision-makers, but rather that human discretion may become obscured inside technical systems that resist scrutiny, challenge or clear lines of responsibility. Building on this analysis, the paper proposes a "Human-Centred Algorithmic Criminal Justice Model" grounded in principles of legality, proportionality, non-discrimination, transparency, explainability, human oversight, independent auditing and access to effective remedies. It contends that AI ought to function as a supporting, accountable tool in the decision-making process, not as an independent source of coercive authority in matters touching on life, liberty and the right to a fair trial. The comparative review shows that each jurisdiction's approach contributes something valuable yet remains partial: the EU's rights-centred framework, the US's risk-management orientation, the UK's emphasis on transparency-based governance, and India's still-developing digital criminal justice regime. The paper closes by outlining a rights-based

regulatory framework intended for India and other jurisdictions seeking to incorporate AI into criminal justice while safeguarding rule-of-law principles.

Keywords: Artificial Intelligence, Algorithmic Decision-Making, Criminal Justice, Rule of Law, Due Process, Fair Trial, Algorithmic Bias, Predictive Policing, Human Oversight, AI Governance, India, Comparative Law

1. INTRODUCTION

Human judgment has traditionally sat at the core of criminal justice. Police officers set investigative priorities; prosecutors weigh whether the evidence supports pursuing a case; judges assess evidence and apply the law; and sentencing bodies consider the particulars of both offence and offender. These decisions are far from perfect, since human decision-makers remain vulnerable to error, bias, inconsistency and pressures arising from the institutions they work within. Against this backdrop, AI appears appealing precisely because it can process information at a scale and pace no individual could match.¹

Modern AI systems can now sift through vast datasets, detect patterns, generate predictions, sort individuals into categories, identify faces, work through documents and produce recommendations. Within criminal justice, this has given rise to tools such as predictive policing, recidivism-risk scoring, facial recognition, automated document processing, forensic analysis and judicial decision-support systems.

Yet beneath this technological appeal lies a more fundamental legal difficulty. Criminal justice cannot be reduced to a matter of prediction or efficiency alone — it involves the exercise of coercive state authority, and this distinction matters enormously.

Consider the contrast: a streaming service's algorithm that suggests the wrong film causes little more than mild inconvenience. An algorithm that feeds into decisions about arrest, bail, surveillance, sentencing or imprisonment, however, operates in a fundamentally different legal space, one where the stakes touch directly on individual liberty.

This raises the central question of the article: *Can decisions generated by algorithms meet the rule-of-law standards that have long been expected of human decision-makers?*

This question has grown more pressing as AI tools become woven into the fabric of public institutions. The European Union's AI Act, for instance, explicitly acknowledges that certain law-enforcement uses of AI can bear on surveillance, arrest and deprivation of liberty, and may encroach upon rights relating to a fair trial, legal defence and the presumption of innocence. Consequently, the Act classifies these particular applications as high-risk, subjecting them to regulatory obligations around accuracy, transparency and accountability. ([Eur-Lex][1])²

Similarly, the Council of Europe's Framework Convention on AI and Human Rights, Democracy and the Rule of Law, opened for signature in September 2024, represents the first international legally binding treaty specifically addressing AI through these normative principles. ([Portal][2])³

India is also experiencing rapid digitisation of criminal justice. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) expressly accommodates audio-video electronic means in criminal procedure, including

¹Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, 2024/1689.[\[source\]](#).

²Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, 2024/1689.[\[source\]](#).

³Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No 225, opened for signature 5 September 2024).[\[source\]](#).

recording of search and seizure and electronic modes of trial and proceedings. ([India Code][3]) The Bharatiya Sakshya Adhiniyam, 2023 (BSA) constitutes the current statutory framework governing evidence and expressly seeks to provide general rules and principles of evidence for fair trial. ([India Code][4]) The Supreme Court of India has also begun addressing the consequences of AI-generated legal material. In July 2026, the Court considered a case involving reliance on AI-generated, non-existent case citations and highlighted the implications for the integrity of judicial decision-making. ([Supreme Court of India][5]) These developments demonstrate that the movement towards algorithmic justice is no longer hypothetical.⁴

2. RESEARCH PROBLEM

The fundamental research problem is the tension between “algorithmic efficiency and legal accountability”.

AI may potentially reduce some forms of human inconsistency. However, algorithmic systems introduce a different set of risks:

- I. biased training data;
- II. discriminatory outcomes;
- III. false positives;
- IV. opaque decision-making;
- V. unreliable predictions;
- VI. automation bias;
- VII. lack of explainability;
- VIII. proprietary restrictions;
- IX. inadequate human supervision;
- X. unclear allocation of responsibility.

This issue grows especially concerning when a person lacks the capacity to understand or challenge an algorithmic assessment that has contributed to the exercise of State power. An algorithm may therefore be statistically sophisticated while remaining legally problematic. This produces what may be termed the “algorithmic legitimacy gap”: the gap between an algorithm's technical ability to generate a prediction and its legal legitimacy to influence a decision affecting individual rights.

3. RESEARCH GAP

- I. Scholarship on AI and criminal justice has grown at a fast pace, with existing work covering ground such as predictive policing, algorithmic bias, automated decision-making, risk assessment, surveillance and the broader ethics of AI. Even so, three notable gaps persist in this body of work. The first concerns how technical literature tends to treat accuracy as the main benchmark for evaluating these systems. But criminal justice demands something beyond mere accuracy: a system can perform with technical precision and still fall short on privacy protections, equal treatment or due-process guarantees.⁵
- II. The second gap lies in how legal scholarship tends to study individual technologies in isolation. Predictive policing, facial recognition, sentencing algorithms and AI-generated evidence are commonly examined as separate, self-contained topics, with comparatively little focus placed on

⁴Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530. [\[source\]](#); Bharatiya Sakshya Adhiniyam 2023. [\[source\]](#); *Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd*, 2026 INSC 668 (2 July 2026). [\[source\]](#).

⁵Walter L Perry and others, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (RAND Corporation 2013). [\[source\]](#); Danielle Keats Citron, ‘Technological Due Process’ (2008) 85 Washington University Law Review 1249. [\[source\]](#); Julia Angwin and others, ‘Machine Bias’ (ProPublica, 23 May 2016). [\[source\]](#).

what might be called the continuum of algorithmic decision-making running across the criminal process as a whole.⁶

III. Third, comparative legal scholarship has yet to adequately bring India's emerging framework into dialogue with the more established approaches found in Europe, the United States and Britain.⁷

This article seeks to address these three gaps by approaching AI not merely as a technological instrument, but as a form of public decision-making in its own right.

4. RESEARCH OBJECTIVES

The article has the following objectives:

- a. To examine the transformation of criminal justice from human-centred to algorithm-assisted decision-making.
- b. To identify major applications of AI within criminal justice.
- c. To analyse the implications of algorithmic decision-making for the rule of law.
- d. To examine algorithmic bias and discrimination.
- e. To analyse transparency and explainability requirements.
- f. To comparatively examine AI governance in India, the EU, the US and the UK.
- g. To assess the compatibility of AI-assisted criminal justice with due process and fair-trial principles.
- h. To propose a human-centred regulatory framework for algorithmic criminal justice.

5. RESEARCH QUESTIONS

Q1:- How is AI transforming traditional human decision-making within criminal justice systems?

Q2:- Can algorithmic decision-making satisfy the rule-of-law principles of legality, equality, transparency and accountability?

Q3:- To what extent can algorithmic bias undermine equality and fair trial rights?

Q4:- What level of explainability should be legally required when AI contributes to decisions affecting liberty?

Q5:- How do India, the EU, the US and the UK regulate or govern AI applications in criminal justice?

Q6:- What regulatory principles should govern AI-assisted criminal justice decision-making in India?

6. METHODOLOGY

The article employs a “doctrinal and comparative legal methodology”.

- a. Primary legal sourcesThe research examines:
 - i. constitutional principles;
 - ii. statutes;
 - iii. judicial decisions;
 - iv. regulatory instruments;
 - v. government policies;

⁶Walter L Perry and others, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (RAND Corporation 2013). [\[source\]](#); Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, 2024/1689. [\[source\]](#); European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment* (Council of Europe 2018). [\[source\]](#).

⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, 2024/1689. [\[source\]](#); National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1 (2023). [\[source\]](#); Government Digital Service, “Algorithmic Transparency Recording Standard” (UK Government, updated 2025). [\[source\]](#);

- vi. international conventions;
- vii. judicial guidelines.

b. Comparative jurisdictions

The EU, US and UK are selected because they represent substantially different governance approaches:

- i. Jurisdiction
- ii. Principal orientation
- iii. European Union
- iv. Rights-based, risk-based regulation
- v. United States | Sectoral regulation and risk-management approach
- vi. United Kingdom | Principles-based and transparency-oriented governance
- vii. India | Developing technology-enabled criminal justice framework

c. Secondary materials

The article draws on:

- i. peer-reviewed scholarship;
- ii. books;
- iii. institutional reports;
- iv. AI governance literature;
- v. empirical research;
- vi. judicial and governmental studies.

7. ARTIFICIAL INTELLIGENCE AND CRIMINAL JUSTICE

AI in criminal justice should not be understood as one technology. It encompasses multiple computational techniques and applications.

7.1 Predictive Policing

Predictive policing involves using statistical or computational techniques to identify locations, persons or circumstances considered more likely to be associated with criminal activity.⁸

According to the US Office of Justice Programs, predictive policing involves using analytical methods to pinpoint probable targets for police action, with the aim of preventing or resolving criminal activity. It distinguishes prediction of crimes, offenders, perpetrators and victims. ([Office of Justice Programs][6])

The legal difficulty arises when historical crime data become the basis for future police intervention.⁹

If policing has historically been concentrated in particular communities, the resulting dataset may indicate higher levels of recorded crime in those communities. An algorithm trained on such data can then recommend increased policing in the same locations.

The process becomes:

“Historical policing → Historical data → Algorithmic prediction → Increased policing → New data → Reinforcement of original pattern”

This creates a potential “algorithmic feedback loop”.¹⁰

⁸Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530.[\[source\]](#).

⁹Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530.[\[source\]](#).

¹⁰Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530.[\[source\]](#).

8. ALGORITHMIC RISK ASSESSMENT

Risk assessment systems seek to estimate the probability of future conduct, including reoffending. The most prominent international debate arose around systems such as COMPAS in the United States. ProPublica's investigation of COMPAS reported significant racial disparities in false-positive risk classifications, generating extensive debate concerning fairness and predictive validity. ([ProPublica][7])¹¹

The deeper legal question is not simply whether the algorithm is statistically accurate.

It is: Should a person's liberty be affected by a probabilistic prediction of future behaviour?

Traditional criminal law generally focuses on conduct that has occurred and legally established culpability. Algorithmic risk assessment potentially shifts attention towards *predicted future behaviour*.

This raises concerns regarding:

- I. presumption of innocence;
- II. proportionality;
- III. individual autonomy;
- IV. equality;
- V. evidentiary standards;
- VI. procedural fairness.

9. FACIAL RECOGNITION AND ALGORITHMIC IDENTIFICATION

Facial recognition technology allows law-enforcement agencies to compare facial images against databases. Its advantages include rapid identification and investigative efficiency. However, false matches can result in innocent individuals becoming subjects of police investigation.¹²

Three legal concerns arise.

- First: Accuracy

A false positive may result in investigation or arrest.

- Second: Discrimination

Accuracy may vary across demographic groups.

- Third: Surveillance

Continuous or widespread facial recognition can transform public spaces into environments of persistent identification.

The legal issue is therefore not merely whether facial recognition “works”, but whether its use is “necessary, proportionate and legally authorised”.¹³

10. AI AND JUDICIAL DECISION-MAKING

AI can assist judges and courts in:

- legal research;
- document analysis;

¹¹Julia Angwin and others, ‘Machine Bias’ (ProPublica, 23 May 2016).[\[source\]](#);

¹² Julia Angwin and Jeff Larson, ‘Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say’ (ProPublica, 30 December 2016).[\[source\]](#).

¹³Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, 2024/1689.[\[source\]](#).*Anuradha Bhasin v Union of India* (2020) 3 SCC 637.[\[source\]](#).*State of Madras v VG Row*, AIR 1952 SC 196.[\[source\]](#).

- case classification;
- transcription;
- case management;
- precedent identification;
- prediction of litigation outcomes.

The Council of Europe's CEPEJ recognised these possibilities in its 2018 Ethical Charter. It identifies AI applications including processing judicial decisions and data, legal research, prediction of possible case outcomes and case management. ([Portal][8])However, judicial decision-making is qualitatively different from administrative decision-making.¹⁴

A judicial decision requires:

- interpretation of law;
- evaluation of evidence;
- consideration of competing rights;
- procedural fairness;
- reasoned justification;
- institutional legitimacy.

An algorithm can assist these activities, but whether it can legitimately replace judicial reasoning remains a substantially different question.

11. THE RULE OF LAW AND ALGORITHMIC DECISION-MAKING

The rule of law traditionally incorporates several principles relevant to algorithmic governance.

11.1 Legality

State power must have a legal basis. AI cannot create State authority merely because technology makes an action possible. A police department should therefore not assume that the technical availability of predictive policing authorises its deployment. “Technology does not itself constitute legal authority.”

11.2 Equality

Article 14 of the Indian Constitution requires equality before law and equal protection of laws. Algorithmic systems may challenge this principle because apparently neutral variables can produce discriminatory outcomes.¹⁵

An algorithm can therefore be:

“formally neutral but substantively discriminatory.”

This makes algorithmic impact assessment particularly important.

11.3 Procedural Fairness

Affected individuals should have an opportunity to know and challenge the basis of consequential decisions. Danielle Citron's concept of “technological due process” is particularly relevant. She argues that automated decision-making can collapse adjudication and rulemaking while failing to preserve traditional procedural safeguards. ([WashU Open Journals][9]) This insight is directly applicable to criminal justice.¹⁶

¹⁴European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment* (Council of Europe 2018).[\[source\]](#).

¹⁵“Maneka Gandhi v Union of India” (1978) 1 SCC 248.[\[source\]](#).

¹⁶Danielle Keats Citron, ‘Technological Due Process’ (2008) 85 Washington University Law Review 1249.[\[source\]](#).

12. THE BLACK-BOX PROBLEM

Algorithmic opacity represents one of the most important challenges to algorithmic criminal justice. Frank Pasquale's concept of the “black box society” highlights how important decisions can be shaped by algorithms whose operation remains inaccessible to those affected by them. ([DigitalCommons@UM Carey Law][10])¹⁷

The problem is amplified when algorithms are:

- proprietary;
- technically complex;
- based on machine learning;
- continuously updated;
- trained using undisclosed datasets.

Suppose an AI system assigns an accused person a high-risk score. The accused asks:

- i. Why am I considered high risk?

If the answer is simply: “The algorithm determined it,” the conventional relationship between “reason, decision and accountability” breaks down. A judicial system based on reasons cannot easily accommodate unexplained technological conclusions.

13. EXPLAINABILITY AND THE RIGHT TO CHALLENGE

Explainability should not necessarily require disclosure of every line of source code. A more practical legal standard is “meaningful explanation”.¹⁸

A person affected by an AI-assisted decision should ordinarily be able to understand:

1. what the system was designed to do;
2. what categories of data were used;
3. what factors materially influenced the outcome;
4. the system's known limitations;
5. its error rate;
6. whether human review occurred;
7. how the decision can be challenged.

This produces a distinction between:

“Technical transparency” and “Legal explainability”.

The latter is more important for procedural justice.¹⁹

14. ALGORITHMIC BIAS

AI does not necessarily eliminate human bias. It can reproduce, amplify or conceal it.

Bias may enter at several stages:²⁰

- Dataset bias

¹⁷Frank Pasquale, “The Black Box Society: The Secret Algorithms That Control Money and Information” (Harvard University Press 2015).[\[source\]](#).

¹⁸Danielle Keats Citron, ‘Technological Due Process’ (2008) 85 Washington University Law Review 1249.[\[source\]](#);

¹⁹National Institute of Standards and Technology, ‘Artificial Intelligence Risk Management Framework (AI RMF 1.0)*’, NIST AI 100-1 (2023).[\[source\]](#).

²⁰Julia Angwin and others, ‘Machine Bias’ (ProPublica, 23 May 2016).[\[source\]](#);

Historical data may reflect discriminatory practices.

- Selection bias

Certain populations may be overrepresented in datasets.

- Labelling bias

Human classifications used to train systems may contain subjective assumptions.

- Design bias

Developers may choose variables that indirectly correlate with protected characteristics.

- Deployment bias

An accurate system may nevertheless be inappropriate in a particular institutional environment.

Consequently: “The absence of an explicitly discriminatory variable does not guarantee the absence of discriminatory outcomes.”

15. COMPARATIVE ANALYSIS

15.1 European Union

The EU has developed the most comprehensive binding AI regulatory framework among the jurisdictions considered.

The *EU AI Act, Regulation (EU) 2024/1689*, adopts a risk-based approach. Certain law-enforcement applications are treated as high-risk because they may affect fundamental rights, including fair trial, defence and presumption of innocence. The Regulation specifically identifies applications involving risk assessment, evidence evaluation and criminal profiling among the areas requiring heightened scrutiny. ([Eur-Lex][1])²¹

The EU approach is therefore:

Risk classification → obligations → documentation → transparency → oversight → accountability. This model is particularly relevant to criminal justice because it recognises that not all AI applications pose equal risks.

16. COUNCIL OF EUROPE APPROACH

The Council of Europe's 2018 CEPEJ Ethical Charter identifies five fundamental principles:

1. respect for fundamental rights;
2. Non-discrimination;
3. quality and security;
4. transparency, impartiality and fairness;
5. user control. ([Council of Europe Bookshop][11])

These principles matter because they reject the notion that efficiency alone should be the deciding factor in determining AI's suitability for the justice system. The later “Council of Europe Framework Convention on AI and Human Rights, Democracy and the Rule of Law” strengthens this normative orientation by placing AI governance directly within human rights, democracy and rule-of-law principles. ([Portal] [2])²²

²¹Frank Pasquale, “The Black Box Society: The Secret Algorithms That Control Money and Information” (Harvard University Press 2015). [\[source\]](#).

²²European Commission for the Efficiency of Justice (CEPEJ), “European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment” (Council of Europe 2018). [\[source\]](#);

17. UNITED STATES

The United States presents a more fragmented model.

Rather than one comprehensive federal AI statute equivalent to the EU AI Act, AI governance has historically been involved.

- constitutional protections;
- sector-specific legislation;
- administrative law;
- judicial decisions;
- state legislation;
- technical standards.

The “NIST AI Risk Management Framework” provides an important governance model. It is voluntary, rights-preserving and designed to assist organisations in identifying and managing AI risks. ([NIST][12])²³

The US experience also demonstrates the difficulty of relying exclusively on algorithmic accuracy. The COMPAS controversy illustrated the conflict between predictive performance, racial fairness and procedural transparency. ([ProPublica][7]) The American model therefore provides an important lesson: “Technical validation cannot substitute for legal accountability.”²⁴

18. UNITED KINGDOM

The UK has adopted a comparatively principles-based approach to AI governance. An important feature is the “Algorithmic Transparency Recording Standard (ATRS)”, which promotes transparency concerning the use of algorithmic tools by public bodies. UK government materials specifically document the standard and its relevance to police forces. ([GOV.UK][13])

The UK experience demonstrates the value of institutional transparency even in the absence of a single comprehensive AI statute governing every criminal justice application. For criminal justice, however, transparency alone may be insufficient. An algorithm can be completely disclosed and still be discriminatory or disproportionate. Thus: “Transparency is necessary but not sufficient.”²⁵

19. INDIA

India presents a distinctive situation. The country has entered a period of significant criminal-law and digital-procedure reform.

The BNSS, 2023 expressly incorporates electronic means into criminal proceedings. Section 105 provides for recording search and seizure through audio-video electronic means, while Section 530 permits trials, inquiries and proceedings to be conducted through electronic communication or audio-video electronic means. ([India Code][3])²⁶

The BSA, 2023 now provides the statutory framework governing evidence and expressly states that it provides general rules and principles of evidence for fair trial. ([India Code][4])²⁷

²³Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No 225, opened for signature 5 September 2024). [\[source\]](#).

²⁴National Institute of Standards and Technology, “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”, NIST AI 100-1 (2023). [\[source\]](#).

²⁵Government Digital Service, “Algorithmic Transparency Recording Standard” (UK Government, updated 2025). [\[source\]](#).

²⁶Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530. [\[source\]](#).

²⁷Bharatiya Sakshya Adhiniyam 2023. [\[source\]](#).

India has also enacted the *Digital Personal Data Protection Act, 2023*, which establishes a statutory framework concerning processing of digital personal data and recognises both individual data protection and lawful processing needs. ([MeitY][14])²⁸

The Supreme Court has separately explored AI use in the judiciary, including AI-based transcription of arguments and proceedings. ([Supreme Court of India][15])²⁹

More recently, the Court's treatment of AI-generated false legal authorities demonstrates that algorithmic reliability is becoming a direct judicial concern. ([Supreme Court of India][5])

20. COMPARATIVE MATRIX

Issue	India	EU	USA	UK
General AI Framework	Developing	Comprehensive, risk-based	Fragmented/sectoral	Principles-based
Criminal Justice AI	Emerging	High-risk regulation	Application-specific	Transparency-oriented
Fundamental Rights Basis	Constitutional	Charter of Fundamental Rights/ECHR framework	Constitutional rights	Human rights framework
Algorithmic Transparency	Developing	Stronger statutory requirements	Variable	ATRS (Algorithmic Transparency Recording Standard)
Human Oversight	Emerging principle	Strong requirement for high-risk systems	Context-dependent	Governance principle
Algorithmic Auditing	Developing	Increasingly institutionalised	Risk-management approach	Emerging
AI Evidence	Developing	Risk-sensitive	Case-specific	Developing
Principal Challenge	Regulatory fragmentation	Implementation	Fragmentation	Enforceability

21. FROM HUMAN JUDGMENT TO ALGORITHMIC JUDGMENT

The central thesis of this article is that the transformation is not simply:

“Human → Machine” Instead, it is: “Human Judgment → Human + Algorithm → Algorithm-Shaped Human Judgment”. This distinction is crucial.

Even where a judge formally makes the final decision, an algorithm may influence:

- which information is presented;
- which defendants receive additional scrutiny;

²⁸Digital Personal Data Protection Act 2023. [\[source\]](#).

²⁹Supreme Court of India, ‘Design, Development, and Implementation of Artificial Intelligence (AI) Solution, Tools for Transcribing Arguments and Court Proceedings’ (23 May 2023). [\[source\]](#);

- which cases are prioritised;
- how risk is characterised;
- which precedents are retrieved;
- which evidence receives attention.

The algorithm therefore does not need formal decision-making authority to exercise “de facto influence”. This phenomenon may be called “algorithmic framing.”

22. AUTOMATION BIAS

Automation bias occurs when human decision-makers place excessive confidence in computer-generated recommendations. A judge may theoretically disagree with an algorithm.

But if the algorithm is presented as:

- statistically validated;
- technologically sophisticated;
- objective;
- data-driven;

The human decision-maker may be psychologically inclined to accept its recommendation. Therefore, the requirement of human oversight should not mean merely: “A human clicked the approval button.” It should require “meaningful human judgment”.³⁰

23. HUMAN-IN-THE-LOOP PRINCIPLE

The article proposes three categories of AI use.

I. Level I — Administrative AI

Examples:

- scheduling;
- transcription;
- document organisation;
- case management.

“Regulatory risk:” Low to moderate.

II. Level II — Investigative/Analytical AI

Examples:

- pattern identification;
- evidence analysis;
- investigative prioritisation;
- document analysis.

“Regulatory requirement:” Human verification and auditability.

III. Level III — Rights-Affecting AI

Examples:

- risk assessment influencing liberty;
- automated identification leading to arrest;

³⁰Supreme Court of India, “White Paper on Artificial Intelligence and Judiciary” (Centre for Research and Planning, November 2025).[\[source\]](#).

- sentencing recommendations;
- AI-generated assessment of evidence;
- decisions materially influencing bail or detention.

“Regulatory position:” Mandatory meaningful human oversight, disclosure and effective challenge.

24. PROPOSED HUMAN-CENTRED ALGORITHMIC CRIMINAL JUSTICE FRAMEWORK

The comparative analysis suggests that an effective framework should contain “eight principles”.

a. Principle 1: Legality

AI should be deployed by public authorities only where there is clear legal authority.

b. Principle 2: Necessity

AI should not be deployed merely because it is technologically available.

c. Principle 3: Proportionality

The benefits must justify the interference with individual rights.

d. Principle 4: Non-discrimination

AI systems should undergo systematic bias testing.

e. Principle 5: Transparency

People and the organizations responsible for overseeing them need adequate visibility into how AI is being used in high-stakes situations.

f. Principle 6: Explainability

Affected individuals should receive meaningful reasons for decisions materially influenced by AI.

g. Principle 7: Human Accountability

A human official must remain legally responsible for consequential decisions.³¹

h. Principle 8: Effective Remedy

Individuals must be able to challenge inaccurate, discriminatory or unlawful algorithmic decisions.³²

25. PROPOSED ALGORITHMIC IMPACT ASSESSMENT

Before deploying high-impact AI in criminal justice, authorities should undertake an “Algorithmic Criminal Justice Impact Assessment (ACJIA).”

It should examine:

Assessment Criterion	Guiding Question
Legal	Is there statutory authority for deployment of the system?
Rights	Which fundamental rights are affected by its use?
Accuracy	How reliable and accurate is the system's output?

³¹European Commission for the Efficiency of Justice (CEPEJ), “European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment” (Council of Europe “Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd”, 2026 INSC 668 (2 July 2026).[\[source\]](#).

³²Danielle Keats Citron, ‘Technological Due Process’ (2008) 85 Washington University Law Review 1249.[\[source\]](#); “Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd”, 2026 INSC 668 (2 July 2026).[\[source\]](#).

Bias	Are particular groups disproportionately affected by its outcomes?
Explainability	Can meaningful reasons be provided for its decisions?
Security	Can the integrity of the data and model be adequately protected?
Human Oversight	Who is responsible for the final decision?
Remedy	How can an affected person challenge the system's output?
Audit	Who conducts independent evaluation of the system?
Sunset	When will the system be reassessed or reviewed?

This proposed assessment could be one of the article's principal contributions.³³

26. AI AND THE PRESUMPTION OF INNOCENCE

Algorithmic prediction presents a particularly difficult challenge to the presumption of innocence.

The traditional criminal process asks:

What has the accused done?

Predictive systems may instead ask:

What is the accused likely to do?

The shift from retrospective adjudication to prospective prediction creates normative tension. Criminal justice should not transform probability into culpability. A risk score should therefore never be treated as equivalent to proof of criminal conduct.³⁴

27. AI AND THE RIGHT TO A FAIR TRIAL The right to a fair trial requires more than an accurate outcome. It includes procedural legitimacy.

A defendant should have the ability to:³⁵

- understand the case against them;
- challenge evidence;
- question expert evidence;
- contest adverse findings;
- receive an impartial adjudication;
- obtain reasons for the decision.

If AI materially contributes to an adverse decision but its operation cannot be meaningfully scrutinised, the fairness of the process becomes questionable.

The EU AI Act expressly recognises this concern by connecting insufficient transparency, explainability and documentation with possible impairment of fair-trial, defence and presumption-of-innocence rights. ([Eur-Lex][1])³⁶

³³National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)", NIST AI 100-1 (2023).[\[source\]](#); Government Digital Service, "Algorithmic Transparency Recording Standard" (UK Government, updated 2025).[\[source\]](#).

³⁴Julia Angwin and others, 'Machine Bias' (ProPublica, 23 May 2016).[\[source\]](#); "Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd", 2026 INSC 668 (2 July 2026).[\[source\]](#).

³⁵Danielle Keats Citron, 'Technological Due Process' (2008) 85 Washington University Law Review 1249.[\[source\]](#);

³⁶Mohd Hussain v State (Govt of NCT of Delhi) (2012) 2 SCC 584.[\[source\]](#).

28. AI-GENERATED EVIDENCE

Generative AI creates a new evidentiary challenge.

Synthetic:

- photographs;
- videos;
- audio;
- documents;
- transcripts;
- witness materials; may be created or manipulated with increasing sophistication.

The BSA provides the contemporary Indian statutory framework for evidence, while the BNSS incorporates extensive electronic procedures. ([India Code][4])³⁷

The challenge therefore moves beyond admissibility to:

“Authenticity → Integrity → Provenance → Reliability → Attribution”

Courts may increasingly need to determine not merely whether a digital file exists, but:³⁸

“Who created it, how it was created, whether it was manipulated, and whether its algorithmic provenance can be independently verified.”

29. ACCOUNTABILITY AND ATTRIBUTION

One of the most difficult questions is:

Who is responsible when AI-assisted criminal justice produces a wrongful outcome?

Possible actors include:³⁹

- software developers;
- vendors;
- data providers;
- police authorities;
- prosecutors;
- judges;
- government departments;
- system administrators.

A fragmented accountability model can create a situation where everyone is involved but nobody is responsible.⁴⁰

The proposed model therefore adopts:

- Human accountability despite algorithmic assistance.

The use of AI should never create an accountability vacuum.

³⁷Bharatiya Sakshya Adhiniyam 2023.[\[source\]](#);Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530.[\[source\]](#).

³⁸Bharatiya Sakshya Adhiniyam 2023.[\[source\]](#);Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530.[\[source\]](#).

³⁹“Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd”, 2026 INSC 668 (2 July 2026).[\[source\]](#).

⁴⁰“Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd”, 2026 INSC 668 (2 July 2026).[\[source\]](#);

30. WHY AI OUGHT TO SUPPORT HUMAN DECISION-MAKING INSTEAD OF SUBSTITUTING FOR IT

The comparative analysis supports a “human-centred rather than machine-substitution model”. Human decision-making has weaknesses. AI has weaknesses.⁴¹

The objective should therefore be to combine their respective strengths while preventing the transfer of unreviewable power to algorithms.

a. Human strengths

- contextual reasoning;
- moral judgment;
- interpretation;
- empathy;
- proportionality.

b. AI strengths

- processing large datasets;
- pattern recognition;
- consistency;
- speed;
- information retrieval.

The preferred model is therefore: “Human judgment + AI assistance + legal safeguards” rather than: “Algorithmic recommendation + automatic acceptance.”⁴²

31. FINDINGS

The research produces seven principal findings.

1. Finding 1

AI can improve criminal justice efficiency but efficiency alone cannot establish legal legitimacy.

2. Finding 2

The exclusion of protected characteristics from an algorithm's explicit inputs does not, by itself, ensure that the system operates in a fair or unbiased manner.

3. Finding 3

Opaque algorithms create a significant challenge to procedural fairness.

4. Finding 4

Human oversight must be meaningful rather than merely formal.

5. Finding 5

AI-generated predictions should not be treated as equivalent to proof of criminal culpability.

6. Finding 6

The EU provides the strongest emerging example of risk-based AI regulation, while the US, UK and India provide complementary governance approaches.

⁴¹Danielle Keats Citron, ‘Technological Due Process’ (2008) 85 Washington University Law Review 1249.[\[source\]](#).

⁴²European Commission for the Efficiency of Justice (CEPEJ), ‘European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment’ (Council of Europe 2018).[\[source\]](#);

7. Finding 7

India requires a dedicated governance framework for high-impact AI applications in criminal justice.

32. RECOMMENDATIONS

32.1 Enact sector-specific

AI rules for criminal justice India should consider a dedicated framework governing AI applications in:

- policing;
- investigation;
- prosecution;
- evidence;
- bail;
- sentencing;
- corrections.

32.2 Mandatory algorithmic impact assessment

High-impact AI systems should undergo pre-deployment and periodic impact assessments.

32.3 Independent auditing

AI systems used in criminal justice should be independently audited for:

- accuracy;
- bias;
- security;
- reliability;
- explainability.

32.4 Disclosure

Where AI materially contributes to a decision affecting an accused person, the use of AI should ordinarily be disclosed.

32.5 Right to challenge

Individuals should have a meaningful mechanism to challenge consequential algorithmic outputs.

32.6 Human responsibility

Final decisions concerning liberty should remain attributable to identifiable human decision-makers.

32.7 Algorithmic evidence protocols

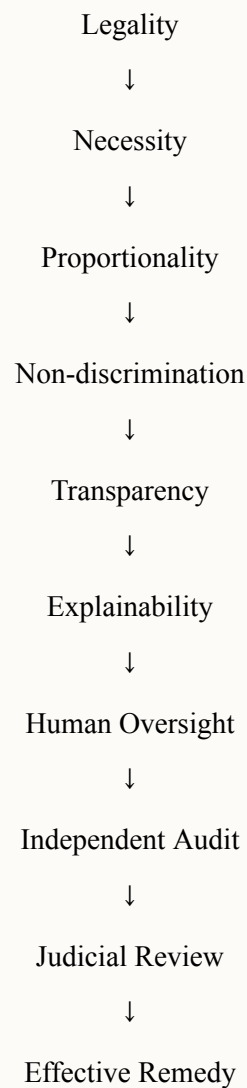
Courts should develop protocols for AI-generated and AI-manipulated evidence.

32.8 Periodic reassessment

AI systems should not receive permanent authorisation. Their deployment should be subject to periodic review and, where necessary, suspension.

33. ORIGINAL CONCEPTUAL CONTRIBUTION

The central contribution of this research is the proposed: “Human-Centred Algorithmic Criminal Justice Model”



This model integrates the strongest elements emerging from the EU, Council of Europe, US, UK and Indian approaches. The objective is not to prevent technological innovation. Rather, it is to ensure: “The more consequential the algorithmic decision, the stronger the legal safeguards surrounding it.”⁴³

34. CONCLUSION

Shifting from human judgment to algorithm-driven decisions marks one of the most profound changes now facing the modern criminal justice system. AI has considerable potential. It can help police analyse complex datasets, assist lawyers and judges in processing information, improve administrative efficiency and potentially identify patterns that would otherwise remain undetected. But criminal justice is not merely an information-processing exercise. It is an institutional system for determining guilt, protecting rights and exercising coercive State power. That distinction places constitutional and rule-of-law limits upon technological deployment.

The central lesson emerging from the comparative analysis is that “AI should not be regarded as an autonomous source of legal authority”. Algorithms can identify patterns, generate predictions and assist decision-makers, but they cannot by themselves supply the legitimacy required for decisions affecting human liberty. The EU's risk-based approach, the Council of Europe's human-rights framework, the US emphasis on risk management, the UK's transparency mechanisms and India's rapidly developing digital

⁴³Supreme Court of India, “White Paper on Artificial Intelligence and Judiciary” (Centre for Research and Planning, November 2025).[\[source\]](#).

criminal justice infrastructure demonstrate different components of a broader regulatory response. None is complete.⁴⁴

India, in particular, stands at an important regulatory moment. The introduction of the BNS, BNSS and BSA has modernised the statutory architecture of criminal justice and created greater scope for electronic processes. At the same time, developments in AI require the legal system to confront questions that cannot be answered solely through technological efficiency. ([India Code][3])⁴⁵

The ultimate objective should therefore not be to choose between humans and machines. It should be to create a system in which: “AI assists justice, humans remain accountable, and law remains supreme.”

The future of criminal justice should accordingly be understood not as algorithmic justice, but as “human-centred justice enhanced by accountable algorithms”.

References

A. Books and Scholarly Literature

1. Citron, D. K. (2008). Technological Due Process. *Washington University Law Review*, 85(6), 1249–1313. ([WashU Open Journals][9])
2. Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press. ([De Gruyter Brill][16])
3. Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND/US Department of Justice. ([Office of Justice Programs][6])
4. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias. ProPublica. ([ProPublica][17])
5. Angwin, J., & Larson, J. (2016). Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say. ProPublica. ([ProPublica][18])
6. European Commission for the Efficiency of Justice (CEPEJ). (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. Council of Europe. ([Portal][19])

B. International and Regulatory Materials

1. European Union. (2024). “Regulation (EU) 2024/1689 – Artificial Intelligence Act”. EUR-Lex. ([Eur-Lex][1])
2. Council of Europe. (2024). “Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law”. ([Portal][2])
3. National Institute of Standards and Technology (NIST). (2023). “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”, NIST AI 100-1. ([NIST][20])
4. National Institute of Standards and Technology. (2024). “Artificial Intelligence Risk Management

⁴⁴Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L, 2024/1689. [\[source\]](#); Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No 225, opened for signature 5 September 2024). [\[source\]](#); National Institute of Standards and Technology, “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”, NIST AI 100-1 (2023). [\[source\]](#); Government Digital Service, “Algorithmic Transparency Recording Standard” (UK Government, updated 2025). [\[source\]](#); Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530. [\[source\]](#).

⁴⁵Bharatiya Nagarik Suraksha Sanhita 2023, ss 105, 530. [\[source\]](#); Bharatiya Sakshya Adhiniyam 2023. [\[source\]](#); Digital Personal Data Protection Act 2023. [\[source\]](#).

Framework: Generative Artificial Intelligence Profile”, NIST AI 600-1. ([NIST][12])

5. Council of Europe, CEPEJ. (2018). “European Ethical Charter on AI in Judicial Systems”. ([Portal][21])
6. UK Department for Science, Innovation and Technology. (2024). “Algorithmic Transparency Recording Standard”. ([GOV.UK][13])

C. Indian Legal Materials

1. Government of India. (2023). “Bharatiya Nagarik Suraksha Sanhita, 2023”. India Code. ([India Code][3])
2. Government of India. (2023). “Bharatiya Sakshya Adhiniyam, 2023”. India Code. ([India Code][4])
3. Government of India. (2023). “Digital Personal Data Protection Act, 2023”. Ministry of Electronics and Information Technology. ([MeitY][14])
4. Supreme Court of India. (2023). “Design, Development and Implementation of Artificial Intelligence Solution/Tools for Transcribing Arguments and Court Proceedings”. ([Supreme Court of India][15])
5. Supreme Court of India. (2025). “White Paper on Artificial Intelligence and Judiciary”. Supreme Court of India. ([Supreme Court of India][22])
6. Supreme Court of India. (2026). “Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd.”, 2026 INSC 668. ([Supreme Court of India][5])

D. Foundational Judicial Authorities to Incorporate

For a Scopus-level Indian law article, I strongly recommend incorporating the following authorities into the final manuscript rather than relying only on AI-specific cases:

1. “Maneka Gandhi v. Union of India”, (1978) 1 SCC 248 — substantive and procedural fairness under Article 21.
2. “Justice K.S. Puttaswamy (Retd.) v. Union of India”, (2017) 10 SCC 1 — constitutional right to privacy.
3. “Anuradha Bhasin v. Union of India”, (2020) 3 SCC 637 — proportionality and restrictions affecting fundamental rights.
4. “State of Madras v. V.G. Row”, AIR 1952 SC 196 — proportionality and reasonableness.
5. “Selvi v. State of Karnataka”, (2010) 7 SCC 263 — involuntary techniques in criminal investigation and personal liberty.
6. “Shreya Singhal v. Union of India”, (2015) 5 SCC 1 — freedom of speech and intermediary regulation.
7. “Armesh Kumar v. State of Bihar”, (2014) 8 SCC 273 — safeguards concerning arrest and individual liberty.
8. “D.K. Basu v. State of West Bengal”, (1997) 1 SCC 416 — procedural safeguards in custodial contexts.
9. “Mohd. Hussain v. State (Govt. of NCT of Delhi)”, (2012) 2 SCC 584 — fair trial and procedural justice.



© 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>)