ISSN (Print): 1060-6076
ISSN (Online): Applied

The Journal of African Development
2026; Vol 7: Issue 1
https://www.afea-jad.com/

Algorithmic Evidence in Criminal Trials: Comparative Admissibility, Disclosure, and Challenge Rights

Dr Shubhankar Paul [1], Ms Tuhina Sinha [2], Priya Chaudhari[3], Srija Mondal[4]

[1]Assistant Professor, Amity University Jharkhand.

E-mail: shubhankarp2@gmail.com

[2.] Assistant Professor, Amity University Jharkhand.

[3.] Assistant Professor, Amity University Jharkhand.

[4]Srija Mondal, Research Scholar, Amity University Jharkhand

Cite This Paper as: Dr Shubhankar Paul , Ms Tuhina Sinha , Priya Chaudhari, Srija Mondal (2026) Algorithmic Evidence in Criminal Trials: Comparative Admissibility, Disclosure, and Challenge Rights. The Journal of African Development l, Vol.7, No.1, 663-673

KEYWORDS

algorithmic evidence, criminal trials, disclosure, expert evidence, facial recognition, probabilistic genotyping, fair trial

ABSTRACT

Algorithmic evidence is moving from the police workstation to the criminal courtroom. Facial recognition outputs, probabilistic genotyping likelihood ratios, risk scores, and tool-generated investigative leads now shape arrest, charging, bail, plea bargaining, and, increasingly, proof at trial. Yet criminal procedure still assumes that evidence is either human testimony or a readable artefact whose reliability can be tested through disclosure and cross-examination. This paper argues that courts must examine not only the algorithm's final result, but also the full process that produced it, because that process decides whether the result is trustworthy. Through doctrinal and comparative analysis of India, the European human rights and data protection framework, the United Kingdom's disclosure and expert evidence regime, and the United States' Daubert and Frye reliability gatekeeping, the paper develops a three-part account. First, admissibility must demand demonstrated validity for the claimed use, plus error characterisation that is usable in Court. Second, disclosure must be structured around meaningful defence challenge rather than vendor secrecy, using calibrated protective orders where necessary. Third, defence rights must include effective access to technical assistance, preservation of run artefacts, and credible remedies for non-disclosure. Recent judicial responses, including exclusion of facial recognition outputs under Frye Mack, appellate scrutiny of undisclosed facial recognition disclaimers in warrant practice, and appellate approval of probabilistic genotyping where code access issues are addressed on the record, show both the promise and the limits of existing tools. For India, the immediate task is doctrinal adaptation, electronic record admissibility establishes authenticity, but algorithmic inference requires a reliability and contestability layer anchored in Article 21 fair trial, Article 14 non-arbitrariness, and surveillance legality.

1. INTRODUCTION

Algorithmic systems now produce outputs that look like facts. A facial recognition system returns a ranked list, a "match", or a similarity score. A probabilistic genotyping tool returns likelihood ratios from complex DNA mixtures. A predictive model flags a person or a location as "high risk". These outputs often enter criminal process informally, as intelligence, but they can harden into courtroom proof when embedded in expert reports, warrant affidavits, or investigative narratives. The legal problem is not only novelty. It is a structural mismatch between algorithmic pipelines and classical adversarial testing. Courts consistently apply established jurisprudential principles to ascertain evidentiary relevance, to weigh probative value, and to control the admission and use of expert opinion. They also have disclosure duties and confrontation norms. But those doctrines assume that the defence can see what it must challenge. Algorithmic systems complicate that assumption because the "reason" for the output is distributed across software design, model versioning, training data, preprocessing choices, parameter tuning, thresholds, audit logs, and human interpretation. The inference is rarely a single readable artefact; it is a chain of transformations.

This paper addresses a central question: How should criminal courts treat algorithmic evidence, in admissibility, disclosure,

and defence challenge rights, across India, the EU, the UK, and the US? It argues for a structured approach. First, admissibility should require demonstrated validity for the claimed use, not generic claims of technological sophistication. Second, disclosure should be defined by the needs of meaningful challenge, balanced against legitimate secrecy through calibrated judicial controls. Third, defence rights should include technical capacity and strong remedies when transparency fails.

Recent judicial signals have rendered the issue pressing rather than speculative. A Minnesota district court, applying the Frye Mack standard, excluded facial recognition evidence on the ground that the underlying technology and its operational deployment did not meet the threshold of reliability for courtroom use. An Ohio appellate decision similarly notes that a facial recognition report itself carried express disclaimers that it was not intended for use in court filings, and it records that a trial court, following a Franks hearing , suppressed the

evidence, although the appellate Court later reversed and remanded.[1] In Oklahoma, an appellate court upheld the admission of probabilistic genotyping evidence under Daubert[2] while squarely engaging a demand for access to source code.[3] At the supranational level, the European Court of Human Rights has found facial recognition surveillance to be exceptionally intrusive, implicating Articles 8 and 10 and requiring heightened safeguards.[4] Taken together, these developments confirm that algorithmic evidence is already a live site of contestation within contemporary litigation, not a distant matter of policy design.

CONCEPTUALISING ALGORITHMIC EVIDENCE

2.1 What Counts as Algorithmic Evidence

For criminal adjudication, algorithmic evidence may be understood as information produced by computational systems that transform data into inferences, classifications, rankings, or probabilistic estimates, which is then relied upon to prove or lend support to facts in issue.[5] At its core, the category encompasses outputs such as facial recognition matches, actuarial risk scores deployed in bail and sentencing, probabilistic genotyping, predictive policing leads, and automated speech or video analytics.[6]

Crucially, these outputs do not always arrive in Court in the formal guise of "evidence." They often operate earlier in the chain, as investigative intelligence. Yet upstream deployment is not evidently inert. It conditions what is searched for, to whom suspicion attaches to, which alternatives are discounted, and what ultimately finds its way into the record.[7] When an algorithm points investigators towards a particular suspect, later "independent" corroboration may be shaped by suggestion, confirmation bias, or selective documentation, with the result that the apparent solidity of downstream proof is partly a product of the initial computational lead. The evidentiary inquiry, therefore, cannot sensibly be detached from the procedural history of the pipeline through which the output travelled.

2.2 Investigative Intelligence Versus Courtroom Proof

A helpful analytical separation can be drawn between investigative intelligence and courtroom proof. Intelligence functions to direct institutional attention; it assists in identifying avenues of inquiry.[8] Proof, by contrast, is presented to satisfy a legally defined burden within an adjudicative forum. The central risk is a collapse of categories, where an initial lead is gradually converted into proof through iterative citation in police paperwork, or through the compressive authority of expert summarisation.[9]

---

[1] State v. Tolbert, 2025-Ohio-4469 (Ohio Ct. App. 8th Dist. Sept. 25, 2025).

[2] Daubert v Merrell Dow Pharmaceuticals, Inc, 509 US 579 (1993).

[3] Napoleon v State, 2025 OK CR 25 (Okla Crim App, Dec 18, 2025).

[4] Glukhin v Russia, App No 11519/20, Judgment (ECtHR, Jul 4, 2023).

[5] Andrea Roth, "The Use of Algorithms in Criminal Adjudication" in Woodrow Barfield (ed.), *The Cambridge Handbook of the Law of Algorithms* 407 (Cambridge University Press, Cambridge, 2020).

[6] Clare Garvie, Alvaro Bedoya and Jonathan Frankle, *The Perpetual Line Up: Unregulated Police Face Recognition in America* 1 (Center on Privacy and Technology, Georgetown Law, Oct. 18, 2016).

[7] John S. Hollywood, Michael J.D. Vermeer, Dulani Woods, Sean E. Goodison and Brian A. Jackson, *Using Video Analytics and Sensor Fusion in Law Enforcement: Building a Research Agenda That Includes Business Cases, Privacy and Civil Rights Protections, and Needs for Innovation* (RAND Corporation, Santa Monica, 2018).

[8] Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment" 105 Minn L Rev 1105 (2021).

[9] Gary Edmond, Jason M Tangen, Rachel A Searston and Itiel E Dror, "Contextual Bias and Cross Contamination in the Forensic Sciences: The Corrosive Implications for Investigations, Plea Bargains, Trials and Appeals" 14 Law Prob Risk 1 (2015).

This strain is especially apparent in warrant litigation. In *State v Tolbert*,[10] the record refers to a facial recognition disclaimer emphasising that the results were investigative leads only, required independent verification, and were not intended for admissible evidence or for court filings. The disclaimer is doctrinally significant because it marks a governance boundary, one that later investigative practice and subsequent litigation narratives may quietly efface. If such limitations are omitted from affidavits, the issue is not confined to trial admissibility. It also goes to the integrity of the probable cause determination itself, namely, whether the issuing authority was presented with a materially distorted account of the method's reliability.

2.3 Why Algorithmic Outputs Are Hard to Test

Algorithmic outputs raise three common evidentiary problems—first, a lack of transparency. The defence often cannot examine key materials needed to test the system, such as source code, training and validation information, decision logs, and internal audits, because companies claim trade-secret protection, and second, because error rates are unclear. Every system has a risk of error, and its accuracy can vary depending on the data used and the conditions under which it is applied. If courts are not told the error rate and known limits, calling the tool "reliable" becomes an assertion, not something that can be checked.[11] Third, human judgment still matters. These tools usually require people to make choices, for example, which image to use, where to set the matching threshold, and whether to accept or reject a result. A court must therefore examine both the technology and the human steps around it, because error or bias can enter at either point and can influence the outcome.[12]

COMPARATIVE ADMISSIBILITY AND RELIABILITY GATEKEEPING

3.1 United States: Daubert, Frye, And the Model as Method

US courts usually screen new or contested scientific techniques through the law of expert evidence. In many jurisdictions, judges apply the Daubert reliability framework.[13] In others, they apply Frye-type general acceptance tests.[14] Algorithmic outputs often reach the courtroom through expert testimony, but the real "method" is not the printed result alone. It is the model, plus the full pipeline through which the result is generated and used.

In *State v Archambault*,[15] a Minnesota district court held that the facial recognition technology and the process used in that case did not satisfy Frye Mack reliability, and it granted suppression of evidence linked to that facial recognition use.[2] The point matters because the Court refused to treat the algorithmic output as a mere investigative hint that becomes reliable once later steps repeat it. Instead, the Court treated the process itself as the evidentiary object and asked a direct question, whether it could produce accurate results reliably and consistently.

By contrast, in *Napoleon v State*,[16] the Oklahoma Court of Criminal Appeals upheld the admission of probabilistic genotyping evidence under Daubert. The Court stressed familiar markers of scientific reliability, including validation, peer review, and general acceptance, and it dealt with the defence claim about access to source code by noting, on that record, that the underlying algorithms were open source and downloadable. *Napoleon* shows a common judicial comfort zone. Algorithmic evidence is more readily admitted when it can be placed within recognised validation pathways, and when access concerns are treated as addressed to the Court's satisfaction. The caution, however, is straightforward, "addressed" should mean genuinely contestable by the defence, not merely asserted by the proponent.

3.2 United Kingdom: Expert Evidence Discipline Plus Disclosure Culture

The UK does not apply Daubert as a formal test, but it still exercises strong control over expert evidence. Experts must be independent, they must set out their methods, and they must explain limits and uncertainties. In practice, algorithmic outputs in the UK are likely to come before the Court through forensic, biometric, or digital expert reports.[17]This framework

[10] *State v Tolbert*, 2025 Ohio 4469 (Ohio Ct App, 8th Dist, Sep 25, 2025).

[11] President's Council of Advisors on Science and Technology, Report: *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature Comparison Methods* (Sept., 2016).

[12] Gary Edmond, Jason M. Tangen, Rachel A. Searston and Itiel E. Dror, "Contextual Bias and Cross Contamination in the Forensic Sciences: The Corrosive Implications for Investigations, Plea Bargains, Trials and Appeals" 14 Law Prob Risk 1 (2015).

[13] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

[14] *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).

[15] *State v. Archambault*, No. 62-CR-20-5866 (Minn. Dist. Ct., Ramsey County, Sept. 13, 2024) (Order).

[16] *Napoleon v. State*, 2025 OK CR 25 (Okla. Crim. App., Dec. 18, 2025).

[17] Crown Prosecution Service, "Expert Evidence" (20 Nov. 2023), available at: https://www.cps.gov.uk/prosecution-guidance/expert-evidence (Visited on Jan. 14, 2026).

works best when the tool is open to scrutiny and has been independently validated. It becomes much weaker when commercial secrecy blocks the defence from examining how the system works, where it fails, and how errors are detected or measured.

That is why disclosure rules matter so much in the UK. The Criminal Procedure and Investigations Act system, together with the disclosure code, structures what must be revealed and when. Where material is sensitive, courts can control it through public interest immunity procedures rather than simple non-disclosure.[18] The comparative point is not that secrecy can never exist. It is that the Court must manage secrecy through principled, transparent balancing, not by private vendor contract terms that operate outside adversarial testing.

3.3 EU And ECHR: Legality and Safeguards as Reliability's Outer Boundary

European approaches add a clear rights first layer. In *Glukhin v Russia*, the European Court of Human Rights treated facial recognition surveillance as a highly intrusive practice, held that it engages Articles 8 and 10, and stressed the need for stronger safeguards.[19]Although *Glukhin* is not a decision on evidence admissibility in the narrow criminal procedure sense, it still speaks directly to algorithmic evidence pipelines. Where proof is generated from surveillance that lacks legality or adequate safeguards, a court has reason to treat the resulting material with greater caution, because legality and safeguards are part of evidentiary integrity, not matters external to it.

At the level of the European Union, the legal landscape also includes sector specific data protection rules for law enforcement processing, alongside newer horizontal regulation of artificial intelligence.[20] Regulation (EU) 2024/1689, the EU AI Act, adopts a risk-based structure of duties and restrictions and imposes particularly strict constraints on certain biometric practices.[21] The relevance for criminal courts may be indirect, but it is tangible. Compliance duties tend to produce records, documentation, audit trails, and traceability, and those materials can be demanded and evaluated when algorithmic outputs are relied upon in Court.

3.4 Comparative Synthesis: What Admissibility Must Ask

Across legal systems, admissibility must involve more than a relevance check, because courts also have to decide whether an output is safe and fair to use in an adversarial trial. Algorithmic results can look objective, but their trustworthiness depends on how they were built, how they were used, and whether the defence can test them. Four questions should therefore guide the Court.

First, fitness for the claimed purpose should be shown through validation for the exact use that is being asserted, under conditions that resemble the case in hand. Second, error must be made visible, because courts and counsel need usable information about error rates, limits, and known weaknesses for proper cross-examination. Third, human involvement must be accounted for, because analyst choices, threshold settings, and confirmatory steps can shape outcomes, and suggestive procedures can contaminate later proof. Fourth, contestability must be real, meaning that the defence has access to relevant material and, where necessary, technical assistance to test the claim.

This framework highlights India's adaptation challenge. India already has a disciplined route for proving electronic records, but algorithmic inference still needs a court led reliability and contestability inquiry that is anchored in Article 21 fair trial and Article 14 non-arbitrariness.

4. INDIA: DOCTRINAL ANCHORS FOR ALGORITHMIC EVIDENCE

[18] *R v H and C* [2004] UKHL 3, [2004] 2 AC 134.

[19] European Court of Human Rights, Press Release, "Use of facial-recognition technology breached rights of Moscow underground protestor, Glukhin v Russia (application no. 11519/20)" (ECHR 206 (2023), July 4, 2023), available at: https://hudoc.echr.coe.int/app/conversion/pdf/?filename=Judgment+Glukhin+v.+Russia+-+use+of+facial-recognition+technology+against+Moscow+underground+protestor.pdf&id=003-7694109-10618091&library=ECHR (Visited on Jan. 14, 2026).

[20] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016), available at: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng (Visited on Jan. 14, 2026).

[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024), available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (Visited on Jan. 14, 2026).

4.1 Why India is not starting from zero

Indian criminal courts are not strangers to proof that depends on method and is shaped by technology. Two legal lines are especially important.

First is the law on electronic records. The Bharatiya Sakshya Adhiniyam, 2023, which came into force on 1 July 2024, treats electronic records as documents and lays down specific rules for their admissibility.[2223] This continues the discipline developed under the earlier Section 65B case law.[24] The basic idea is simple; authenticity is never presumed. It must be shown through a defined legal route.

Second is the fair trial and disclosure line. Article 21 speaks of procedure established by law, but the Supreme Court has consistently read this as a requirement of fairness, and Article 14 adds a clear constraint against arbitrariness.[25] For algorithmic evidence, these are not merely abstract principles. They support practical courtroom demands, first, meaningful disclosure of how the output was produced, second, equality of arms so the defence can test the claim effectively, and third, remedies where unfairness has affected the process.[26]

4.2 Electronic record admissibility is necessary, but insufficient

The electronic record framework is essential because most algorithmic outputs are, in form, electronic records. They appear as reports, logs, screenshots, score sheets, and sometimes audio-visual files. But authenticity is only the first step. Proving that an output was generated by a system does not, by itself, prove that the system's inference is sound for the claim being made in Court.[27]

In that sense, the Supreme Court's strict approach to electronic records is useful by analogy. In *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, [28]the Court reaffirmed that the special route for electronic records is a complete framework, and it clarified how certificates operate and how courts may use procedural powers to secure them when needed. This posture matters for algorithmic evidence because it shows that courts already accept a threshold discipline for certain kinds of technology-based proof, not merely a free-flowing assessment of weight at the end. The next logical move is to carry this discipline forward, from authenticity to inferential reliability.

A recent illustration in the context of audio visual material appears in *Kailas Bajirao Pawar v State of Maharashtra* (2025 INSC 1117).[29] The Court indicated that once a video record is authenticated through the required certificate route, the law does not impose a general requirement that it must be converted into a transcript in each witness's words as a condition of admissibility. The point for algorithmic evidence is conceptual. Courts do not usually invent ritualistic hurdles once authenticity is established. But where the inference itself is disputed, they may still insist on reliability and contestability. Algorithmic outputs fall into that latter category, authenticity opens the door, it does not settle the question.

4.3 Surveillance legality is part of evidentiary integrity

Algorithmic evidence often begins far from the courtroom. It may come from surveillance systems, CCTV footage, facial recognition searches, mobile device extraction, location analysis, or social media monitoring. In India, the most important constitutional resource for evaluating such practices is the privacy decision in *Justice K S Puttaswamy (Retd) v Union of India* (2017).[30] The Court recognised privacy as a fundamental right and held that any limitation must satisfy legality, a legitimate aim, necessity, proportionality, and effective safeguards against abuse.

For algorithmic evidence, this matters in two connected ways.

First, pipeline legality. If the initial collection and processing lack legal authority or adequate safeguards, courts should approach the later outputs with greater caution. This is not only about exclusion, where the law permits it. It is also about judging reliability and fairness, because defective upstream practices can shape and distort what later appears as proof.

Second, safeguards and records. A proportionality-based approach to surveillance requires governance, clear authorisation,

---

[22] *The Bharatiya Sakshya Adhiniyam, 2023* (Act 47 of 2023), s 1(3) (commencement by Central Government notification), Enforcement Date: 1 July 2024.

[23] *The Bharatiya Sakshya Adhiniyam, 2023* (Act 47 of 2023), s 2(1)(d) (definition of "document" includes electronic and digital records).

[24] *Anvar P.V. v P.K. Basheer*, (2014) 10 SCC 473.

[25] *Maneka Gandhi v Union of India*, (1978) 1 SCC 248.

[26] *Zahira Habibulla H. Sheikh v State of Gujarat*, (2004) 4 SCC 158.

[27] Paul W Grimm, Maura R Grossman and Gordon V Cormack, "Artificial Intelligence as Evidence" 19 Nw J Tech & Intell Prop 9 (2021).

[28] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.*

[29] *Kailas s o Bajirao Pawar v State of Maharashtra 2025 INSC 1117 (SC)*

[30] *Justice K. S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.

limits on retention, and auditability. These are also the very materials the defence needs to test the prosecution's claim. In this sense, constitutional rights and evidentiary integrity point in the same direction.

India's statutory data protection framework does not dilute this constitutional baseline. The Digital Personal Data Protection Act, 2023 includes exemptions for certain law enforcement and legal purposes, but statutory exemptions cannot remove the demand for legality and procedural fairness when criminal liberty is at stake.[31] The doctrinal point is straightforward. Even where exemptions apply, courts remain constitutional guardians when opaque processing is converted into proof against an accused.

4.4 Disclosure duties in India, moving from form to meaningful challenge

Indian criminal procedure does contain disclosure rules, but algorithmic evidence exposes a practical question, whether disclosure is implemented in a way that allows a real defence challenge. Recent Supreme Court decisions have begun treating disclosure not as a routine provision of relied-upon papers, but as part of the constitutional idea of a fair trial.

Two decisions are especially important.

First, in *Manoj v State of Madhya Pradesh*[32], the Court held that the prosecution must furnish, in all criminal cases, lists of statements, documents, material objects, and exhibits that the investigating officer has not relied upon. The Court linked this to Article 21 and to the prosecutor's duty to assist the Court in doing justice. This is a structural shift. It recognises that the defence cannot use procedural rights effectively unless it can see the wider universe of material, including what the prosecution chooses not to place in the foreground.

Second, in *Sarla Gupta v Directorate of Enforcement*[33], the Court addressed whether an accused is entitled to copies of documents collected during investigation but not relied upon, and whether the prosecution can refuse copies, at least at certain stages. The judgment frames the issue through Article 21 fair trial and through the working of Sections 207 and 208 CrPC principles, noting their continuation under the Bharatiya Nagarik Suraksha Sanhita, 2023. Whatever the precise stage wise boundaries, the message is clear. Disclosure disputes are not merely administrative. They go to constitutional fairness and to the accused's ability to defend.

For algorithmic evidence, these decisions provide a direct doctrinal bridge. The defence may need access to model documentation, version history, error information, run outputs, and system disclaimers, because without these, cross examination becomes performance rather than testing. The Court's disclosure approach supports organising disclosure around meaningful challenge, not around the convenience of the proponent or the secrecy preferences of a vendor.

SUPREME COURT JURISPRUDENCE ON TECHNOLOGY-MEDIATED EVIDENCE: A FOUR-CASE SYNTHESIS

Technology-mediated evidence has become routine in Indian criminal adjudication, ranging from CCTV footage and call detail records to device extractions, digital logs, and software-generated forensic reports. As these materials increasingly shape arrest, bail, charging, and trial outcomes, the Supreme Court has emphasised that courts must examine the legal and procedural conditions under which such evidence is created, preserved, and produced. This section synthesises four decisions to explain why that discipline is especially important for algorithmic outputs. The central proposition is that a court cannot assess trustworthiness by looking only at the final output placed on record. The true evidentiary object is the full process that generated the output, including upstream collection, system settings, human interventions, and disclosure to the defence. When that process is weak, even a polished result can mislead, but when it is transparent and contestable, reliability can be meaningfully tested.

***Justice K S Puttaswamy (Retd) v Union of India*[34]: Pipeline legality and safeguards as evidentiary preconditions**

Puttaswamy treats privacy as a fundamental right, and it requires legality, a legitimate aim, necessity, proportionality, and safeguards whenever the State intrudes. In the context of algorithmic evidence, this functions as an upstream filter for the Court. If a facial recognition search, a biometric match, or a predictive model output is produced through surveillance that lacks legal authority or adequate safeguards, the Court should view the output with caution. This is not only an argument about exclusion, because Indian criminal procedure is generally careful with exclusionary remedies. It is also an argument about knowledge and reliability, because a rights deficient pipeline is usually a weak evidentiary pipeline. When there is no clear authorisation, audit trail, minimisation, or retention discipline, the Court cannot easily verify what was done, what was changed, and how errors were controlled.

---

31 *The Digital Personal Data Protection Act, 2023* (Act 22 of 2023), s 17(1)(c).

32 *Manoj v State of Madhya Pradesh*, 2022 SCC OnLine SC 677, para 179 (SC, May 20, 2022).

33 *Sarla Gupta v Directorate of Enforcement*, 2025 INSC 645 (SC, May 7, 2025).

34 *Justice K S Puttaswamy (Retd) v Union of India*, (2017) 10 SCC 1.

***Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[35]: Procedural discipline for technology based artefacts**

In *Arjun Panditrao*, the Court reaffirmed that electronic records must be proved through a structured process and clarified that courts may exercise their procedural powers to secure the required certificate when justice demands it. This approach is important for algorithmic evidence because it shows the Court's basic attitude towards technology-mediated proof. The Court accepts that certain kinds of technological material require threshold compliance, and it treats that compliance as part of legality and fairness, not as a mere technical formality. For algorithmic outputs, the parallel is that courts should insist on threshold reliability showings before treating an inference as proof. That should include validation of the claimed use, usable disclosure of errors and limitations, and preservation of run artefacts and logs that enable later testing.

***Manoj v State of Madhya Pradesh*[36] : Disclosure as an element of Article 21 fair trial**

Manoj strengthens the idea that disclosure is not a concession by the prosecution, but an intrinsic part of a fair trial under Article 21, and it emphasises that the prosecutor must assist the Court in doing justice rather than merely secure a conviction. This has direct force for algorithmic evidence because the most important reliability information often sits outside the final report. A single-page match result rarely shows the full story about limitations, false match risk, subgroup performance cautions (where available), or procurement and use disclaimers. *Manoj* provides the constitutional footing for courts to require disclosure that makes challenge possible, including clear lists and structured packets that enable the defence to identify, request, and test what is truly material.

Sarla Gupta v Directorate of Enforcement[37]: Contestability, access to material, and equality of arms

Sarla Gupta is significant because it addresses, in direct terms, whether an accused can seek copies of documents collected during investigation but not relied upon, and it frames the issue through Article 21 and the continuing procedural scheme under the new criminal codes. The deeper implication for algorithmic evidence is about equality of arms. If the State relies on a computational inference that the accused cannot realistically test, because key material is withheld as not relied upon, or is refused as proprietary, then the trial can become unfair in a constitutional sense. *Sarla Gupta* strengthens the basis for courts to treat transparency disputes involving algorithmic systems as fair-trial disputes, rather than routine discovery disagreements that can be brushed aside.

Read together, these four decisions point towards a practical position that Indian courts can apply without waiting for new legislation. First, *Puttaswamy*[38] makes clear that when algorithmic outputs come from surveillance or large scale data processing, courts must ask whether the entire evidentiary pathway was lawful and safeguarded, because legality and safeguards shape both fairness and reliability. Second, *Arjun Panditrao*[39] confirms that technology based material is never exempt from threshold discipline, and that authenticity and process compliance operate as gatekeeping conditions, not as optional technical formalities. Third, *Manoj*[40] places disclosure within the core of Article 21 fairness, and it reminds prosecutors that their obligation is to assist justice, which requires disclosure that enables real defence challenge. Fourth, *Sarla Gupta*[41] strengthens the principle that access to material needed for defence is constitutionally grounded, and that fairness may require disclosure even of material the prosecution has chosen not to rely upon.

Together, these principles form the doctrinal spine for an Indian framework on algorithmic evidence. Courts can give them operational form through structured admissibility hearings, targeted disclosure directions, and effective remedies grounded in fair trial and non-arbitrariness.

DISCLOSURE: WHAT MUST BE SHARED FOR MEANINGFUL CHALLENGE

Disclosure becomes decisive once the prosecution relies on an algorithmic output, because the defence cannot test what it cannot see. In ordinary cases, a document can be read, challenged, and explained through cross-examination. With algorithmic material, the printed result is rarely enough. A match, a score, or a likelihood ratio carries meaning only when the Court and the defence can examine how it was produced, what assumptions were built into the system, and what limits were known at the time of use.

This section explains what must be shared to make challenge real rather than symbolic. The guiding idea is that disclosure should be organised around contestability, not around convenience. Courts should require the prosecution to provide the information that allows the defence to ask proper questions about validity, error, human involvement, and whether the output was used within its intended boundaries. Where confidentiality is genuine, the answer is careful judicial

[35] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[36] *Manoj v State of Madhya Pradesh*, 2022 SCC OnLine SC 677.
[37] *Sarla Gupta v Directorate of Enforcement*, 2025 INSC 645.
[38] *Justice K S Puttaswamy (Retd) v Union of India*, (2017) 10 SCC 1.
[39] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[40] *Manoj v State of Madhya Pradesh*, 2022 SCC OnLine SC 677.
[41] *Sarla Gupta v Directorate of Enforcement*, 2025 INSC 645.

management, not a blanket refusal that leaves the defence arguing in the dark.

6.1 Disclosure as A Fair Trial Technology

Disclosure is what turns the right to defend into something real, because nobody can challenge a claim that is kept hidden. With algorithmic evidence, giving only the final output, such as a match statement or a risk score, is usually not enough. The defence needs the surrounding material that explains what the tool did, how it did it, and its limits, otherwise cross-examination becomes largely symbolic.[42]

In simple terms, a court-ordered disclosure package should usually cover seven types of information. First, the Court should know which tool was used and in what form, including the product name, the exact model version, and the settings that were applied in the case, because a different version or a different threshold can change the result.[43] Second, the defence should receive the tool's own documentation, showing the intended use, known limits, and the meaning of any confidence or similarity scores, because a number without context can mislead.[44] Third, there should be a summary of how the tool was tested, including the type of data used and how it performed, because testing demonstrates whether the tool is fit for the claim being made. Fourth, the prosecution should disclose error information, including false match and false non match rates, calibration, and any audit or independent validation reports, because "reliability" must be supported by measurable performance.[45] Fifth, there should be case-specific run material, such as the inputs used, any preprocessing, the candidate list, the scores generated, and a record of what the analyst changed or confirmed, because human choices can shape the outcome. Sixth, courts should require governance documents, including policies, retention rules, and disclaimers, because these materials often specify what the tool is not intended for. Seventh, the Court should ensure a workable method of technical review, which may involve source code access, escrow, protective orders, or review by a neutral expert, because meaningful testing sometimes needs technical help.[46]

The reason governance papers and disclaimers matter can be explained without jargon. In *Tolbert*,[47] the case record notes that the facial recognition report carried a disclaimer saying that the result was only an investigative lead, that it needed independent verification, and that it was not designed for court filings. If the defence never sees that disclaimer, the judge may be told, directly or indirectly, that the match is stronger than the tool itself claims. That can affect probable cause at the warrant stage and also shape the story that later reaches the trial court.

6.2 Trade Secrets, National Security, And Judicial Balancing

Secrecy is the usual objection in algorithmic evidence disputes. Vendors invoke trade secrets, and the State may invoke operational security. These concerns can be genuine, but they cannot operate as automatic vetoes. The real question for a court is whether confidentiality can be protected while still allowing a meaningful defence challenge.[48]

A workable approach is to use a structured balancing test. First, the Court should ask about materiality, and it should require the defence to show that the requested item is reasonably needed to test reliability, bias, or the integrity of the process. Second, the Court should ask about specific harm, and it should demand a concrete explanation of what damage would follow from disclosure, because vague claims of risk do not assist judicial reasoning. Third, the Court should consider less restrictive options, such as redaction, protective orders, expert only access, sealed hearings, or review by a neutral technical expert, because these tools often protect confidentiality without blocking scrutiny. Fourth, the Court should apply a fair-trial floor and recognise that, when meaningful contestation is impossible without the withheld item, non-disclosure must carry consequences, including exclusion or an equivalent remedy.[49][50]

This approach fits the basic idea of equality of arms. A conviction should not rest on an algorithmic proposition that the accused is unable to contest in any realistic and informed way.

6.3 India: disclosure levers that can be activated now

India already has disclosure levers that courts can activate without waiting for new legislation, and the central move is to

---

[42] Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System" 70 *Stanford Law Review* 1343 (2018).

[43] Patrick J Grother, Mei L Ngan and Kayee K Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (National Institute of Standards and Technology, NISTIR 8280, 2019).

[44] Itiel E Dror, "Biases in Forensic Experts" 360 *Science* 243 (2018).

[45] President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature Comparison Methods* (Executive Office of the President, Washington DC, 2016).

[46] Margot E Kaminski and Jennifer M Urban, "The Right to Contest AI" 121 *Columbia Law Review* 1957 (2021).

[47] *State v Tolbert*, 2025-Ohio-4469, paras 63–68 (Ohio Court of Appeals, Eighth District, Sept 25, 2025).

[48] *R v H; R v C* [2004] UKHL 3, [2004] 2 AC 134.

[49] Margot E Kaminski and Jennifer M Urban, "The Right to Contest AI" 121 *Columbia Law Review* 1957 (2021).

[50] *Rowe and Davis v United Kingdom* (App no 28901/95) (2000) 30 EHRR 1.

treat disclosure disputes as constitutional questions rather than routine paperwork disagreements. *Manoj*[51] and *Sarla Gupta*[52] provide the doctrinal language for this approach, because they connect disclosure to fair trial under Article 21 and they frame the prosecutor's role as fairness driven. Courts can insist on complete and timely supply of relied upon material, and they can require lists of unused statements and documents so the defence can identify what is relevant. When the State relies on an algorithmic output, courts should treat the supporting material as part of the same evidentiary universe, including model documentation, version details, error information, system logs, device extraction records, forensic tool reports, and disclaimers about intended use. Where confidentiality is genuinely at issue, courts can use limited-access directions, sealed inspections, and neutral expert review to protect sensitive material while preserving meaningful challenge. If non-disclosure renders contestation impossible, courts should treat that failure as a breach of the fair trial guarantee and provide effective remedies.

DEFENCE CHALLENGE RIGHTS: CONFRONTATION, EQUALITY OF ARMS, REMEDIES

Defence challenge rights are the practical core of a fair criminal trial, because they ensure that the State's case is tested rather than accepted on authority. In cases involving algorithmic outputs, the right to confront evidence must include the right to question the method that generated the result, not merely the witness who repeats it. Equality of arms requires that the defence has access to the materials and technical support needed to examine reliability, error, and human interventions within the process. When those conditions are denied, remedies must be real, because a trial cannot be fair if the challenge is only formal.

7.1 The Defence Right Is Not Only To Cross-Examine, but It Is To Understand

Confrontation is meaningful only when the defence can understand what it is being asked to accept. When an algorithmic inference effectively replaces an eyewitness or supplies the core conclusion in an expert report, the defence must be able to question the method that produced the result, and not merely question the person who operated the tool. If the defence cannot probe how the output was generated, where it can fail, and what human choices shaped it, cross-examination becomes largely formal.

Comparative experience shows why these matters. Courts have sometimes treated reliability as satisfied even without full transparency, as in *Napoleon*, where the source code access concern was considered resolved on the record before the Court.[53] That is a cautionary example for India. Indian courts should treat contestability as a built-in requirement of admissibility and disclosure, rather than postponing it to a general argument about weight at trial.

7.2 Effective legal representation requires technical capacity

Algorithmic evidence often raises technical questions that most defence teams cannot answer without specialised assistance, and ordinary legal aid budgets rarely cover that kind of support. If equality of arms is to have real meaning in such cases, the defence must have a practical ability to test the prosecution's claim with competence and independence.

Three requirements follow from that premise. First, courts should ensure timely appointment and proper funding of defence experts, including forensic statisticians and machine learning specialists, when the evidentiary issue demands such expertise. Second, the defence should receive adequate time and access to the relevant tools, data, and computing resources, because technical testing cannot be performed quickly or through mere argument. Third, where replication is feasible, the defence should be able to rerun the system using the same inputs and parameters, as replication is often the clearest way to check whether the result is stable, reproducible, and reliable.

7.3 Remedies for non-disclosure

Remedies for non-disclosure must have real bite, because disclosure duties are meaningless if breach carries no consequence. Courts can apply a simple ladder of responses that matches the seriousness of the failure and its effect on the defence.

First, where disclosure is late and the prosecution causes delay, the Court can grant an adjournment and impose costs, so that the defence is not punished for the State's default. Second, where key logs or technical materials are missing without a credible explanation, the Court can draw an adverse inference, because the missing record may have mattered to reliability. Third, where meaningful testing is blocked, the Court can exclude the algorithmic output and any expert opinion based on it. Fourth, at the warrant stage, the Court can treat misleading omissions about system limits as a suppression problem, because probable cause cannot rest on a distorted account of reliability. Fifth, where fairness has been permanently damaged and no lesser step can cure it, the Court can stay the proceedings.

The *Tolbert* litigation illustrates this point clearly, because omissions about facial recognition disclaimers and limitations

---

[51] *Manoj v State of Madhya Pradesh*, 2022 SCC OnLine SC 677.

[52] *Sarla Gupta v Directorate of Enforcement*, 2025 INSC 645.

[53] *Napoleon v State*, 2025 OK CR 25 (Okla Crim App, Dec 18, 2025), available at: https://www.okcca.net/cases/2025/OK-CR-25/ (Visited on Jan 15, 2026).

can be framed as *Franks*-type issues at the warrant stage, not only as questions of admissibility at trial.[54]

8. REFORM PROPOSALS: COURT-READY RULES AND GUIDELINES

The recommendations below are written as practical rules that courts can adopt immediately, with minor adjustments for local procedure. They are meant to make algorithmic material testable in Court, and to ensure that fairness is not defeated by technical opacity.

Early notice of algorithmic reliance

Any party relying on an algorithmic output, whether directly or through an expert, should give early notice stating the system used, its version, the purpose of use, and the exact fact for which the output is offered.

Validation for the claimed use

An output should be admitted only when the system has been validated for the specific use and conditions being claimed, and general vendor assurances should never be treated as sufficient.

Error information that can be tested

The proponent should disclose known error rates, confidence measures, and practical limitations in a form that can be used for cross-examination, and absence of usable error information should weigh strongly against reliance.

Case-specific process record

Disclosure should include the inputs used, any preprocessing, thresholds applied, candidate lists where relevant, analyst interventions, and logs that allow the Court to reconstruct how raw data became the final result.

Duty to preserve

Investigating agencies should preserve run artefacts and logs once the algorithmic output materially contributes to suspicion, arrest, charging, or a warrant application, and failure should trigger a presumption against reliance unless harmlessness is clearly shown.

Defence access protocol for proprietary tools

When a tool is proprietary, courts should order a workable pathway for defence testing, such as expert access under protective orders, code escrow review by a neutral expert with defence participation, or independent audits adequate for challenge, because trade secrecy cannot override the fair trial minimum.

Balancing test for contested disclosure

Courts should balance materiality, concrete harm, less restrictive alternatives, and the fair trial floor, and when meaningful challenge is impossible without the withheld item, the output should not be relied upon.

No sole reliance for high-risk inferences

Where the output carries a known risk of false positives, courts should not allow it to be the sole basis of identity or guilt unless there is independent corroboration that does not come from the same evidentiary pathway.

Stronger duties for experts using algorithms:

Experts who rely on algorithmic tools should explain the method, the validation basis, known limits, and case-specific checks, and opinions that merely repeat vendor outputs without scrutiny should be treated as unreliable.

Remedies that have consequences:

Where there is non-disclosure or preservation failure, courts should move through a remedies ladder that includes adjournment, adverse inference, exclusion, suppression, and, where fairness cannot be repaired, a stay.

These proposals reflect emerging judicial practice. *Archambault*[55] shows that courts can exclude facial recognition when reliability is not demonstrated. *Tolbert*[56] shows that tool disclaimers and omissions can matter at the warrant stage, and not only at trial. *Napoleon*[57] shows that probabilistic genotyping may be admitted when validation and contestability are addressed on the record. In India, recent Supreme Court trends on privacy, electronic records, and disclosure provide a

[54] State v Tolbert, 2025-Ohio-4469, paras 63–68 (Ohio Ct App, 8th Dist, Sept 25, 2025).

[55] *State of Minnesota v Gerald Paul Archambault*, File No 62-CR-20-5866, Order (Minn Dist Ct, Second Judicial District, Ramsey County, Sept 13, 2024).

[56] State v Tolbert, 2025-Ohio-4469 (Ohio Ct App, 8th Dist, Sept 25, 2025).

[57] *Napoleon v State*, 2025 OK CR 25 (Okla Crim App, Dec 18, 2025).

doctrinal foundation for translating these instincts into structured courtroom practice.

9. CONCLUSION

Algorithmic evidence forces criminal procedure to make a clear choice. Courts can treat algorithmic outputs like ordinary exhibits and assume that trial questioning will separate reliability from error. Courts can also recognise that these outputs are method-based inferences, and therefore require structured screening, structured disclosure, and real defence capacity. Comparative experience supports the second approach, because without these safeguards, the courtroom often receives a result without the tools needed to test it.

For India, the task is adaptation rather than reinvention. The Bharatiya Sakshya Adhiniyam's rules on electronic records help courts establish authenticity, but authenticity alone does not prove that an algorithmic inference is reliable for the claim being made. A further layer is needed, and that layer should be grounded in Article 21 fair trial, Article 14 non-arbitrariness, and the legality of upstream surveillance. Recent Supreme Court decisions already provide the doctrinal building blocks. *Puttaswamy*[58] supplies the legality and safeguards framework for pipelines that generate such outputs. *Arjun Panditrao*[59] reinforces threshold discipline for technology-based material.*Manoj*[60] strengthens disclosure as part of a fair trial. *Sarla Gupta* supports meaningful defence access when contestation would otherwise be impossible.

The immediate agenda is practical and implementable. Courts need standard disclosure packets for algorithmic systems, police procurement must ensure auditability and disclosure readiness, and legal aid structures must make room for defence technical assistance. Without these steps, algorithmic outputs may enter the Court as supposedly objective proof, while remaining insulated from the adversarial testing that gives criminal justice its legitimacy..

References

N\A

[58] *Justice K. S. Puttaswamy (Retd) v Union of India*, (2017) 10 SCC 1.

[59] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

[60] *Manoj v State of Madhya Pradesh*, 2022 SCC OnLine SC 677.