

Beyond the Match Score: Admissibility, Reliability and Fair-Trial Safeguards for Facial Recognition Evidence under the Bharatiya Sakshya Adhiniyam, 2023

S. Kalpana

Assistant Professor, School of Law,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Chennai, Tamil Nadu, India.
kalpanakavismk@gmail.com

Abstract

Facial recognition technology is increasingly used to generate investigative leads, yet Indian evidence law does not contain a facial-recognition-specific rule of admissibility or weight. This article asks how a police-generated candidate or match report should be treated under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), constitutional fair-trial guarantees, and the emerging data- and AI-governance framework. It uses structured doctrinal analysis of legislation, leading Indian judgments on electronic and expert evidence, official Indian AI policy, and selected comparative authorities. The analysis separates four questions often collapsed in practice: lawful collection, electronic-record authenticity, scientific reliability, and probative weight. Section 63 BSA can authenticate a computer output and its provenance; it does not demonstrate that a facial-recognition model is valid for the deployed population, that the selected threshold is appropriate, or that a candidate is the accused. Section 39 makes expert opinion relevant, but leaves courts to evaluate methodology and grounds. Law-enforcement processing may also fall within exemptions in the Digital Personal Data Protection Act, 2023, while the India AI Governance Guidelines remain principle-based. The article proposes the MATCH protocol: Mandate the use, Audit performance, Trace the complete inference, enable Challenge, and require Human verification plus independent corroboration. Under this approach, an unexplained match score is an investigative lead, not self-proving identity and not a sufficient basis for conviction. The protocol can be implemented through procurement conditions, investigation manuals, disclosure orders, expert-evidence practice and judicial directions without waiting for a comprehensive AI statute.

Keywords: facial recognition; electronic evidence; criminal procedure; fair trial; algorithmic accountability; Bharatiya Sakshya Adhiniyam

1. Introduction

A facial-recognition system does not see identity. It converts a probe image into a numerical representation, compares that representation with templates in a gallery, and returns candidates whose similarity exceeds or approaches a selected threshold. The legal danger begins when this probabilistic ranking is translated into the categorical language of a police file: the system ‘identified’ the accused. That translation can conceal the quality of the source image, the size and composition of the gallery, the model version, the threshold, the number of candidates returned, and the role of the human examiner. Each hidden choice bears on error and fairness.

The distinction matters because criminal adjudication operates through proof, disclosure and contestation. An accused must be able to test the evidence used to connect her to an offence, while a court must distinguish an authentic electronic record from a reliable scientific inference. A hash can show that a report was not altered after extraction. It cannot show that the software was accurate, that its training data were representative, or that the top-ranked face belonged to the suspect. Likewise, a section 63 certificate under the Bharatiya Sakshya Adhiniyam, 2023 (BSA) may satisfy a statutory route for admitting a computer output, but it cannot by itself convert an algorithmic candidate into proof beyond reasonable doubt. The problem is a criminal-evidence version of ‘technological due process’: legal safeguards weaken when consequential rules and inferences are embedded in systems that affected persons cannot inspect or contest (Citron, 2008; Kroll et al., 2017; Cobbe, 2019).

Indian law now offers an unusual moment for doctrinal clarification. The BSA and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) came into force on 1 July 2024 and expressly accommodate electronic records and digital processes. The Digital Personal Data Protection Act, 2023 (DPDP Act) defines processing broadly enough to include automated operations and places accuracy obligations on data used to make decisions. The final Digital Personal Data Protection Rules, 2025 add due diligence concerning technical measures, including algorithmic software, for Significant Data Fiduciaries, although the principal substantive provisions are subject to phased commencement. Separately, the India AI Governance Guidelines, released in November 2025,

recommend risk-proportionate safeguards, human oversight, transparency reporting, audit and grievance redressal. None of these instruments, however, supplies a complete evidentiary rule for police facial recognition.

This article addresses that gap. It asks three questions. First, what does Indian evidence law actually authenticate when a facial-recognition report is tendered? Second, what information must be disclosed if the defence and the court are to assess reliability rather than merely inspect the final score? Third, which safeguards can be derived from existing constitutional, evidentiary, procedural and data-governance norms without treating a voluntary policy document as binding legislation?

The argument is that facial-recognition evidence must be disaggregated into a chain of propositions. The prosecution must establish a lawful and sufficiently precise basis for the search; preserve the probe, gallery and software context; authenticate each electronic output; demonstrate fit-for-purpose performance; identify the human steps between candidate generation and police action; disclose material necessary for an effective challenge; and produce independent corroboration. The proposed MATCH protocol translates those requirements into a practicable sequence: Mandate, Audit, Trace, Challenge and Human verification. It does not impose a blanket prohibition. It makes the legal weight of the evidence correspond to what the technology can actually prove.

The contribution is both doctrinal and operational. Doctrinally, it separates admissibility from weight and data protection from fair-trial disclosure. Operationally, it gives investigators, prosecutors, defence counsel, forensic laboratories and courts a common record of what must accompany a match report. The result is a framework capable of preserving useful searches while preventing the match score from becoming an inscrutable substitute for proof.

2. Research Design and Scope

The study adopts a structured doctrinal method. Primary Indian materials were selected where they govern one of four stages: acquisition and processing of facial images; production and authentication of electronic records; reception and evaluation of expert opinion; or disclosure and trial fairness. The core materials are the Constitution of India, the Information Technology Act, 2000, the BSA, the BNSS, the DPDP Act and Rules, and the India AI Governance Guidelines. Leading Supreme Court decisions were selected for the propositions they establish concerning electronic-record authenticity, expert evidence, privacy, reasoned decision-making, non-arbitrariness and access to relied-upon digital material.

Each authority was coded against seven questions: legal basis, notice, integrity, validation, human role, defence access and remedy. The analysis is functional rather than merely textual. For example, the question under section 63 BSA is not only whether a certificate exists, but which link in the facial-recognition pipeline that certificate can logically prove. Comparative materials — principally the European Union AI Act, the decision of the Court of Appeal of England and Wales in *R (Bridges) v Chief Constable of South Wales Police*, and international technical guidance — are used as interpretive comparators, not as sources of Indian legal obligation.

The temporal cut-off is 3 September 2026. At that date, the DPDP framework has been notified in phases, and India has issued a national AI governance framework, but this study identified no reported Supreme Court judgment squarely determining the admissibility or minimum weight of a police facial-recognition match under the BSA. That absence makes analogy necessary but also limits any claim that the proposed protocol states settled law. The article therefore distinguishes current binding rules, principles that can reasonably be derived from existing doctrine, and recommended safeguards requiring rules, practice directions or legislation.

The study does not evaluate any vendor or estimate an Indian error rate. Accuracy is context-specific: it depends on the algorithm, image quality, gallery, threshold and operational procedure. Technical studies are used only to establish why those variables are legally material. The proposed framework is consequently technology-neutral and evidence-focused. It applies whether the system is developed by the State, purchased from a vendor, or operated through a cloud service.

Table 1. Doctrinal corpus and analytical function

Layer	Principal materials	Question asked
Constitutional control	Arts 14 and 21; privacy and fair-trial cases	Non-arbitrariness, legality, necessity, proportionality and meaningful opportunity to answer adverse material.
Evidence law	BSA ss 39–40, 45 and 61–63	Relevance of expert opinion; grounds bearing on that opinion; legal effect and authentication of electronic records.
Criminal procedure	BNSS ss 193 and 230	Investigation record and supply of police report, statements and relied-upon documents to the accused.
Data governance	DPDP Act ss 2, 7–11 and 17; DPDP Rules 2025	Automated processing, accuracy, audit and impact assessment, rights and law-enforcement exemptions.

Layer	Principal materials	Question asked
AI governance	NITI Aayog papers (2021–2022); India AI Governance Guidelines (2025)	Safety, equality, transparency, accountability, human oversight, audit and grievance redressal.
Comparative control	EU AI Act; R (Bridges); INTERPOL framework	Risk-based limits, documentation, impact assessment, human verification and targeted use.

Note: The corpus is purposive, not a citation-count study. Comparative materials are used to test the completeness and practicability of safeguards under Indian law.

3. What a Facial-Recognition Output Is — and Is Not

3.1 Verification, identification and candidate generation

Facial recognition covers materially different tasks. One-to-one verification asks whether a live or submitted image corresponds to a claimed identity. One-to-many identification compares a probe against a gallery and ranks possible candidates. Criminal investigation normally involves the second task. Its output is therefore conditional on the gallery searched and the operating threshold. A high similarity score means that, under the chosen model and parameters, two representations are close. It is not a statement that no other person could produce a similar score or that the candidate committed the offence.

The distinction between a candidate and an identification is standard forensic prudence. INTERPOL describes its system as producing a candidate list and states that trained officers manually examine the images before reporting a potential candidate, no candidate or an inconclusive result. This operational separation should be legally significant. If the machine output is only a search aid, the prosecution must not present it as an autonomous biometric identification. If a human examiner converts the candidate into an opinion, the examiner’s method, competence, observations and grounds become part of the evidence and must be testable under sections 39, 40 and 45 BSA.

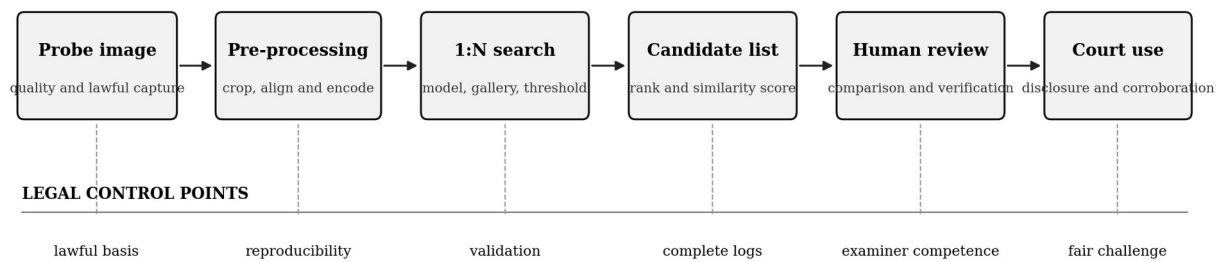
3.2 Error is produced by a system, not only by a model

Accuracy cannot be described by a single vendor percentage. Probe-image resolution, pose, illumination, compression, occlusion and elapsed time can alter similarity. The gallery’s size and composition affect the number of plausible candidates. Thresholds trade false positives against false negatives. Human reviewers may reduce error, but may also become anchored to the machine’s ranking or to contextual information from investigators. A courtroom inquiry focused only on source-code secrecy will therefore miss many ordinary and measurable causes of error.

The National Institute of Standards and Technology has reported wide performance differences across algorithms and demographic differentials in many systems. Its continuing evaluations also emphasize that false-negative differences are strongly affected by image quality and that false-positive variation can persist across demographic groups. Independent research has likewise shown that aggregate accuracy can conceal intersectional performance disparities (Buolamwini and Gebre, 2018; Grother et al., 2019). These findings do not establish how a particular Indian deployment performs. They establish why local validation, image-quality records, threshold disclosure and subgroup testing are relevant to weight, and why apparently neutral data practices can generate disparate effects (Barocas and Selbst, 2016).

A system-level approach also avoids a false choice between complete disclosure of proprietary source code and blind trust. Many challenges can be evaluated from less intrusive materials: model and version identifiers; test protocols; false-match and false-non-match rates at the operational threshold; subgroup results; image-quality metrics; gallery size and inclusion criteria; candidate-list length; audit logs; reviewer instructions; and records of any manual override. Source code may become necessary in a particular case, but it is not the only path to meaningful scrutiny. Verifiable process records can often make an algorithm accountable without assuming that the machine’s assertion is self-authenticating testimony (Kroll et al., 2017; Roth, 2017).

Figure 1. From image capture to courtroom use: six distinct control points



Source: Author's formulation. The figure shows why a final match report cannot establish the integrity or reliability of every upstream stage.

Table 2. Evidentiary objects created across the facial-recognition pipeline

Stage	Material that should be preserved	Legal question
Probe image	Original file, metadata, hash, extraction method, quality metrics and lawful source	Was the image altered, selectively enhanced or too poor for the claimed inference?
Pre-processing	Software version; crop/alignment settings; enhancement steps; generated intermediate files	Can the transformation be reproduced, and did it introduce or suppress features?
Search	Model/version; threshold; gallery snapshot; search mode; validation results	Was the system fit for this use and population at the chosen operating point?
Candidate list	Complete ranked output, scores and non-selected candidates	Did investigators see alternatives, or only a top result stripped of context?
Human review	Reviewer identity, training, method, notes, blind or contextual review, conclusion	Was the machine output independently verified or merely confirmed?
Court use	Section 63 certificate, expert report, disclosure index and corroborating evidence	Is the record authentic, the inference reliable, and the defence able to challenge it?

4. Indian Evidence Law: Authenticity Is Not Accuracy

4.1 Sections 61–63 BSA and the limited work of certification

Section 61 BSA prevents an electronic or digital record from being denied admissibility merely because of its form, subject to section 63. Section 62 directs that the contents of electronic records may be proved under section 63. Section 63 then treats qualifying computer output as a document and requires a certificate when the output is tendered through that route. The statutory Schedule records details of the device or source and requires hash information; section 63(4) also requires the certificate with the electronic record at each instance at which it is submitted for admission.

The Supreme Court's pre-BSA decisions remain analytically valuable because section 63 substantially carries forward the special treatment of computer output under former section 65B of the Indian Evidence Act. In *Anvar P.V. v P.K. Basheer*, the Court treated the certificate as the prescribed mode for admitting secondary electronic evidence. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* reaffirmed the certificate as a condition precedent where the original device is not itself produced and emphasized source and authenticity as the central safeguards. The BSA adds communication devices, semiconductor memory, networked and intermediary environments, and a scheduled certificate format, but the logic remains provenance-oriented.

For facial recognition, at least three electronic objects may exist: the probe image, the gallery or relevant gallery extract, and the generated output. Each may pass through different systems. A certificate for the final PDF report cannot silently authenticate the CCTV file from which the probe was extracted or the gallery as it existed when searched. The prosecution should identify the chain of computer outputs and state which certificate covers which object. Where the output is recreated at a later date, the recreation should not be treated as the contemporaneous result unless the underlying model, gallery and settings are shown to be identical.

Most importantly, statutory authentication does not establish substantive truth. A compliant certificate can prove that a specified system produced a specified candidate list in a described manner. It cannot prove that the model was scientifically valid, that its error rate was acceptable, or that the person ranked first was present at the scene. Treating certification as proof of accuracy would collapse admissibility and weight, contrary to the structure of the BSA.

4.2 Expert opinion and the duty to expose grounds

Section 39(1) BSA makes the opinion of a person specially skilled in science, art or any other field relevant when the court must form an opinion on that point. Section 39(2) specifically recognizes the opinion of an Examiner of Electronic Evidence notified under section 79A of the Information Technology Act, 2000. Section 40 makes facts relevant when they support or are inconsistent with expert opinion, and section 45 makes the grounds on which an expert opinion is based relevant. Read together, these provisions support inquiry beyond the conclusion.

A facial examiner should therefore explain whether the opinion concerns image comparison, system validation, digital integrity or all three. Competence in extracting and hashing a file does not necessarily establish competence in facial comparison or statistical performance. The report should describe the comparison method, observed similarities and differences, limitations in the probe, whether the reviewer knew that the candidate was a police suspect, and how the conclusion was expressed. A bare statement that ‘the software matched the accused at 92 per cent’ is neither a transparent expert method nor a meaningful probability statement.

Courts should also resist automation bias in the assessment of expert evidence. Expert opinion is advisory; adjudicative responsibility remains with the court. A score may appear objective because it is numerical, but its meaning depends on calibration, test population and threshold. Cross-examination is ineffective if the witness can neither identify the model version nor explain the validation report. In such a case the court may admit an authenticated output but assign little weight, exclude an unsupported expert inference where ordinary reliability requirements are not met, or direct production of foundational material before ruling.

4.3 The candidate list as exculpatory context

The complete candidate list can be as important as the selected candidate. If several faces have similar scores, the defence may argue that the system did not discriminate reliably. If the selected candidate was not top-ranked, the human selection process becomes central. If investigators changed thresholds or searched multiple galleries until a desired person appeared, those iterations bear on weight and possible confirmation bias. Disclosure of only the final screenshot removes precisely the context needed to test the inference.

P. Gopalkrishnan @ Dileep v State of Kerala recognized that electronically stored content can be a document in criminal proceedings and considered how defence access should be balanced against the privacy and dignity of a victim. The case supports two relevant propositions: relied-upon digital material cannot be made immune from fair-trial scrutiny merely because it is stored electronically, and access can be structured through safeguards rather than reduced to an all-or-nothing choice. For facial-recognition material, protective orders, supervised inspection, redaction of unrelated identities, confidentiality undertakings and defence-expert access can protect gallery subjects and legitimate security interests while preserving an effective challenge.

Table 3. Indian doctrinal authorities and their application to facial-recognition evidence

Authority	Controlling proposition	Application
<i>E.P. Royappa v State of Tamil Nadu</i> (1974)	Arbitrariness is antithetical to equality under Article 14.	Undisclosed watchlist criteria, ad hoc thresholds or selective follow-up can be reviewed as arbitrary State action.
<i>Maneka Gandhi v Union of India</i> (1978)	Procedure affecting liberty must be fair, just and reasonable.	A significant adverse action should not rest on an opaque score without notice, reasons and opportunity to answer.
<i>Mohinder Singh Gill v CEC</i> (1978)	Public action is judged by the reasons stated, not later supplementation.	Investigators and experts should preserve contemporaneous reasons for selecting a candidate; litigation cannot reconstruct them.
<i>Kranti Associates v Masood Ahmed Khan</i> (2010)	Reasons restrain arbitrary power and make review possible.	A speaking expert report should expose decisive factors, limitations and human judgment, not merely a score.
<i>K.S. Puttaswamy v Union of India</i> (2017)	Privacy is fundamental; intrusion requires legality, legitimate aim and proportionality.	Image collection, gallery construction and broad searches require a lawful, necessary and proportionate design.
<i>Anvar P.V.</i> (2014); <i>Arjun Panditrao</i> (2020)	Electronic output must follow the statutory mode of authentication.	Every material computer output needs source and integrity proof, but certification does not prove match

Authority	Controlling proposition	Application
		accuracy.
P. Gopalkrishnan @ Dileep (2020)	Digital content can be a document; defence access may be structured to protect competing rights.	Courts can permit meaningful testing of FRT material under controlled access conditions.

5. Criminal Procedure and the Right to an Effective Challenge

Section 193 BNSS structures the police report and the transmission of relied-upon material to the Magistrate, while section 230 requires supply to the accused of the police report, first information report, witness statements and other documents forwarded with it, subject to the statutory treatment of voluminous material. Electronic service can facilitate access, but digitization is not completeness. A facial-recognition report may be unintelligible without the supporting records in Table 2.

The prosecution's disclosure obligation should turn on materiality, not on whether a file will be formally exhibited. A validation report, failed candidate search, reviewer note or threshold-change log may undermine the weight of the selected match even if the prosecution does not propose to tender it. Where such material is held by a private vendor, the State should not be permitted to create an evidentiary blind spot by outsourcing. Procurement and deployment contracts must reserve audit, preservation and litigation-access rights. If the State cannot obtain the material needed to test its own system, the resulting score should receive correspondingly diminished weight.

Trade secrets and security do not justify categorical non-disclosure. Wexler's analysis of proprietary criminal-justice technologies shows how private secrecy can obstruct the accused's ability to examine the basis of adverse evidence. Indian courts already manage sensitive material through inspection, confidentiality and limited disclosure. The correct question is which information is necessary to test the prosecution's proposition and whether less restrictive arrangements can protect legitimate interests. In many cases, performance reports and operational logs will answer the legal question without disclosure of source code.

Remedy should track prejudice. Missing metadata that does not affect the contested issue may justify limited weight or an opportunity to cure. Destruction of the gallery snapshot, model version or complete candidate list after the prosecution relies on the result is more serious because the search cannot be reproduced. Deliberate or negligent loss of indispensable records may support exclusion, an adverse inference, recall of a witness, further disclosure, or a direction that the match cannot corroborate identity. The court should record why the chosen remedy protects trial fairness.

6. Privacy, Data Protection and AI Governance

6.1 Constitutional privacy remains the floor

Facial templates are derived from bodily characteristics and enable persistent identification across contexts. Their use therefore implicates informational privacy even where the source photograph was taken in public. *Justice K.S. Puttaswamy (Retd) v Union of India* requires State intrusions to have a legal basis, pursue a legitimate aim and satisfy proportionality. The Aadhaar judgment further illustrates that architecture, purpose limitation and safeguards matter to proportionality. For policing, a general power to investigate does not answer every design question: who may enter a watchlist, which offences justify a search, how wide the location and time window may be, how long templates are retained, and whether persons cleared by the search are deleted.

The comparative decision in *R (Bridges) v Chief Constable of South Wales Police* is instructive because the Court of Appeal did not declare all police facial recognition unlawful. It found that the governing framework left excessive discretion over who could be placed on a watchlist and where the technology could be used; it also found deficiencies in the data-protection impact assessment and performance of the public-sector equality duty. The lesson for India is institutional: proportionality must constrain the operational variables before deployment, not merely justify the objective after a match.

6.2 What the DPDP framework adds — and what it does not

The DPDP Act expressly defines 'automated' processes and 'processing' broadly, includes the State within the definition of person, and applies to digital personal data subject to statutory exclusions. Section 8(3) is directly relevant: where personal data are likely to be used to make a decision affecting a Data Principal, the Data Fiduciary must ensure completeness, accuracy and consistency. Section 10 provides for enhanced duties of a notified Significant Data Fiduciary, including a Data Protection Officer, independent data audit and periodic Data Protection Impact Assessment. The 2025 Rules add annual assessment and audit requirements and due diligence to verify that technical measures, including algorithmic software, are not likely to pose risk to Data Principals' rights.

These provisions can improve governance of facial-recognition databases, but they are not an evidence code. The Act does not create an express right not to be subject to a solely automated decision, a general right to an explanation of a match, or a criminal-discovery rule. Section 7 permits several legitimate uses by the State, and section 17(1)(c) disappplies substantial obligations and Data Principal rights where processing is in the interest of prevention, detection, investigation or prosecution of an offence or contravention. Constitutional review and trial fairness therefore remain necessary even where data-protection remedies are unavailable.

Commencement must also be stated accurately. G.S.R. 843(E), dated 13 November 2025, brought institutional provisions into force immediately, scheduled consent-manager provisions one year later, and scheduled the principal processing obligations and rights eighteen months after Gazette publication. Rule 1 of the DPDP Rules follows a corresponding phased structure. At the study cut-off, the notification is legally important, but many substantive duties relied upon in future-facing compliance analysis have not yet commenced. A court should not misdescribe a future statutory duty as presently enforceable; it may nevertheless treat the legislative design as confirming the relevance of accuracy, impact assessment and audit.

6.3 The 2025 AI Governance Guidelines as an interpretive bridge

The India AI Governance Guidelines organize national policy around seven sutras, including People First, Fairness and Equity, Accountability, Understandable by Design, and Safety, Resilience and Sustainability. They recommend proportionate safeguards, accessible grievance redressal, transparency reporting, algorithmic auditing, and human-in-the-loop mechanisms at critical decision points. They also recognize that sensitive and high-risk uses may require sector-specific regulation. These recommendations are closely aligned with evidentiary needs because an investigator cannot disclose, and a court cannot review, what a system has failed to record.

The Guidelines are not a substitute for legislation and do not create a new ground of criminal admissibility. Their legitimate role is narrower. They can inform procurement standards, police manuals, laboratory accreditation, prosecutorial disclosure practice and the content of reasonable due diligence. They also demonstrate that traceability, explainability and grievance redressal are not foreign constraints being imported into Indian law; they are components of India's own declared governance approach.

NITI Aayog's earlier facial-recognition use-case paper is even more specific. It recommends accessible grievance mechanisms, human review in cases where utility or accuracy is in question, and privacy-by-design documentation. Read with the 2025 Guidelines, it supports a sectoral practice direction stating that law-enforcement facial recognition must not generate an adverse legal consequence without review and a preserved explanation of the reviewer's action.

Table 4. Coverage and residual gaps in the Indian legal framework

Safeguard	Existing legal anchor	Residual gap
Lawful and proportionate search	Constitutional privacy; general criminal law	No uniform statutory rule for watchlist criteria, search scope or prior authorization.
Authentic electronic output	BSA ss 61–63 and scheduled certificate	Authenticates source/integrity; does not validate model or identify the person.
Scientific reliability	BSA ss 39, 40 and 45; expert examination	No FRT-specific validation threshold, error-rate disclosure rule or standard conclusion scale.
Accuracy and algorithmic risk	DPDP Act ss 8(3), 10; DPDP Rules r 13	Phased commencement, Significant Data Fiduciary trigger and law-enforcement exemptions limit coverage.
Human oversight and transparency	India AI Governance Guidelines; NITI Aayog FRT paper	Principle-based and largely non-binding; requires translation into sectoral operating rules.
Defence challenge	BNSS disclosure; Arts 14 and 21; fair-trial doctrine	Operational and vendor records may not be indexed or preserved unless contracts and manuals require it.
Decision and remedy	Judicial evaluation of relevance, weight and fairness	No uniform remedy for missing logs, irreproducible searches or uncorroborated match evidence.

7. Comparative Calibration

Comparative law offers useful design choices but should not be transplanted without regard to Indian constitutional and institutional conditions. The European Union AI Act treats specified biometric identification systems as high-risk and imposes duties concerning risk management, data governance, technical documentation, logging, transparency, human oversight, accuracy, robustness and cybersecurity. It places strict conditions on real-time remote biometric identification for law enforcement in publicly accessible spaces and requires attention to

necessity, proportionality and temporal, geographic and personal limits. Article 86 gives certain affected persons a right to clear and meaningful explanations of the role of a high-risk AI system in an adverse decision.

Three lessons are relevant. First, risk classification should turn on use and consequence, not merely on whether the software is labelled AI. A retrospective search that supplies the principal basis for arrest can be high-impact even if the model itself is commercially ordinary. Second, documentation and logs are substantive safeguards because they make later review possible. Third, an explanation right is not satisfied by revealing source code or a generic description of machine learning. The explanation must connect the system's role and the decisive elements to the affected decision, permitting the person to understand and exercise legal rights (Selbst and Powles, 2017; Wachter et al., 2018).

The Court of Justice of the European Union's *SCHUFA* decision likewise treated scoring as automated decision-making where a third party gives the score a determining role in a decision. The functional point travels well: police cannot avoid scrutiny by describing FRT as merely 'decision support' if officers ordinarily act on its output without independent assessment. Indian courts should examine material influence — whether the output set the investigation on a path, supplied the reason for arrest, shaped witness identification or became the principal link to the accused.

At the same time, explanation alone is insufficient. Edwards and Veale warn against a transparency fallacy in which disclosure of logic is assumed to remedy unfairness. Reliable criminal use also needs validation, record preservation, competent human review, contestability and corroboration. The MATCH protocol therefore treats explanation as one component of an evidentiary system rather than a standalone right capable of curing every defect.

8. The MATCH Protocol

***Core rule:** A facial-recognition result may guide investigation, but it should not prove identity unless the State can show a lawful mandate, validated performance, a traceable inference, meaningful defence access, qualified human verification and independent corroboration.*

8.1 M — Mandate the use

The deploying authority should identify the statutory function and written policy authorizing the use, the offences or circumstances that justify a search, the permissible data sources, retention periods, and the officer empowered to approve deployment. Watchlist inclusion criteria must be objective and auditable. The search should be limited by purpose, location, time and target class. Urgent use may proceed under recorded emergency reasons, followed by prompt supervisory review.

Mandate also requires separating investigative search from legal consequence. A policy should state that FRT alone cannot justify charge, adverse witness exposure or guilt. If a match contributes to arrest or search, the officer should record what independent facts supplied reasonable grounds. This contemporaneous statement prevents a later affidavit from converting an intuitive reliance on the score into a reasoned decision.

8.2 A — Audit fit-for-purpose performance

Before deployment, the authority should obtain independent or independently reviewable validation for the actual task. At minimum, the report should identify the model and version, test data, image conditions, gallery sizes, thresholds, false-match and false-non-match rates, subgroup performance and uncertainty. The operating threshold should be selected for the risk of the criminal use, not inherited from a vendor demonstration. Material software, gallery or camera changes should trigger revalidation.

Case-specific quality assessment is separate from general validation. A high-performing model can produce an unreliable result from a poor probe. The case file should therefore include automated and human quality assessments, any enhancement process and reasons for proceeding despite limitations. Courts should be cautious where a validation report concerns one-to-one verification but the police used one-to-many identification, or where it concerns controlled photographs while the probe is low-resolution CCTV.

8.3 T — Trace the complete inference

Traceability requires an immutable search record: original probe and hash; every derived image; software and model version; threshold; date and time; operator; gallery identifier and snapshot or reproducible manifest; complete candidate list; scores; system messages; manual actions; reviewer notes; exports; and subsequent sharing. Each object should have a stable identifier so that the section 63 certificate and expert report cannot refer ambiguously to 'the footage' or 'the software result'.

A reproducibility statement should disclose whether the search can be rerun. Machine-learning services may change silently, and cloud vendors may not retain old versions. If exact reproduction is impossible, the State should preserve sufficient contemporaneous material for an independent expert to evaluate what happened.

Procurement contracts should specify retention, export formats, hash generation, audit access and litigation holds before operational use begins.

8.4 C — Enable an effective challenge

The accused should receive the match report, section 63 materials, relevant probe and gallery information, complete candidate list, validation summary, threshold, model/version, reviewer notes, limitations and the prosecution's statement of the role the match played. Defence requests for deeper access should be assessed by materiality. The court may use supervised expert inspection, redaction, confidentiality undertakings or sealed proceedings to protect unrelated biometric data and legitimate trade secrets.

The challenge must occur early enough to matter. Disclosure after the prosecution expert has testified may prevent informed cross-examination or independent testing. The trial court should hold a pre-trial reliability hearing where the match is disputed and material to identity. The prosecution bears the burden of establishing the foundation for the inference it asks the court to draw; the accused need not reverse-engineer an undisclosed system merely to show that a challenge is plausible.

8.5 H — Human verification and independent corroboration

A trained examiner should review the images using a documented method and should be able to reach an inconclusive result. Where practicable, the reviewer should initially receive only the information necessary for comparison, reducing contextual bias. A second review is appropriate for high-stakes use. The expert report must distinguish the machine's candidate ranking from the examiner's conclusion and explain observed limitations.

Human review does not make weak data strong. It is a safeguard against automation error, not a ritual endorsement. The final identity proposition should be corroborated by evidence independent of the FRT search, such as reliable witness evidence obtained without suggestion, location evidence, possession, conduct, forensic traces or other circumstances. FRT may help locate that evidence. An uncorroborated match, particularly from a poor image or large gallery, should not be sufficient for conviction.

Table 5. The MATCH protocol for law-enforcement facial recognition

Element	Minimum record or action	Evidentiary purpose
M — Mandate	Written lawful basis; use-case limits; watchlist criteria; approval; retention; recorded emergency process	Prevents indiscriminate or purpose-shifted search.
A — Audit	Task-specific validation; threshold; error rates; subgroup tests; image-quality assessment; drift review	Shows whether the system is fit for the claimed inference.
T — Trace	Hashes; probe and derivatives; gallery manifest; model/version; settings; full candidate list; operator and reviewer logs	Makes the search reproducible and the statutory certificate intelligible.
C — Challenge	Timely defence disclosure; materiality-based expert access; protective orders; pre-trial reliability hearing	Converts formal access into a meaningful opportunity to test evidence.
H — Human and corroborate	Qualified comparison; documented grounds; second review where needed; independent non-FRT evidence	Keeps the score as a lead and prevents circular confirmation.

9. Judicial Treatment of a Disputed Match

A court confronted with facial-recognition material should decide five questions in sequence. First, was the search lawfully and proportionately conducted? Second, have the electronic objects actually relied upon been authenticated under the BSA? Third, is the expert or other witness competent to explain the system and the human comparison? Fourth, has the prosecution demonstrated sufficient reliability for the specific use? Fifth, has the accused received material necessary to challenge the inference? A favourable answer to the second question does not predetermine the fourth.

The purpose for which the evidence is offered should control the threshold. A candidate list may be relevant to explain why police approached a suspect, even when it is too unreliable to prove identity. If offered as substantive proof, the court should require the MATCH foundation. The judgment should state the role assigned to the match, the limitations acknowledged, the corroboration relied upon and why alternative candidates or error evidence do not create reasonable doubt.

Courts should avoid numerical overclaiming. Similarity is not the probability that the accused is the source. Unless an appropriately qualified expert provides a validated likelihood ratio or other interpretable measure, percentages should not be translated into statements such as '92 per cent certain'. Where only a proprietary score is available, the court should describe it as a ranking measure and assess the surrounding evidence.

A useful exclusion principle is narrow: where the prosecution cannot identify the model/version, preserve the relevant probe and output, or provide any fit-for-purpose validation, the score should not be admitted as substantive proof of identity. A useful insufficiency principle is broader: even an authenticated and technically explained FRT result should ordinarily require independent corroboration before it can support conviction. This preserves investigative utility while respecting the asymmetry between generating a lead and depriving a person of liberty.

Table 6. Proposed judicial responses according to evidentiary condition

Condition	Typical finding	Proportionate response
Investigative lead only	Search record may explain police conduct; not tendered for truth of identity	Court prevents prosecution from using the score as corroboration.
Authenticated but weak	Section 63 foundation present; validation, logs or quality evidence incomplete	Admit for limited purpose or assign little weight; order further disclosure where curable.
Reliable and contestable	MATCH foundation substantially established; defence had timely expert opportunity	Treat as supporting identification, subject to ordinary expert-evidence evaluation.
Irreproducible or materially undisclosed	Model/gallery/output lost, or indispensable material withheld without adequate substitute	Exclude the match inference, draw appropriate adverse inference, or prohibit reliance.
Uncorroborated identification	Technically supported result but no independent evidence connects accused to offence	Do not treat the match alone as sufficient for conviction.

10. Implementation Pathway

The MATCH protocol does not require a single legislative intervention. The Bureau of Police Research and Development and State police organizations can incorporate the preservation and human-review fields into standard operating procedures. Forensic laboratories can develop competency and reporting standards for image comparison and system validation. Prosecutors can use a disclosure index that identifies each electronic object and the corresponding section 63 certificate. Trial courts and High Courts can issue practice directions for pre-trial reliability hearings and controlled defence-expert access.

Public procurement is the highest-leverage intervention. A tender should require independent testing on relevant Indian conditions; versioned performance reports; exportable logs; preservation of gallery manifests; notice of model changes; audit and incident rights; limits on secondary use; deletion assistance; litigation holds; and access sufficient to answer court orders. A vendor's refusal to support legal scrutiny should count against technical eligibility, not become a reason to dilute the accused's rights after deployment.

The DPDP compliance timetable offers a parallel opportunity. When section 8 accuracy obligations, section 10 impact-assessment duties and Rule 13 algorithmic due diligence become operative for covered entities, implementing guidance should state that biometric decision systems require use-case-specific testing, recorded thresholds and human escalation. Law-enforcement exemptions should be accompanied by sectoral safeguards, since exemption from specified data-principal rights does not remove Articles 14 and 21 or the judicial duty to evaluate evidence fairly.

Finally, transparency can be layered. Public transparency reports should identify use cases, legal bases, aggregate search numbers, watchlist categories, performance testing, complaints and confirmed misidentifications without revealing active investigations. Regulators and courts should receive fuller confidential technical reports. Accused persons should receive case-specific material necessary for challenge. This model reconciles public accountability, operational security, privacy of gallery subjects and trial fairness more effectively than either total secrecy or indiscriminate publication.

11. Limitations and Future Research

This article is doctrinal and does not measure actual police deployment, vendor performance or trial-court practice. Public documentation of Indian deployments is uneven, and the absence of a reported appellate ruling does not imply that facial-recognition outputs have not been used in investigations or lower-court proceedings. Empirical work should examine case files, procurement contracts, section 63 certificates, disclosure orders and judicial descriptions of computer-assisted identification.

Future research should also test whether local image conditions and demographic composition produce performance differences, compare blind and context-informed human review, and evaluate how often candidate lists change when thresholds or galleries change. A further doctrinal question is the relationship between FRT-

generated suspicion and downstream evidence: a flawed match may lead to a witness identification, search or confession whose apparent independence is contested. Courts will need principled rules for attenuation, prejudice and remedy.

The MATCH protocol is deliberately modular. Its legal force will differ across stages and institutions until specific rules are adopted. That is a limitation, but also a practical advantage: preservation, validation and disclosure can improve immediately, while legislative debate continues over authorization standards and prohibited uses.

12. Conclusion

Facial recognition compresses a complex chain of collection, transformation, comparison and human judgment into a persuasive number. Evidence law must decompress that number. Under the BSA, electronic-record certification can establish provenance and integrity; it does not establish that an algorithmic comparison is scientifically valid or that the accused is the source of an image. Expert-evidence provisions make the grounds and contradictory facts relevant, while criminal-procedure and constitutional guarantees require an opportunity to test material that bears on liberty.

India's data-protection and AI-governance instruments reinforce accuracy, audit, risk assessment, transparency and human oversight, but they do not yet supply a complete law of facial-recognition evidence. The resulting gap should not be filled by either technological exceptionalism or a blanket assumption of unreliability. It should be filled by disciplined proof.

The MATCH protocol provides that discipline: Mandate the use, Audit performance, Trace the full inference, permit Challenge, and require Human verification plus independent corroboration. Its most important proposition is modest. A match score can help an investigation ask the next question. It should never prevent the court from asking how the answer was produced.

References

Cases

- Anvar P.V. v P.K. Basheer, (2014) 10 SCC 473.
Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
E.P. Royappa v State of Tamil Nadu, (1974) 4 SCC 3.
Justice K.S. Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1.
K.S. Puttaswamy (Aadhaar-5J) v Union of India, (2019) 1 SCC 1.
Kranti Associates Pvt Ltd v Masood Ahmed Khan, (2010) 9 SCC 496.
Maneka Gandhi v Union of India, (1978) 1 SCC 248.
Mohinder Singh Gill v Chief Election Commissioner, (1978) 1 SCC 405.
P. Gopalkrishnan @ Dileep v State of Kerala, (2020) 9 SCC 161.
Prem Sagar Manocha v State (NCT of Delhi), (2016) 4 SCC 571.
R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058; [2020] 1 WLR 5037.
SCHUFA Holding AG (Scoring), Case C-634/21, EU:C:2023:957 (CJEU, 7 December 2023).
Selvi v State of Karnataka, (2010) 7 SCC 263.
S.N. Mukherjee v Union of India, (1990) 4 SCC 594.

Legislation and official materials

- Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No 46 of 2023), ss 193 and 230.
Bharatiya Sakshya Adhiniyam, 2023 (Act No 47 of 2023), ss 39–40, 45 and 61–63 and Schedule.
Constitution of India, arts 14, 21, 32 and 226.
Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No 225 (2024).
Digital Personal Data Protection Act, 2023 (Act No 22 of 2023).
Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, 13 November 2025, as corrected.
European Parliament and Council, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689.
Government of India, Commencement Notification under the Digital Personal Data Protection Act, 2023, G.S.R. 843(E), 13 November 2025.
IndiaAI, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (Ministry of Electronics and Information Technology, 2025).
Information Technology Act, 2000 (Act No 21 of 2000), s 79A.

- INTERPOL, World Economic Forum, UNICRI and Netherlands Police, *A Policy Framework for Responsible Limits on Facial Recognition: Use Case — Law Enforcement Investigations* (2nd edn, 2022).
- NITI Aayog, *Approach Document for India: Part 1 — Principles for Responsible AI* (Government of India, 2021).
- NITI Aayog, *Approach Document for India: Part 2 — Operationalizing Principles for Responsible AI* (Government of India, 2021).
- NITI Aayog, *Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology* (Discussion Paper, 2022).
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (adopted 23 November 2021, published 2022).

Books, reports and scholarship

- Barocas, S. and Selbst, A.D. (2016), 'Big Data's Disparate Impact', *California Law Review*, 104(3), 671–732.
- Buolamwini, J. and Gebru, T. (2018), 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', *Proceedings of Machine Learning Research*, 81, 77–91.
- Citron, D.K. (2008), 'Technological Due Process', *Washington University Law Review*, 85(6), 1249–1313.
- Cobbe, J. (2019), 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making', *Legal Studies*, 39(4), 636–655.
- Edwards, L. and Veale, M. (2017), 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For', *Duke Law & Technology Review*, 16, 18–84.
- Garvie, C., Bedoya, A.M. and Frankle, J. (2016), *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology, Georgetown Law.
- Grother, P., Ngan, M. and Hanaoka, K. (2019), *Face Recognition Vendor Test Part 3: Demographic Effects*, NISTIR 8280, National Institute of Standards and Technology. doi:10.6028/NIST.IR.8280.
- Kroll, J.A., Huey, J., Barocas, S., Felten, E.W., Reidenberg, J.R., Robinson, D.G. and Yu, H. (2017), 'Accountable Algorithms', *University of Pennsylvania Law Review*, 165(3), 633–705.
- Roth, A. (2017), 'Machine Testimony', *Yale Law Journal*, 126(7), 1972–2053.
- Selbst, A.D. and Powles, J. (2017), 'Meaningful Information and the Right to Explanation', *International Data Privacy Law*, 7(4), 233–242. doi:10.1093/idpl/ix022.
- Wachter, S., Mittelstadt, B. and Russell, C. (2018), 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR', *Harvard Journal of Law & Technology*, 31(2), 841–887.
- Wexler, R. (2018), 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System', *Stanford Law Review*, 70(5), 1343–1429.