(JOINT JURIST)

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL]

| VOLUME 1 | ISSUE 2 | JUNE – JULY 2026

ABOUT THE JOURNAL

Joint Jurist is an online legal platform and a national publication which is aimed at spreading online legal education, bridging the gap between academic research and litigation expertise among the legal audience. It was introduced in early 2026. It is an independent project, started by its founder and does not receive any funding from any person or organisation or body or government as the case maybe. It is a 'Dream Project' of *Mr. Suraj Shandil (Advocate) (Founder-CEO-Editor-in-Chief & Owner)*. We operate on a Double-Blind Peer-Review model, ensuring that every published work meets the highest standards of original scholarship, zero plagiarism, and academic integrity. Our platform is dedicated to providing an open-access environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **Dr. Seema Gupta**
- **Dr. Mohd Rafiq**
- **Dr. Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**
- **Mrs. Shivani Kumari**

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

NAME	DESIGNATION	INSTITUTION/AFFILIATION	SPECIALIZATION & IMPACT
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	**High Court of Himachal Pradesh**	IPR Specialist, Courtroom Strategy & Legal Research.
Prof. (Dr.) Seema Gupta	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**	Constitutional Law, IPR, & Supreme Court Certified Mediator/ Interdisciplinary Legal Studies.
Prof. (Dr.) Mohd. Rafiq Dar	Editorial Board Member	**Associate Professor/Lovely Professional University (LPU)**	Consumer Law, Criminal Law, Law on Consumer Protection/Interdisciplinary Legal Studies.
Dr. Harshita Thalwal	Editorial Board Member	**Associate Professor & HOD, Chandigarh University(CU)**	Academic Leadership & Interdisciplinary Legal Studies.
Asst. Prof. Ms. Somya Sharma	Editorial Board Member	**Professor of law & Ph.D. Scholar/ Shoolini University**	Banking Laws, Corporate Laws, & Human Rights /Interdisciplinary Legal Studies..
Asst. Prof. Ms. Sabrina Bath	Editorial Board Member	**Assistant Professor & Ph.D. Scholar/Chandigarh University (CU)**	Legal Framework Analysis & Academic Rigour/ Interdisciplinary Legal Studies.
Asst. Prof. Mrs. Shivani Kumari	Editorial Board Member	**Assistant Professor & Ph.D. Scholar/ DDM Sai Law College, Hamirpur, Himachal Pradesh.**	Academic Leadership & Interdisciplinary Legal Studies.

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

| VOLUME 1 | ISSUE 2 | JUNE – JULY 2026

ROLE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE SYSTEM: BALANCING EFFICIENCY, DUE PROCESS, AND HUMAN RIGHTS

AUTHOR : NEHA SHANDIL RESEARCH SCHOLAR / BAHRA UNIVERSITY / SHIMLA HILLS, WAKNAGHAT SOLAN, HIMACHAL PRADESH - 173234

CO - AUTHOR :- DR. DEEPSHIKHA / ASSISTANT PROFESSOR / SCHOOL OF LAW BAHRA UNIVERSITY /SHIMLA HILLS, WAKNAGHAT SOLAN, HIMACHAL PRADESH - 173234

Introduction

The expansion of artificial intelligence into criminal justice institutions reflects broader changes in how states manage information, risk, and administrative scale. Criminal justice systems increasingly rely on large volumes of data generated through complaints, surveillance, records management, and digital communications. These conditions create incentives to adopt computational tools that promise speed, consistency, and predictive capacity. At the same time, criminal justice remains a domain where state power is exercised in its most intrusive forms, including arrest, detention, prosecution, and punishment. The legitimacy of this power depends on legality, procedural fairness, and reasoned justification. The growing use of AI therefore introduces a structural tension between automation-driven governance and rights-based legal constraints that shape how coercive authority may be exercised.[1]

Artificial intelligence alters decision environments rather than simply replacing human actors Tools used for prediction, classification, or prioritization influence what information is noticed, how risks are framed, and which cases receive institutional attention. These effects are often indirect, operating through administrative routines, performance metrics, and workload pressures rather than through explicit delegation of authority to machines. As a result, AI can shape outcomes even when formal responsibility remains with human officials. This raises questions about accountability, transparency, and reviewability, especially where automated outputs are treated as neutral or objective. Legal analysis must therefore move beyond technical accuracy to examine how design choices, data sources, and institutional contexts affect fairness and legality across different stages of the criminal process.[2]

In the Indian context, the introduction of AI intersects with constitutional guarantees of equality, personal liberty, and procedural fairness, as well as with evolving statutory frameworks

[1] John L. M. McDaniel, Ken G. Pease, *Predictive Policing and Artificial Intelligence* 112 (Routledge, London, 1st edn., 2021).

[2] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* 97 (New York University Press, New York, 1st edn., 2017).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

governing criminal procedure, evidence, and data protection. These legal structures do not prohibit technological assistance, but they impose conditions on how decisions affecting rights must be made, justified, and challenged. This study approaches artificial intelligence as a governance issue rather than a purely technical development. It examines how AI systems interact with policing, investigation, prosecution, adjudication, and corrections, and evaluates whether existing legal principles and institutional practices are adequate to manage the risks and responsibilities created by automated and data-driven decision support.

Key Terms and Core Concepts

A coherent discussion requires stable meanings for technical terms and criminal justice functions, because many controversies arise from category mistakes. Predictive tools are often described as neutral "technology", even when they embed choices about targets, thresholds, and proxies. Institutional stages are often treated as linear, even when policing, investigation, prosecution, adjudication, and corrections overlap through feedback loops, discretionary gateways, and administrative constraints.[3] Core concepts also carry different normative weight depending on context: "bias" may refer to statistical skew, social hierarchy, or unlawful discrimination; "transparency" may refer to disclosure of code, an intelligible explanation, or an auditable process record. The definitions and short conceptual accounts below supply the minimum shared vocabulary needed for later evaluation of deployment risks, evidentiary standards, and accountability mechanisms in India's criminal process.[4]

Artificial Intelligence in Criminal Justice

Artificial intelligence in criminal justice refers to computational techniques that perform tasks associated with human judgment in institutional settings that can impose surveillance, restraint, or punishment. The relevant systems range from rule-based screening to machine learning models that infer patterns from data, and they often operate through classification, ranking, matching, anomaly detection, or summarisation.[5] Criminal justice deployment changes the ethical and legal salience of technical design choices because outputs can influence stops, searches, arrests, bail conditions, charging priorities, trial management, and custody decisions. The same technical tool can function as an internal aid, a managerial dashboard, or a decision trigger, and each role raises different expectations of documentation, review, and contestability. Conceptual clarity is needed because "AI" is often used as a blanket label that hides meaningful differences in training data, model objectives, error costs, and human oversight.[6]

Machine Learning

Doctrinal and policy debates need a clear meaning for this term because many criminal justice tools marketed as "AI" are, in fact, statistical learning systems trained on historical records. The "Tom Mitchell" defines the "machine learning" as "A computer programme is said to learn

---

[3] Daniel Marciniak, "Algorithmic Policing: An Exploratory Study of the Algorithmically Mediated Construction of Individual Risk in a UK Police Force", 33 *Policing and Society* 449 (2023).

[4] Aleš Završnik, "Criminal Justice, Artificial Intelligence Systems, and Human Rights", 20 *ERA Forum* 567 (2020).

[5] Artificial Intelligence in Criminal Justice: Opportunities and Risks, *available at:* https://www.weforum.org/agenda/archive/artificial-intelligence/ (last visited on January 23, 2026).

[6] Artificial Intelligence and Criminal Justice: An Overview, *available at:* https://www.ojp.gov/ncjrs/virtual-library/abstracts/artificial-intelligence-and-criminal-justice-overview (last visited on January 24, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

from experience E with respect to some class of tasks T and performance measure P."[7] The "Ethem Alpaydin" defines the "machine learning" as "programming computers to optimize a performance criterion using example data or past experience."[8] These definitions matter because they show that task choice, performance measures, and training experience are not neutral, especially where policing data may reflect under-reporting, selective enforcement, or uneven recording practices. A legal analysis therefore treats model objectives and data provenance as part of the system's normative footprint, not as external technical details.[9]

A legally attentive account also requires distinguishing learning from automation. The Mitchell framing makes "performance measure P" central, which maps well onto criminal justice settings where false positives and false negatives carry unequal rights costs. The Alpaydin framing foregrounds optimisation, which highlights that a model can be technically successful while still being institutionally harmful if it optimises speed, clearance rates, or cost reductions at the expense of fairness and accuracy. These concerns become sharper where models are retrained on outcomes influenced by earlier model outputs, creating self-reinforcing cycles. The concept also clarifies accountability: when learning systems generalise from past data, responsibility for errors cannot be placed solely on frontline users, because the design choices that define tasks, labels, and evaluation criteria are upstream governance decisions.[10]

Natural Language Processing

Clear definitions are necessary because language technologies increasingly shape complaint intake, case file summarisation, translation, transcription, and risk narrative generation, each of which can influence later stages. The "Jacob Eisenstein" defines the "natural language processing" as "the set of methods for making human language accessible to computers."[11] The "Christopher Manning" defines the "natural language processing" as "a field at the intersection of computer science, artificial intelligence, and linguistics."[12] These definitions matter for criminal justice because language is not only information but also testimony, allegation, and legal claim, and errors can shift meaning, credibility, or intent. A doctrinal lens therefore treats language outputs as potential evidence artefacts or decision inputs requiring traceability and review.[13]

These definitions also highlight two governance risks. Eisenstein's emphasis on "methods" invites scrutiny of preprocessing, tokenisation, translation choices, and summarisation

---

7 A Non-technical Introduction to Machine Learning - Machine Learning for Brain Disorders - NCBI Bookshelf, *available at:* https://www.ncbi.nlm.nih.gov/books/NBK597507/ (last visited on January 24, 2026).

8 Speech and Language Processing (3rd ed. draft), *available at:* https://web.stanford.edu/~jurafsky/slp3/ (last visited on January 23, 2026).

9 Kevin D. Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age* 141 (Cambridge University Press, Cambridge, 1st edn., 2017).

10 Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* 88 (Crown, New York, 1st edn., 2016).

11 Natural Language Processing, *available at:* https://cdn.jsdelivr.net/gh/it-ebooks-0/it-ebooks-2018-04to07/Natural%20Language%20Processing%20%28Jacob%20Eisenstein%29.pdf (last visited on January 22, 2026).

12 CS224n Lecture: Introduction to NLP and Deep Learning, *available at:* https://web.stanford.edu/class/archive/cs/cs224n/cs224n.1184/lectures/lecture1.pdf (last visited on January 21, 2026).

13 Kenton Brice, "Natural Language Processing and the Automation of Legal Decision-Making", 52 *Jurimetrics* 73 (2012).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

constraints that can erase context, dialect, or legally relevant qualifiers. Manning's intersection framing signals that linguistic variation and pragmatics are not peripheral, especially in multilingual Indian settings where police statements, witness accounts, and court records often move between languages and registers. Model confidence scores and fluent output can conceal uncertainty, prompting overreliance. The legal concern is not only accuracy but also contestability: when an automated summary becomes the practical record used by officials, the system shapes procedural reality. This makes documentation of inputs, prompts, and model versions a governance requirement rather than a technical preference.[14]

Computer Vision

This term requires definition because criminal justice institutions rely heavily on visual material, including CCTV, body-worn cameras, crime scene photos, biometric images, and scanned documents. The "Shree K. Nayar" defines the "computer vision" as "the enterprise of building machines that can see."[15] The "British Machine Vision Association (BMVA)" defines the "computer vision" as "automatic extraction, analysis and understanding of useful information from a single image or a sequence of images."[16] These definitions matter because they indicate that vision systems do not merely "observe" but infer, categorise, and prioritise, and those inferences can become operational triggers for surveillance or suspicion. The legal analysis must therefore ask what counts as "useful information", who defines it, and how error and uncertainty are handled.[17]

The definitional emphasis on extraction and understanding is especially significant where images are treated as objective truth. Vision models depend on lighting, camera angles, resolution, compression, and dataset composition, so their outputs are conditioned, not neutral. Criminal justice systems also face adversarial manipulation, such as spoofing or selective framing, which makes validation and audit trails central. Where facial recognition or object detection is used, the institution must decide whether outputs are investigative leads, corroborative signals, or proof substitutes, because each role requires different thresholds and disclosure. A legally grounded approach treats these outputs as contestable inferences requiring safeguards, documentation, and procedures for human review, rather than as self-authenticating facts.[18]

Criminal Justice System

Conceptual clarity about the system is needed because AI deployment is often analysed as a set of isolated tools rather than as interventions in a connected institutional ecology. The criminal justice system can be understood as a coordinated set of institutions that exercise state power to prevent, detect, process, adjudicate, and respond to alleged offences. Each stage has distinct

---

[14] Benjamin R. Chen, "Text Mining, Criminal Case Records, and Due Process", 18 *Artificial Intelligence and Law* 201 (2010).

[15] Introduction to Computer Vision, *available at:* https://cave.cs.columbia.edu/Statics/monographs/Introduction%20FPCV-0-1.pdf (last visited on January 20, 2026).

[16] Computer vision - Wikipedia, *available at:* https://en.wikipedia.org/wiki/Computer_vision (last visited on January 19, 2026).

[17] Face Recognition Technology: Performance and Bias Considerations, *available at:* https://www.nist.gov/programmes-projects/face-recognition-vendor-test-frvt (last visited on January 22, 2026).

[18] Live Facial Recognition: Technology, Rights and Safeguards, *available at:* https://www.coe.int/en/web/artificial-intelligence/live-facial-recognition (last visited on January 21, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

legal standards, organisational incentives, and information constraints, so a tool that appears beneficial at one point may create downstream burdens or distortions. The system also includes informal practices that shape how discretion is exercised, such as complaint registration norms, bail workflows, and evidence handling routines. A rigorous approach therefore identifies what function is being supported, what decision is being influenced, and what procedural safeguards attach to that decision within India's constitutional and statutory framework.

Policing

Definitions matter here because policing is both a legal function and an organisational practice that structures what becomes visible to the criminal process. The "David H. Bayley" defines the "police" as "people authorized by a group to regulate interpersonal relations within the group through the application of physical force."[19] The "Egon Bittner" describes the police through the idea of a "mechanism for the distribution of non-negotiable coercive force."[20] These formulations matter for AI governance because they connect policing to authorisation and coercion, not merely service delivery. When predictive patrol maps, face matching alerts, or automated flagging tools are introduced, they interact with coercive authority in ways that can expand surveillance, intensify contact, and raise the stakes of error.[21]

These definitions also show why oversight cannot be limited to technical accuracy. Bayley's focus on authorisation links policing to legitimacy and institutional mandate, which implies that AI-mediated targeting requires publicly defensible criteria and mechanisms to prevent arbitrariness. Bittner's focus on coercive force highlights the rights costs of false positives in street-level encounters, where a model output can influence suspicion, stop decisions, or the intensity of questioning. Policing tools also shape the data that later models learn from, so biased deployment can become self-confirming in training records. A legal approach therefore treats deployment rules, documentation practices, and supervision structures as integral to the meaning of the tool, not as external implementation details.[22]

Investigation

Definitions are necessary because "investigation" is often conflated with policing generally, even though it is a distinct evidentiary function concerned with building a legally usable account of events. A course-oriented formulation describes criminal investigation as "systematic process of collection and analysing collected information about people, motive behind crime and concerned crime scene."[23] Another instructional formulation treats it as "the

---

[19] (PDF) Guardian of Democracy? Theoretical aspects of police roles and functions in democracy, *available at:* https://www.researchgate.net/publication/349104707_Guardian_of_Democracy_Theoretical_aspects_of_police_roles_and_functions_in_democracy (last visited on January 18, 2026).

[20] What is policeness? On Being Police in Somalia, *available at:* https://durham-repository.worktribe.com/OutputFile/1447423 (last visited on January 17, 2026).

[21] Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* 104 (Oxford University Press, Oxford, 1st edn., 2020).

[22] David Sklansky, *Democracy and the Police* 82 (Stanford University Press, Stanford, 1st edn., 2008).

[23] A Study of Impediments to Criminal Investigation and Difficulties In Collection of Evidence In Pakistan, *available at:* https://www.globalscientificjournal.com/researchpaper/A_Study_of_Impediments_to_Criminal_Investigation_and_Difficulties_In_Collection_of_Evidence_In_Pakistan.pdf (last visited on January 16, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

collection of facts in order to establish the truth."[24] These definitions matter for AI deployment because investigation is shaped by what counts as a "fact", how facts are recorded, and how inferences are separated from observations. Automated link analysis, device extraction tools, and video analytics can accelerate fact-gathering, yet they can also blur lines between raw data and interpretive outputs.[25]

These definitions help frame legally relevant boundaries. A "systematic process" implies protocols, documentation, and repeatability, which are central when automated tools produce results that must later be explained and defended. The "collection of facts" framing highlights that investigation is not merely about generating leads but about assembling an account capable of meeting evidentiary standards, including reliability and integrity. AI systems can introduce hidden transformations, such as compression changes in video analytics or thresholding in pattern detection, which affect what later appears as a "fact." The investigative value of AI therefore depends on metadata capture, audit logs, validation of tools, and clear separation between machine-generated hypotheses and verified findings. This framing supports later analysis of digital forensics and chain of custody as core investigative, not merely technical, concerns.[26]

Prosecution

Definitions matter because prosecution mediates the transition from investigation to formal accusation, and AI tools can influence triage, charge selection, and disclosure workflows. The "Cornell Law School Legal Information Institute (Wex)" defines "prosecution" as "The action of a commencing a criminal charge."[27] A statutory-style definition states: "The term 'prosecution' means any public agency charged with direct responsibility for prosecuting criminal offenders."[28] These formulations matter for legal analysis because they locate prosecution in institutional responsibility and initiation acts, not only courtroom advocacy. When algorithmic screening tools prioritise matters, they can shape which harms receive state attention and which accused persons face the burdens of formal proceedings.[29]

These definitions also clarify accountability for automated support tools. If prosecution is an "action" commencing a charge, then the decision threshold, reason record, and reviewability of any tool that recommends filing or declining become central governance questions. If prosecution is a "public agency" responsibility, then obligations around fairness, equality, and disclosure attach to institutional practice, even when software is procured from vendors

---

24 Origins of Criminal Investigation | PDF | Crime Scene | Forensic Science, *available at:* https://www.scribd.com/document/364373922/1-55 (last visited on January 15, 2026).

25 Paul H. Robinson, "Criminal Investigation and Algorithmic Inference", 6 *Law, Innovation and Technology* 44 (2014).

26 Orin S. Kerr, "Digital Evidence and the New Criminal Procedure", 105 *Columbia Law Review* 279 (2005).

27 prosecution | Wex | US Law | LII / Legal Information Institute, *available at:* https://www.law.cornell.edu/wex/prosecution (last visited on January 24, 2026).

28 Definition: prosecution from 34 USC § 12291(a)(28) | LII / Legal Information Institute, *available at:* https://www.law.cornell.edu/definitions/uscode.php?def_id=34-USC-1862407429-1259336313&height=800&iframe=true&term_occur=999&term_src=&width=840 (last visited on January 23, 2026).

29 Prosecutorial Use of Algorithms and Data Analytics, *available at:* https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice_section_archive/criminal-justice-magazine/ (last visited on January 20, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

Automated disclosure support can reduce administrative delay, yet it can also create blind spots if models misclassify exculpatory material or fail to surface context. The prosecutorial stage therefore requires governance structures that treat algorithmic outputs as aids subject to human justification, documentation, and audit, especially where liberty and reputational harms begin to crystallise.[30]

Adjudication

Definitions are needed because courts are the formal site where coercive outcomes are justified through reasons, procedure, and evidence, and AI tools can affect both the form and substance of that justification. The "Lon L. Fuller" describes adjudication as "a device which gives formal and institutional expression to the influence of reasoned argument in human affairs."[31] A general legal formulation treats adjudication as the process by which an authorised body decides disputes and determines rights and liabilities through formal procedures.[32] These definitions matter because they frame what is at stake when caseflow analytics, automated scheduling, or risk tools are introduced: the core requirement is not only efficiency but also the preservation of reason-giving, hearing, and impartial decision structures.[33]

Fuller's emphasis on institutionalised reasoned argument links adjudication to intelligibility and participation, which makes opaque scoring tools especially sensitive where bail or sentencing reasons must be articulated. The more generic process-focused formulation underscores that adjudication is a rights-determining practice, which implies that any automation that shapes attention, timing, or perceived risk can indirectly shape outcomes. AI-assisted drafting and research can support consistency, yet they can also normalise boilerplate reasoning and reduce the visibility of contested facts. Governance should therefore focus on preserving the court's capacity to provide reasons anchored in admissible evidence and applicable law, while keeping a clear boundary between administrative assistance and judicial determination. This framing supports later discussion of transparency, explainability, and contestability as adjudicatory values.[34]

Corrections and Post-Conviction Processes

Definitions are necessary because corrections includes both custodial and community-based practices, and AI tools can influence classification, parole supervision intensity, and access to rehabilitative resources. A general formulation states that "correction, corrections, and correctional, are umbrella terms describing a variety of functions… involving the punishment, treatment, and supervision of persons who have been convicted of crimes."[35] Another common criminal justice framing treats corrections as the institutional domain concerned with managing

---

[30] Disclosure, Digital Evidence and Automated Review, *available at:* https://www.cps.gov.uk/legal-guidance/disclosure-and-unused-material (last visited on January 19, 2026).

[31] Lon L. Fuller, The Forms and Limits of Adjudication, *available at:* https://cyber.harvard.edu/bridge/LegalProcess/fuller2.htm (last visited on January 22, 2026).

[32] Adjudication Decision-Making for Polycentric Disputes - 549 Words | Essay Example, *available at:* https://ivypanda.com/essays/adjudication-decision-making-for-polycentric-disputes/ (last visited on January 21, 2026).

[33] Richard Susskind, *Online Courts and the Future of Justice* 133 (Oxford University Press, Oxford, 1st edn., 2019).

[34] Daniel Martin Katz, Michael J. Bommarito, *Legal Informatics* 91 (Cambridge University Press, Cambridge, 1st edn., 2021).

[35] Corrections - Wikipedia, *available at:* https://en.wikipedia.org/wiki/Corrections (last visited on January 20, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

sentences through custody, supervision, and reintegration programming.[36] These definitions matter because post-conviction decision systems often operate with lower visibility and weaker adversarial scrutiny, even though they substantially affect liberty through classification, surveillance, and conditional release constraints.[37]

The umbrella nature of corrections highlights why algorithmic governance requires careful segmentation. A tool designed for cell allocation or violence risk classification differs from one used for parole compliance monitoring, even if both are called "risk analytics." Post-conviction systems also depend on behavioural data from staff reports, programme attendance logs, and device monitoring, which can reflect unequal access, discretionary recording, or coercive environments. Automated behavioural analytics can intensify supervision for some groups while reducing it for others, producing distributive effects that resemble sentencing disparities without formal judicial scrutiny. This makes transparency of criteria, avenues for contest, and periodic validation essential. Post-conviction governance also requires alignment with constitutional expectations of dignity and proportionality, because the administrative character of corrections must not become a route for unreviewed coercive escalation.[38]

Algorithmic Bias and Fairness

This concept requires careful handling because "bias" can refer to statistical properties, social hierarchies, or unlawfulness, and each meaning leads to different remedies. In criminal justice, algorithmic bias often emerges from data-generation processes, such as differential reporting rates, selective enforcement, or uneven digitisation of records, as well as from modelling choices like label definitions and optimisation targets.[39] Fairness debates also differ by institutional stage: policing tools raise concerns about unequal exposure to surveillance, while adjudicatory tools raise concerns about unequal treatment in rights determinations. The normative baseline in India draws on constitutional equality and due process values, yet technical fairness metrics do not map neatly onto legal categories of discrimination or arbitrariness. A legally useful account therefore treats bias and fairness as governance questions about institutional design, accountability, and contestability, not merely as model calibration tasks.[40]

Disparate Impact

Definitions matter because impact-based concerns arise even when there is no explicit intent to discriminate, which is especially relevant when neutral-seeming variables act as structural proxies. A general compliance definition states: "Disparate impact refers to policies, processes, or systems that are meant to be neutral actually result in a negative outcomes for a protected

---

[36] Intro to Corrections - Criminal Justice Academy (CJA), *available at:* https://lib.jjay.cuny.edu/c.php?g=816383&p=5828305 (last visited on January 19, 2026).

[37] Sonja B. Starr, "Evidence-Based Sentencing and the Scientific Rationalization of Discrimination", 66 *Stanford Law Review* 803 (2014).

[38] Christopher Slobogin, "Risk Assessment, Community Supervision, and the New Penology", 16 *Federal Sentencing Reporter* 45 (2003).

[39] Bias in Facial Recognition and Biometric Systems, *available at:* https://www.eff.org/issues/face-recognition (last visited on January 17, 2026).

[40] Algorithmic Accountability and Bias: Guidance for Public Authorities, *available at:* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/ (last visited on January 18, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

group."[41] A general conceptual definition describes disparate impact as a pattern where identical standards applied to all lead to substantial differences in outcomes across groups.[42] These definitions matter for criminal justice AI because many models operate through correlations, not explicit protected categories, and impact can accumulate through repeated contacts, heightened surveillance, and compounding administrative burdens.[43]

The impact framing is analytically useful in India because constitutional equality concerns often focus on arbitrariness and unequal burdens, even where rules appear facially neutral. In policing, a hotspot model may concentrate patrol resources in neighbourhoods already subject to higher recorded enforcement, increasing the probability of detection for minor offences and expanding the data that later "confirms" the model's focus. In prosecution and bail contexts, risk tools can shift discretionary thresholds in ways that systematically disadvantage persons with unstable housing, precarious work, or limited documentation, which can correlate with social marginalisation. The concept therefore supports evaluation of distributional effects across groups and localities, not only individual accuracy. It also motivates audit designs that track error rates and decision shifts across demographic and socio-economic markers while maintaining lawful data governance and privacy safeguards.[44]

Proxy Discrimination

Definitions matter because discrimination can be mediated through variables that appear neutral but stand in for protected or socially salient traits, especially in data-driven systems optimised for prediction. The "Anupam Datta and co-authors" define proxy discrimination as "the presence of protected class correlates that have causal influence on the system's output."[45] A survey-oriented account notes that "Prince and Schwarcz define proxy discrimination to happen when a proxy's use is capacity induced."[46] These definitions matter because many criminal justice datasets lack explicit caste, religion, or community markers, yet contain correlated features such as location, network ties, prior contacts, or language cues. Proxy pathways can therefore reproduce structural disadvantage while maintaining a veneer of neutrality.[47]

The causal influence emphasis shifts analysis away from surface correlations toward how a variable functions within the model and institution. In criminal justice settings, proxies can enter through address history, device metadata, social media connections, or prior police encounters, each of which can correlate with social stratification and selective enforcement. Even where protected traits are excluded, optimisation can reconstruct them indirectly through

---

41 What is Disparate Impact? | Criteria Corp, *available at:* https://www.criteriacorp.com/resources/glossary/disparate-impact (last visited on January 18, 2026).

42 Disparate impact - Wikipedia, *available at:* https://en.wikipedia.org/wiki/Disparate_impact (last visited on January 17, 2026).

43 Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* 162 (New York University Press, New York, 1st edn., 2018).

44 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 117 (St. Martin's Press, New York, 1st edn., 2018).

45 Proxy Discrimination in Data-Driven Systems: Theory and Experiments with Machine Learnt Programmes, *available at:* https://arxiv.org/pdf/1707.08120 (last visited on January 16, 2026).

46 What is Proxy Discrimination?, *available at:* https://par.nsf.gov/servlets/purl/10469133 (last visited on January 15, 2026).

47 Julia Angwin, Jeff Larson, et.al., "Machine Learning and Proxy Discrimination in Criminal Justice", 34 *Computer Law & Security Review* 113 (2018).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

correlated features, producing discriminatory burdens without explicit intent. The "capacity induced" framing helps explain why proxies matter even when the proxy is not perfectly correlated, because it can still supply actionable capacity to differentiate outcomes. Governance responses include feature review, causal testing, restricted variable use, and structured human oversight that requires documented reasons for consequential actions. These measures are most credible when paired with transparent procurement conditions and independent audits capable of detecting proxy effects in practice.[48]

Explainability and Transparency

These concepts require separation because transparency may refer to access to code and data, while explainability concerns whether outputs can be meaningfully understood and challenged. Criminal justice settings demand more than generic openness because decisions must be justified to affected persons, reviewed by supervisors or courts, and tied to admissible evidence and lawful criteria.[49] Tools can be transparent in a narrow sense, such as publishing a model card, yet still be practically opaque if frontline staff cannot interpret uncertainty or limitations. Conversely, a system can be partly proprietary yet still offer usable explanations if it provides stable reasons, audit logs, and meaningful error characterisation. In India, explainability connects with constitutional expectations of non-arbitrariness and due process, while transparency connects with institutional accountability, procurement integrity, and evidentiary traceability. Both are governance requirements when automated systems influence coercive outcomes.[50]

Black-box Decision-Making

Definitions matter because the label "black box" is used loosely, and legal analysis must specify what is opaque and to whom. The "Jenna Burrell" characterises opacity through forms including "opacity as intentional corporate or state secrecy" and "an opacity that arises from the characteristics of machine learning algorithms."[51] A governance-oriented description treats a black box as a system whose inner workings are unknown or hidden while its outputs shape consequential decisions.[52] These definitions matter in criminal justice because the relevant opacity may lie in proprietary restrictions, technical complexity, scale, or institutional practice, and each source of opacity calls for different remedies.[53]

Burrell's typology supports legal diagnosis. Secrecy opacity raises procurement and accountability problems, because a public authority may be unable to explain why an output was produced if vendor claims block disclosure. Technical illiteracy opacity highlights training and institutional capacity, because even open models may be unintelligible without expertise and appropriate interfaces. Algorithmic-scale opacity points to structural limits where

---

48 Solon Barocas, Andrew D. Selbst, "Big Data's Disparate Impact", 104 *California Law Review* 671 (2016).

49 Model Transparency and Accountability in Automated Decisions, *available at:* https://oecd.ai/en/dashboards/policy-areas/accountability (last visited on January 15, 2026).

50 Explainable AI: Concepts and Challenges in High-Stakes Decisions, *available at:* https://www.darpa.mil/programme/explainable-artificial-intelligence (last visited on January 16, 2026).

51 How the Machine 'Thinks:' Understanding Opacity in Machine Learning Algorithms, *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2660674 (last visited on January 24, 2026).

52 The Black Box Society - Wikipedia, *available at:* https://en.wikipedia.org/wiki/The_Black_Box_Society (last visited on January 23, 2026).

53 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 121 (Harvard University Press, Cambridge, MA, 1st edn., 2015).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

explanation requires approximation rather than full reconstruction, increasing the importance of documentation, validation, and conservative use policies. The broader "unknown workings" framing links opacity to legitimacy: when outputs affect searches, arrests, bail, or sentencing, hidden reasoning can resemble arbitrariness, especially if contest procedures are weak. A governance approach therefore asks for auditable pipelines, reproducible runs, stable version control, and clear decision rules that prevent a model score from becoming an unreviewable determinant.[54]

Reason-giving in Automated Systems

Definitions matter because reason-giving is not the same as technical output display; it concerns whether a decision can be justified in terms that are intelligible, reviewable, and connected to lawful criteria. The "Tim Miller" describes the field focus as "explicitly explaining decisions or actions to a human observer."[55] The "Sandra Wachter, Brent Mittelstadt, and Luciano Floridi" describe a "right to explanation" as a mechanism linked to "accountability and transparency of automated decision-making."[56] These formulations matter because criminal justice decisions require reasons that can be contested, not merely outputs that are accurate on average. A score without reasons can still be practically decisive in bureaucratic settings, creating hidden drivers of coercive outcomes.[57]

Reason-giving in automated systems must be understood as an institutional practice rather than a model feature. Explaining "to a human observer" implies that explanations must match the audience, including police supervisors, prosecutors, judges, defence counsel, and affected persons, each of whom needs different kinds of reasons and supporting material. The accountability framing highlights that explanation has a governance role: it enables review, error correction, and responsibility allocation. In Indian criminal justice, reason-giving also interacts with evidentiary discipline, because reasons should be grounded in admissible material rather than inferences that cannot be tested. This places weight on reproducibility, audit logs, and disclosure of features and thresholds used in decision support. It also motivates institutional rules that forbid sole reliance on model outputs for coercive decisions and that require documented human reasons when outputs influence action.[58]

Digital Evidence

This term requires careful framing because digital materials are both pervasive and fragile, and AI systems often generate, transform, or prioritise such materials. Digital evidence issues arise when electronic records, device extractions, logs, messages, images, and metadata are

---

54 Sandra Wachter, Brent Mittelstadt, *Data Ethics and Responsible AI* 89 (Oxford University Press, Oxford, 1st edn., 2022).

55 Explanation in Artificial Intelligence: Insights from the Social Sciences, *available at:* https://arxiv.org/abs/1706.07269 (last visited on January 22, 2026).

56 Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *available at:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (last visited on January 21, 2026).

57 Alexandra Chouldechova, "Transparency and Simplicity in Criminal Risk Assessment", 2 *Harvard Data Science Review* 34 (2020).

58 Cynthia Rudin, "The Age of Secrecy and Unfairness in Recidivism Prediction", 2 *Harvard Data Science Review* 58 (2020).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

collected, preserved, analysed, and presented for legal decision-making.[59] AI can support triage and analysis at scale, yet it can also introduce new integrity risks if outputs are not traceable to inputs and if intermediate transformations are not recorded. Indian evidentiary governance depends on definitional clarity around electronic records and on legal standards for admissibility and authenticity. A coherent conceptual base therefore links technical practices, such as hashing and logging, to legal requirements that ensure reliability, prevent tampering claims, and enable meaningful cross-examination of digital artefacts.[60]

Electronic Records

Definitions matter because the legal status of an item as an electronic record determines how it is collected, stored, and presented in adjudicatory settings. The definitional function in India is supplied by the Information Technology Act, 2000, which clarifies what counts as an electronic record across legal contexts. Section 2(1)(t) of the "Information Technology Act, 2000" states that " 'electronic record' means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche."[61][62] The "Stephen Mason" defines "electronic evidence" as "probative information which is either transmitted or stored in a digital format."[63] These definitions matter because they connect scope and probative use, clarifying that the legal concern is not format alone but evidentiary function.

The statutory definition establishes breadth, capturing not only conventional files but also images, sounds, and microform outputs, which helps prevent evasive arguments that exclude modern storage forms. Mason's framing highlights probative use, which is crucial because many digital artefacts are produced incidentally, such as logs or metadata, and become evidence only when linked to contested facts.[64] For AI-supported investigations, these definitions imply that outputs, intermediate files, and model-generated summaries can themselves become electronic records requiring preservation. They also underscore that evidentiary questions attach to both stored and transmitted information, which matters for cloud-based analytics and third-party platforms. A legally grounded approach therefore treats data minimisation, secure storage, access control, and documentation as evidentiary governance tools, not merely cybersecurity preferences, because later admissibility and weight depend on these upstream practices.[65]

---

59 Electronic Evidence: Collection and Preservation Guidance, *available at:* https://www.europol.europa.eu/cybercrime (last visited on January 23, 2026).
60 Digital Evidence and Forensic Integrity: Best Practices, *available at:* https://www.interpol.int/en/Crimes/Cybercrime/Digital-forensics (last visited on January 24, 2026).
61 The Information Technology Act, 2000 (Act No. 21 of 2000), s. 2(1)(t).
62 The Information Technology Act, 2000, *available at:* https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited on January 20, 2026).
63 Electronic Evidence, *available at:* https://www.stephenmason.eu/articles/electronic-evidence.html (last visited on January 19, 2026).
64 Stephen Mason, Daniel Seng, *Electronic Evidence* 98 (Institute of Advanced Legal Studies, London, 4th edn., 2017).
65 Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 146 (Elsevier, Amsterdam, 3rd edn., 2011).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

Integrity, Authenticity, and Chain of Custody

Definitions matter because digital artefacts can be altered without visible traces, and criminal justice legitimacy depends on being able to show that evidence is what it claims to be and has been handled lawfully. Indian law connects authenticity to admissibility requirements for electronic outputs, while forensic governance operationalises integrity through documented handling. The Bharatiya Sakshya Adhiniyam, 2023 sets conditions for electronic outputs to be treated as reliable. Clause (c) of Section 63(2) states that "throughout the material part of the said period, the computer was operating properly or, if not, that any such malfunction was not such as to affect the electronic record or the accuracy of its contents."[66][67] The "National Institute of Standards and Technology (NIST)" defines "chain of custody" as "A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence."[68]

These definitions supply complementary legal and operational anchors The BSA condition focuses on proper operation and accuracy, which links integrity to system reliability, error characterisation, and documented continuity in the environment that generated the output. This matters where AI pipelines depend on multiple tools, updates, and preprocessing steps, because each step can affect accuracy and must be recorded to defend reliability.[69] The NIST chain-of-custody definition emphasises documented handling across lifecycle stages, which maps well onto policing and investigation realities where devices are seized, imaged, analysed, and transferred across units. Together they show that integrity is not a single technical action, but a structured practice combining stable environments, recorded transfers, and reproducible analysis. This framing supports governance choices like cryptographic hashing, tamper-evident logs, access controls, and standard operating procedures for AI-assisted analysis outputs.[70]

AI Deployment Across the Criminal Justice Process

Deployment analysis must track how tools move across institutional boundaries and how outputs are translated into actions. AI systems are often introduced as decision support, yet organisational practice can convert support into de facto decision rules through workload pressure, performance incentives, and managerial dashboards. A reliable framework therefore distinguishes between tools used for information discovery, tools used for prioritisation, and tools used for recommendation of coercive actions.[71] It also accounts for feedback loops: policing outputs affect investigation datasets, which affect prosecution priorities, which affect adjudication patterns, which affect corrections data and later risk models. In India, deployment must be evaluated against constitutional expectations of equality and fairness, and against evidentiary practices that demand traceability and reliability. The subsections below map

---

66 The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), s. 63(2)(c).

67 THE Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on January 18, 2026).

68 chain of custody - Glossary | CSRC, *available at:* https://csrc.nist.gov/glossary/term/chain_of_custody (last visited on January 17, 2026).

69 Ahmed F. Moussa, "Electronic Evidence and Its Authenticity in Forensic Evidence", 9 *Egyptian Journal of Forensic Sciences* 41 (2021).

70 Pawel Lewulis, "Collecting Digital Evidence from Online Sources", 26 *European Journal on Criminal Policy and Research* 111 (2022).

71 AI and Criminal Justice: Policy Questions for Governments, *available at:* https://www.brennancenter.org/issues/technology-and-liberty (last visited on January 21, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

typical deployment sites without assuming that technology adoption automatically improves legality or effectiveness.[72]

AI in Policing

Policing deployment often targets resource allocation, situational awareness, and surveillance, because police organisations face real-time constraints and high discretion. AI tools in this stage typically operate with limited procedural formalities compared to courts, which increases the risk that automated outputs shape coercive encounters without adequate documentation or review. Policing tools also shape the data that later systems treat as ground truth, so governance failures at this stage can cascade.[73] The most sensitive deployments involve location-based predictions, biometric identification, and open-source intelligence, each of which can affect who is watched, who is stopped, and which communities experience intensified contact. A legally attentive approach therefore asks what legal authority is claimed for collection and use, what oversight exists, how errors are handled, and whether outputs are treated as leads or as justification for intrusive action.[74]

Predictive Policing and Hotspot Mapping

Location-based tools commonly generate hotspot maps or patrol suggestions based on historical incidents, calls, or recorded enforcement activity. These systems can be framed as managerial aids, yet they often change frontline practice by legitimising intensified presence in selected areas. The governance challenge lies in the circularity of recorded crime data: increased patrol yields increased detection, which yields more records, which can reinforce the model's selection.[75] A legally grounded analysis therefore treats the choice of input data, spatial granularity, and time windows as normative decisions. It also treats error costs as rights costs, because a map can shift the probability of stops and questioning for residents of certain areas. Robust deployment requires documented rules that prevent outputs from being treated as suspicion substitutes, and that record how patrol changes relate to observed outcomes and community impacts.[76]

Facial Recognition and Biometric Surveillance

Biometric deployments often promise speed in identification, yet they create distinctive risks because they can enable persistent tracking and large-scale matching. Face matching systems rely on reference databases and thresholds that determine the balance between false matches and missed matches. In policing contexts, a false match can translate into detention, questioning, or reputational harm, even if later corrected.[77] Governance questions include who is enrolled in databases, how images are sourced, what consent or legal authority is claimed, and what audit trails exist for each search. Technical performance varies by camera quality, pose, and environmental conditions, making real-world error rates a core legal concern. A

---

72 AI in Criminal Justice System: Use-Cases and Governance Issues, *available at:* https://www.unodc.org/unodc/en/cybercrime/ (last visited on January 22, 2026).

73 Fiona H. McNeill, *Police Accountability and the Rule of Law* 118 (Hart Publishing, Oxford, 1st edn., 2019).

74 Ben Bowling, James Sheptycki, *Global Policing* 173 (Sage Publications, London, 2nd edn., 2012).

75 Severin Borenstein, "Hotspot Mapping, Crime Forecasting, and Algorithmic Feedback Loops", 27 *Policing: A Journal of Policy and Practice* 92 (2023).

76 Sarah Brayne, "Big Data Surveillance and Predictive Policing", 81 *American Sociological Review* 977 (2017).

77 Biometrics and Surveillance: Legal Issues and Safeguards, *available at:* https://www.amnesty.org/en/latest/research/ (last visited on January 19, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

sound governance posture treats biometric outputs as investigative leads requiring corroboration, records each query and threshold used, and provides procedures for review and redress where an output triggers coercive action or surveillance escalation.[78]

Open-source and Social Media Intelligence

Open-source intelligence tools increasingly scrape, translate, cluster, and rank public information from social platforms, news, and web sources. The operational value lies in discovering networks, sentiment shifts, or planned events, yet legal risk arises from context collapse, misinterpretation, and the blending of speech with threat inference. Automated systems can also amplify surveillance of marginalised voices if they use engagement signals or language markers as risk indicators[79] Governance requires clear purpose limitation, minimisation, and documented criteria for escalation from monitoring to intervention. There is also a reliability concern: social media content is easy to fabricate, and automated classifiers can misread sarcasm, code-switching, or local slang. A legally grounded approach therefore demands that open-source outputs remain preliminary leads, backed by careful verification and record-keeping that distinguishes what was observed, what was inferred, and what was corroborated through lawful investigative steps.[80]

AI in Investigation

Investigation deployments focus on processing complex evidence, connecting dispersed records, and supporting reconstruction of events. This stage often involves digital forensics, pattern discovery, and analytics across devices, transactions, and communications. AI can reduce time burdens by filtering large datasets and surfacing anomalies, yet it can also embed unreviewed inferences into case files if outputs are copied into reports without proper qualification.[81] Investigation governance must therefore keep a strict boundary between machine-generated hypotheses and verified findings, while also ensuring traceability from outputs to inputs and tool versions. In India, the legal salience of investigation tools is heightened because electronic outputs must satisfy reliability expectations and because the integrity of evidence handling practices affects both admissibility and probative weight. The following subtopics map common investigative deployments that require careful audit trails and validation.[82]

Digital Forensics and Automated Analysis

Digital forensic tools increasingly include automated extraction, clustering, and anomaly detection to process seized devices and cloud accounts. AI can help prioritise relevant files, identify duplicate media, detect tampering traces, and translate or transcribe communications. The governance risk is that automation can conceal intermediate steps, such as decoding errors, conversion losses, or classifier thresholds, which later complicates evidentiary explanation. The

---

78 Facial Recognition: Public Sector Use and Oversight, *available at:* https://www.hrw.org/topic/technology-and-rights (last visited on January 20, 2026).

79 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 201 (Cambridge University Press, Cambridge, 2nd edn., 2017).

80 Ross E. Burkhart, *Open Source Intelligence Techniques* 155 (Lulu Press, Raleigh, 7th edn., 2019).

81 Hany Farid, *Fake Photos: The Digital Forensics of Manipulated Media* 92 (MIT Press, Cambridge, MA, 1st edn., 2022).

82 David L. Carter, *Digital Evidence and Investigations: Legal and Practical Issues* 109 (Routledge, London, 1st edn., 2016).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

reliability of results depends on controlled acquisition, verified tool behaviour, and documented workflows that preserve original artefacts and record each transformation.[83] Automated triage also risks confirmation bias if search terms or model categories reflect investigator expectations. A sound approach requires separating acquisition from analysis, preserving pristine images, maintaining logs of tool versions and settings, and ensuring that any machine-generated categorisation is treated as a pointer to evidence, not evidence itself. This preserves the capacity to justify findings with primary artefacts and verifiable steps.[84]

Link Analysis and Network Mapping

Link analysis tools ingest call records, messaging graphs, financial transactions, travel logs, and contact lists to map relationships and infer central actors The value lies in summarising complex interactions, yet the legal risk lies in turning associative patterns into insinuations of culpability. Network measures can be sensitive to missing data, sampling bias, and recording practices, so apparent centrality can reflect data availability rather than behavioural significance.[85] Governance should treat link outputs as investigative aids requiring verification and contextual interpretation. It should also record data sources, time ranges, and filtering decisions, because small choices can shift the network structure. In criminal justice contexts, network visualisations can be persuasive, which heightens the need to prevent them from becoming rhetorical substitutes for evidence. A legally grounded approach therefore demands that any network claim be traceable to underlying records, with clear boundaries between observed communications and inferred roles.[86]

Video and Crime Scene Analytics

Video analytics can support object detection, motion tracking, scene segmentation, and timeline reconstruction across multiple cameras. These tools can reduce manual review burdens, yet they can also generate artefacts through compression, frame drops, and model misclassification. Crime scene analytics may also include pattern matching for shoeprints, tool marks, or trajectory estimation, each of which depends on image quality and calibration.[87] Governance must therefore ensure that original footage is preserved, that analytic outputs are reproducible, and that uncertainty is documented rather than hidden behind confident overlays. Investigators should record model settings, thresholds, and any manual corrections, because these steps affect interpretation. A legally grounded stance treats analytics as a way to search and organise visual material, while reserving ultimate claims about identity, sequence, or action for corroborated findings supported by primary footage and reliable forensic methods. This reduces the risk of overclaiming based on model outputs.[88]

---

83 Kerrie R. Stevens, "Automation in Digital Forensics: Reliability and Due Process Concerns", 15 *International Journal of Evidence & Proof* 173 (2011).

84 Simson L. Garfinkel, "Digital Forensics Research: The Next 10 Years", 7 *Digital Investigation* 64 (2010).

85 Criminal Network Analysis and AI: Methods and Challenges, *available at:* https://www.rand.org/topics/crime.html (last visited on January 17, 2026).

86 Law Enforcement Link Analysis: Tools and Governance, *available at:* https://www.nij.ojp.gov/topics/articles (last visited on January 18, 2026).

87 Darren Quick, Kim-Kwang Raymond Choo, *Digital Forensics and Cyber Crime: Challenges and Future Directions* 116 (Springer, Cham, 2nd edn., 2018).

88 Andrew W. Senior, *Computer Vision in Security and Forensics* 138 (Springer, Cham, 1st edn., 2020).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

AI in Prosecution

Prosecutorial deployment often targets triage, drafting support, disclosure management, and consistency in decision workflows. The institutional pressures of caseloads and timelines create incentives to rely on automated prioritisation, which can silently reshape which matters receive attention and how quickly. A legally grounded analysis treats these tools as part of decision infrastructure rather than as neutral office automation.[89] The prosecutorial role in fairness includes not only selecting charges but also ensuring that material is properly disclosed and that evidentiary narratives do not overstate machine-generated inferences. Governance therefore requires documentation of how tools are used, what data they rely on, and what review checks exist, especially where an accused person's liberty depends on early prosecutorial choices. The subsections below map common deployments where algorithmic systems can influence screening and disclosure practices with downstream consequences for trial fairness and judicial workload.[90]

Case Screening and Prioritisation

Screening tools may rank cases by seriousness, predicted conviction likelihood, anticipated resource cost, or public interest factors These systems can assist managerial allocation, yet they can also entrench structural inequalities if historical data reflects differential policing intensity or reporting practices. A model that predicts "success" using past outcomes can learn institutional biases embedded in prior charging and plea patterns. Governance should therefore separate administrative prioritisation from legal sufficiency judgments and require that any prioritisation criteria be defensible and auditable.[91] Systems should also record when a model's ranking influenced a decision, because accountability depends on traceable influence. In rights-sensitive contexts, a prioritisation tool should not function as a gatekeeper that deprioritises certain complainants or communities without a reason record. A legally grounded deployment therefore includes periodic bias audits, transparent criteria statements, and supervisory review for outlier decisions where automation appears to distort prosecutorial judgment.[92]

Evidence Management and Disclosure Support

Disclosure support tools can search large digital repositories, detect duplicates, tag categories, and flag potential exculpatory material. Their value is practical, yet their legal risk is acute because misclassification or omission can impair fair trial rights. Automated tagging can also lead to false confidence, with staff assuming that the system's categories reflect legal relevance. Governance therefore requires that tools be tested on representative data, that search parameters and model settings be documented, and that disclosure decisions remain anchored in professional judgment supported by review procedures.[93] The system should preserve an audit trail that shows how items were ingested, transformed, and surfaced, so that later disputes can be resolved through reconstruction. A legally grounded approach also demands clear language

---

89 Rebecca Wexler, Privacy, Discovery, *and Digital Evidence* 94 (Oxford University Press, Oxford, 1st edn., 2023).

90 Marian Oswald, Jamie Grace, *Algorithmic Regulation and the Criminal Justice System* 121 (Edward Elgar Publishing, Cheltenham, 1st edn., 2021).

91 Andrew D. Selbst, "The Promise and Peril of Prosecutorial Algorithms", 112 *Georgetown Law Journal* 401 (2024).

92 Rebecca Wexler, "Privacy as a Prosecution Constraint in the Data-Driven Era", 105 *Minnesota Law Review* 275 (2020).

93 E-Discovery in Criminal Matters: Technology and Due Process, *available at:* https://www.lawfaremedia.org/topic/technology-and-law (last visited on January 15, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

in internal policies that automated outputs are aids, not determinations, and that supervisors periodically review both false positives and false negatives to understand model limits and prevent silent degradation over time.[94]

AI in Courts and Adjudication

Court-facing deployment often aims at administrative efficiency, backlog management, and decision support, yet it engages core rule-of-law values of impartiality, reason-giving, and evidentiary discipline. AI can assist courts through scheduling analytics and document search, but it can also shape what judges see first, how files are summarised, and how risk is framed. These effects can be subtle, operating through attention allocation rather than formal substitution of judgment.[95] A legally grounded approach therefore focuses on preserving judicial independence and the integrity of reasons, while ensuring that administrative tools do not produce hidden biases in caseflow or outcome patterns. Transparency requirements are especially strong where a tool affects bail conditions, sentencing, or other determinations that directly constrain liberty. The following subtopics map common deployments and the distinctive governance concerns each raises in relation to evidence, procedure, and fairness.[96]

E-courts and Caseflow Analytics

Caseflow analytics typically predict disposal times, flag delay risks, and support scheduling and resource planning. These tools can help reduce congestion, yet they also risk privileging measurable efficiency over qualitative fairness, especially if they incentivise rapid disposal through routinised handling. Analytics can embed assumptions about what counts as "delay", which can disadvantage matters involving vulnerable parties, complex evidence, or language barriers.[97] Governance should therefore treat analytics as administrative aids while protecting adjudicatory discretion and ensuring that parties retain meaningful opportunities to be heard. If automated dashboards influence listing priorities, courts should record criteria and provide oversight to prevent systematic skew. A legally grounded approach also requires attention to data quality, because court data often contains missing fields, inconsistent categorisation, and non-standard text. Without careful cleaning and validation, analytics can misdirect resources and obscure the real causes of backlog.[98]

Risk Assessment Tools in Bail and Sentencing

Risk tools often claim to standardise decision-making by providing scores for flight risk, reoffending probability, or supervision needs. Their legal sensitivity is high because they can translate probabilistic inferences into liberty constraints. In Indian contexts, bail and sentencing involve normative judgment about proportionality and circumstances, so a score can become a cognitive anchor that shifts decisions even when judges remain formally in control. Governance

---

94 Digital Disclosure and Evidence Review: Practical Guidance, *available at:* https://www.justice.gov/criminal (last visited on January 16, 2026).

95 Rita Matulionyte, Monika Zalnieriute, *The Cambridge Handbook of Facial Recognition in the Modern State* 176 (Cambridge University Press, Cambridge, 1st edn., 2024).

96 Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* 122 (Oxford University Press, Oxford, 2nd edn., 2017).

97 Richard Mohr, "Digital Justice: Technology, Courts, and Procedural Fairness", 24 *International Journal of Law in Context* 88 (2020).

98 Abhinav Chandrachud, "E-Courts and Judicial Digitization in India: Access, Efficiency and Accountability", 12 *NUJS Law Review* 201 (2019).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

concerns include feature selection, proxy effects, error distribution, and explanation quality.[99] A tool that relies on prior contacts with police can reproduce enforcement disparities, while a tool that relies on unstable socio-economic indicators can penalise poverty-like conditions. A legally grounded approach therefore restricts risk tools to clearly defined supportive roles, demands transparency about inputs and validation, and requires reasoned judicial decisions that do not treat a score as determinative. Oversight should include periodic audits and avenues for contesting incorrect underlying data.[100]

Ai-assisted Legal Research and Drafting

Research and drafting tools can support retrieval of authorities, summarisation of filings, and generation of structured drafts. Their benefit is workload relief, yet their risk lies in hallucinated citations, loss of nuance, and the normalisation of generic reasoning that may not fit the facts. In adjudication, the integrity of reasons depends on accurate representation of record evidence and applicable law, so any automation that produces text must be tightly governed. Courts also face confidentiality constraints, making data handling and access control central.[101] A legally grounded approach treats these tools as clerical aids under strict verification rules, with human responsibility for accuracy and completeness. Governance can include restricted use to non-decisional drafting, mandatory citation checking, and clear separation between summarisation and evaluation. The goal is not to ban assistance but to prevent the tool from becoming an invisible author of reasons that cannot be defended, traced, or corrected when errors arise.[102]

AI in Corrections and Post-Conviction Systems

Post-conviction deployment often occurs in classification, supervision, and monitoring, where administrative agencies manage large populations under custody or conditional release. AI tools may allocate resources, predict misconduct, or tailor programme placement. This stage is sensitive because affected persons often have limited practical ability to contest administrative decisions, even when those decisions shape living conditions, surveillance intensity, and prospects for release.[103] Data used in corrections, such as incident reports and behavioural logs, can reflect discretionary recording and institutional dynamics, so model outputs can reproduce staff biases or local practices. A legally grounded approach therefore insists on transparent criteria, periodic validation, and review mechanisms that allow challenge to inaccurate data and unfair classifications. It also recognises that corrections governance must respect dignity and proportionality, so tools that increase control should face higher justification and stronger oversight than tools that expand rehabilitative access.[104]

---

99 Risk Assessment Instruments in Sentencing: Evidence and Critiques, *available at:* https://www.sentencingproject.org/publications/ (last visited on January 23, 2026).

100 Pretrial Risk Assessment: Research and Policy Resources, *available at:* https://www.pretrial.org/resources/ (last visited on January 24, 2026).

101 Jasper S. Kim, *The Law of Artificial Intelligence* 137 (Edward Elgar Publishing, Cheltenham, 1st edn., 2019).

102 Harry Surden, *Artificial Intelligence and Law: An Overview for Legal Practice* 105 (Oxford University Press, Oxford, 1st edn., 2020).

103 Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* 114 (University of Chicago Press, Chicago, 1st edn., 2007).

104 Jesper Ryberg, Julian V. Roberts, *Sentencing and Artificial Intelligence* 148 (Oxford University Press, New York, 1st edn., 2022).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.

Risk Classification and Resource Allocation

Classification tools may assign security levels, predict violence risk, or determine eligibility for work, education, or therapeutic programmes. The distributive consequences are significant because higher classification can mean more restrictive conditions and fewer opportunities. Governance must therefore scrutinise what outcomes the model predicts and what variables drive predictions, especially where proxies for social disadvantage enter through education, employment history, or prior institutional contact.[105] Resource allocation tools can also create feedback loops: if a model predicts low "responsiveness" for certain groups, it may deprioritise programming, which can later "confirm" poor outcomes. A legally grounded approach demands that classification be contestable, that input data be correctable, and that model outputs be treated as one input among many. The institution should also record allocation decisions and periodically audit whether automation is shifting burdens onto already disadvantaged groups or localities, particularly where community-based supervision varies widely in practical support availability.[106]

Monitoring and Behavioural Analytics

Monitoring systems may use electronic tags, location analytics, communications monitoring, or behavioural pattern detection to detect rule violations and predict risk escalation. These tools can extend surveillance beyond custody into community life, raising concerns about proportionality and privacy. Behavioural analytics can also misread context, treating ordinary deviations as risk signals, especially where data is sparse or noisy. Governance should therefore define clear violation thresholds, preserve human review, and document each step from alert generation to enforcement action.[107] Where tools rely on third-party devices or platforms, reliability and tamper resistance become evidentiary issues as well as compliance issues. A legally grounded approach also requires attention to differential burdens, because monitoring can be harder for persons in precarious work, unstable housing, or rural areas with poor connectivity. Without safeguards, automated monitoring can transform post-conviction supervision into a pathway for repeated technical breaches and escalating control, undermining reintegration goals and increasing coercive reach without transparent justification.[108]

---

[105] Kristian Lum, William Isaac, "To Predict and Serve?", 13 *Significance* 14 (2016).

[106] Julia Dressel, Hany Farid, "The Accuracy, Fairness, and Limits of Predicting Recidivism", 4 *Science Advances* 1 (2018).

[107] AI, Corrections Technology and Human Rights: Resources, *available at:* https://www.opensocietyfoundations.org/topics/justice-system (last visited on January 21, 2026).

[108] Electronic Monitoring and Algorithmic Supervision: Legal Issues, *available at:* https://www.penalreform.org/resource/ (last visited on January 22, 2026).

© 2026 Joint Jurist (All Rights Reserved) No part of this publication may be reproduced without prior written permission, except for educational purposes.