



# LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.324>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: [www.lijdlr.com](http://www.lijdlr.com)

Under the Platform of LawFoyer – [www.lawfoyer.in](http://www.lawfoyer.in)

---

*After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.*

---

*In case of any suggestions or complaints, kindly contact ([info.lijdlr@gmail.com](mailto:info.lijdlr@gmail.com))*

*To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)*

---

# OPINION WITHOUT AN OPINION-HOLDER: SECTION 39 BSA, EXPERT EVIDENCE, AND ALGORITHMIC BLACK-BOX TESTIMONY

---

Samarth Udasin<sup>1</sup>, Harshwardhan Yadav<sup>2</sup> & Mohit Jain<sup>3</sup>

## I. ABSTRACT

*Section 39 of the Bharatiya Sakshya Adhiniyam 2023 carries forward, almost unchanged, the nineteenth-century architecture of opinion evidence: a person “especially skilled” in a field furnishes the court with reasoned criteria it can independently test. Section 330 of the Bharatiya Nagarik Suraksha Sanhita 2023 compounds the difficulty by allowing an expert's report to be read into evidence, and the expert to go unexamined, unless a party affirmatively disputes it. Both provisions presuppose a human opinion-holder, someone who studied a subject, formed a view, and can defend that view under cross-examination. That presupposition fails when the witness produced in court is a police technician who ran a proprietary facial-recognition or predictive-risk tool without access to its training data, its matching logic, or its validated error rates. This article argues that such testimony is not opinion evidence within the meaning of section 39 at all, but a species of proof Indian evidence law has not yet named. It develops an analytical taxonomy of the opacity such testimony presents, and reads section 39 and section 330 against three comparative bodies of law: the American Daubert–Frye reliability tradition and its confrontation-clause jurisprudence on machine-generated forensic reports; the English common-law presumption that computers operate correctly and its catastrophic failure in the Post Office Horizon scandal; and the European Union's data-protection and artificial-intelligence law, which increasingly regulates algorithmic opacity before a tool is ever deployed rather than after it produces evidence. The comparative material shows both that mature legal systems have not settled on a common answer, and that each has*

---

<sup>1</sup> 5th year B.Sc. LL.B. (Hons.) [Cyber Security] student at National Law Institute University, Bhopal (India). Email: samarthudasin.bscllb@nliu.ac.in

<sup>2</sup> 5th year B.Sc. LL.B. (Hons.) [Cyber Security] student at National Law Institute University, Bhopal (India). Email: harshwardhanyadav.bscllb@nliu.ac.in

<sup>3</sup> 5th year B.Sc. LL.B. (Hons.) student at National Law Institute University, Bhopal (India). Email: mohitjain.bscllb@nliu.ac.in

*learned something India can still learn pre-emptively. The article closes with a doctrinal response anchored in the certification model Indian law already applies to electronic records.*

## II. KEYWORDS

Opinion evidence; expert testimony; algorithmic opacity; Bharatiya Sakshya Adhiniyam 2023; machine testimony.

## III. INTRODUCTION

In 2020, Robert Williams was arrested at his home in Farmington Hills, Michigan, in front of his wife and two daughters, after facial-recognition software matched his driving-licence photograph to grainy CCTV footage of a shoplifter.<sup>4</sup> The detective who sought the warrant relied “almost exclusively” on the algorithm's output; he did not, and on the facts could not, explain why the software matched Williams's face to the suspect's rather than any of the thousands of other faces in the database.<sup>5</sup>

The matter never reached a criminal trial; the charges were dropped and Williams later settled a civil claim against the city, so no court ever had to decide what kind of witness the detective was, or whether his testimony about the software's output could survive cross-examination. India's courts will not have that luxury for much longer.

In August 2026, the Supreme Court of India agreed to hear a writ petition filed by a Rajya Sabha member challenging the Delhi Police's use of live facial-recognition and biometric surveillance tools, including a vehicle-mounted system and camera-equipped smart spectacles, against protesters at Jantar Mantar.<sup>6</sup> The petition is

---

<sup>4</sup>Civil Rights Litigation Initiative, University of Michigan Law School and American Civil Liberties Union, 'Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on Facial Recognition Technology' (ACLU, 28 June 2024) [www.aclu.org/press-releases/civil-rights-advocates-achieve-nations-strongest-police-department-policy-facial](https://www.aclu.org/press-releases/civil-rights-advocates-achieve-nations-strongest-police-department-policy-facial) accessed 8 September 2026.

<sup>5</sup>*ibid*; see also Reason, 'Faulty Facial Recognition Tech Got Him Arrested. Now He's Getting a \$300,000 Payout' (23 July 2024) <https://reason.com/2024/07/23/faulty-facial-recognition-tech-got-him-arrested-now-hes-getting-a-300000-payout/> accessed 8 September 2026.

<sup>6</sup>Indian MP Asks the Supreme Court to Halt Police Facial Recognition at Protests' (IDTechWire, 28 July 2026) <https://idtechwire.com/indian-mp-asks-the-supreme-court-to-halt-police-facial-recognition-at-protests/> accessed 8 September 2026; 'India's Supreme Court to Hear Challenge to Police Facial Recognition at Protests' (IDTechWire, 14 August 2026) <https://idtechwire.com/indias-supreme-court-to-hear-challenge-to-police-facial-recognition-at-protests/> accessed 8 September 2026. The matter is listed as *AA Rahim MP v Union of India*, Diary No 45049 of 2026 (SC, pending).

framed, understandably, in the language of privacy; it invokes the legality-necessity-proportionality test laid down in *Justice K.S. Puttaswamy (Retd) v Union of India*<sup>7</sup>, and it will be decided, if at all, on that constitutional terrain.

But every one of the technologies it describes will, sooner or later, generate an output that the prosecution wishes to use as evidence: a face matched to a name, a person flagged as a risk. When that day comes, the question will no longer be whether the State was entitled to collect the data. It will be whether the resulting output is opinion evidence under section 39 of the Bharatiya Sakshya Adhiniyam 2023 ('BSA'), and, if it is called at all, whether the person called to explain it can actually do so.

This article is not about facial-recognition policy, algorithmic bias, or the wisdom of predictive policing. Those are important questions, and they are being litigated in the privacy, administrative-law, and data-protection registers where they belong, which this article draws on comparatively, in Parts VI and VII, precisely because they have already confronted versions of the opacity problem this article is about.

Its own question is narrower and more technical: does the testimony of a technician who operates a proprietary algorithmic tool, without access to its internal logic, training data, or error rates, fit within the doctrinal category that section 39 BSA calls "opinion of an expert", and can section 330 of the Bharatiya Nagarik Suraksha Sanhita 2023 ('BNSS') safely extend its unless-disputed shortcut to reports of that kind?

Part II reconstructs what Indian case law actually requires of an "expert" under section 39. Part III examines how section 330 BNSS's cross-examination shortcut interacts with that requirement, and where it breaks down. Part IV names the resulting gap precisely, and builds an analytical taxonomy of the different kinds of opacity that produce it. Parts V to VII turn comparative, to the American reliability-and-confrontation tradition, to the English common-law presumption of computer reliability and its collapse in the Post Office Horizon scandal, and to the European Union's newer, ex-ante regulatory model, not to import any one of them wholesale,

---

<sup>7</sup>(2017) 10 SCC 1.

but because each shows a mature system wrestling with a version of the same problem, without a shared answer.

Part VIII reads section 39 and section 330 against the certification model India already uses for electronic records and against the constitutional overlay supplied by *Puttaswamy* and the pending *Rahim* litigation. Part IX proposes a doctrinal fix that draws on all three comparative traditions.

### **A. Research Objectives**

This paper seeks to identify the doctrinal gap that arises when algorithmic outputs are tendered as expert opinion evidence under section 39 of the Bharatiya Sakshya Adhiniyam 2023.

It examines whether a technician who merely operates a proprietary algorithmic tool can properly be treated as an expert opinion-holder, particularly where the witness lacks access to the tool's internal logic, training data, validation methodology, or error rates. The paper further evaluates the interaction between section 39 BSA and section 330 of the Bharatiya Nagarik Suraksha Sanhita 2023, and proposes a doctrinal response grounded in India's existing certification model for electronic records.

### **B. Research Questions**

This paper addresses the following research questions: first, whether testimony by a technician who operates a proprietary facial-recognition or predictive-risk tool, without access to its internal logic, training data, or validated error rates, falls within the doctrinal category of "opinion of an expert" under section 39 BSA; secondly, whether section 330 BNSS can safely extend its unless-disputed shortcut to algorithmic expert reports of this kind; and thirdly, what doctrinal safeguards Indian evidence law should adopt to ensure that algorithmic evidence is tested for reliability before being relied upon in criminal proceedings.

### **C. Research Methodology**

The paper adopts a doctrinal and comparative-law methodology. It first analyses the text of section 39 BSA, section 330 BNSS, and the Indian case law governing expert

opinion evidence, particularly the requirement that an expert provide reasons, data, and scientific criteria capable of judicial scrutiny.

It then undertakes a comparative examination of American reliability and confrontation-clause jurisprudence, English law on computer-generated evidence and the Post Office Horizon scandal, and the European Union's data-protection and artificial-intelligence regulatory framework. This comparative material is used not as a direct transplant, but as an analytical aid for developing a doctrinal response suited to Indian evidence law.

#### IV. SECTION 39 BSA AND THE OPINION-HOLDER REQUIREMENT

Section 39(1) BSA provides that “[w]hen the Court has to form an opinion upon a point of foreign law or of science or art, or any other field, or as to identity of handwriting or finger impressions, the opinions upon that point of persons specially skilled in such foreign law, science or art, or any other field ... are relevant facts and such persons are called experts.”<sup>8</sup> The phrase “or any other field” does not appear in section 45 of the repealed Indian Evidence Act 1872, which confined expert opinion to foreign law, science, art, and the identity of handwriting or finger impressions; commentators have noted that the BSA deliberately widens the category of subject-matter on which expert opinion may be led.<sup>9</sup>

Section 39(2) separately provides that where a court must form an opinion on information transmitted or stored in a computer resource or other electronic or digital form, the opinion of the “Examiner of Electronic Evidence” referred to in section 79A of the Information Technology Act 2000 is itself a relevant fact.<sup>10</sup> This second subsection matters for the present argument, and its limits matter more: it creates a designated expert for the authenticity and integrity of stored or transmitted electronic

---

<sup>8</sup>Bharatiya Sakshya Adhiniyam 2023, s 39(1).

<sup>9</sup>See J.P. Associates, 'Bharatiya Sakshya Adhiniyam, 2023' (Mondaq, 2023) [www.mondaq.com/india/new-technology/1417594/bharatiya-sakshya-adhiniyam-2023](https://www.mondaq.com/india/new-technology/1417594/bharatiya-sakshya-adhiniyam-2023) accessed 8 September 2026, noting the widening of the term 'expert' under s 39 BSA to include persons skilled in 'any other field'.

<sup>10</sup>Bharatiya Sakshya Adhiniyam 2023, s 39(2), referring to the Examiner of Electronic Evidence under the Information Technology Act 2000, s 79A.

material, but it says nothing about the reliability of an inference, a facial match, a risk score, that a piece of software draws from that material. Whether such an inference belongs under section 39(1)'s general “any other field” language, or falls into a gap between the two sub-sections, is precisely the question this article presses.

The statutory text alone does not tell a court what makes a witness “specially skilled”, so the content of the requirement has been supplied by case law carried forward without material change from the identically worded section 45 of the 1872 Act. In *State of Himachal Pradesh v Jai Lal*<sup>11</sup>, the Supreme Court held that an expert witness is “one who has made the subject upon which he speaks a matter of particular study, practice or observation”, and that expert evidence is “of an advisory character”; it does not go into evidence automatically merely because a witness is labelled an expert.

The Court quoted with approval the proposition that “the duty of an expert witness is to furnish the Judge with the necessary scientific criteria for testing the accuracy of the conclusions so as to enable the Judge to form his independent judgment by the application of this criteria to the facts proved.”<sup>12</sup> On the facts, the prosecution's horticulture-department witness failed this test: he could not show that his assessment of an apple orchard's productive capacity rested on any scientific study, and his conclusions were accordingly held to carry no evidentiary weight, regardless of his official designation.

The Supreme Court elaborated the same principle a decade later in *Ramesh Chandra Agrawal v Regency Hospital Ltd*<sup>13</sup>, holding that expert evidence is admissible only where three conditions are jointly satisfied: the expert must be within a recognised field of expertise; the evidence must be based on reliable principles; and the expert must be qualified in that discipline.<sup>14</sup> The Court was explicit that “mere assertion without mentioning the data or basis is not evidence, even if it comes from an expert”, and that

---

<sup>11</sup>AIR 1999 SC 3318 : (1999) 7 SCC 280.

<sup>12</sup>Jai Lal (n 8), applying the principle later restated in *Ramesh Chandra Agrawal v Regency Hospital Ltd* (2009) 9 SCC 709, para 12.

<sup>13</sup>(2009) 9 SCC 709.

<sup>14</sup>ibid para 12, citing Alan Merry and Alexander McCall Smith, *Errors, Medicine and the Law* (CUP 2001) 178.

where an expert “give[s] no real data in support of their opinion, the evidence ... may be excluded from consideration as affording no assistance in arriving at the correct value.”<sup>15</sup>

Read together, *Jai Lal* and *Ramesh Chandra Agrawal* establish that section 39 does not simply ask whether a witness carries an expert label or operates within a technical field; it asks whether the particular witness before the court can supply reasoning, namely data, method, and the connection between the two, that the court can test for itself. Call this the opinion-holder requirement. It is nowhere stated as a discrete element of section 39, but no authority applying the section can be read without it.

A further, structural feature of the traditional expert-opinion regime deserves attention because it disappears entirely in the algorithmic context. In *Murari Lal v State of Madhya Pradesh*<sup>16</sup>, the Supreme Court held that a handwriting expert's opinion does not require corroboration as a matter of law; an expert, the Court said, is “no accomplice”, but it immediately qualified that holding by noting the imperfect state of the science of handwriting identification and by affirming that a court may, and often should, verify the expert's reasoning through its own comparison of the disputed and admitted writings.<sup>17</sup>

That residual power of independent judicial verification, comparing samples, checking a chemist's calculation, weighing a medical opinion against the treatise it purports to apply, is a quiet but real safeguard built into the traditional model of expert evidence. It has no equivalent where the “expert” output is a similarity score generated by a neural network whose weights no judge, and typically no witness, can inspect.

The judge who could compare two signatures cannot compare two embeddings in a proprietary vector space. The internal check that *Murari Lal* treats as available even without corroboration is, for algorithmic opinion evidence, simply unavailable, a

---

<sup>15</sup>ibid, quoting the observation that mere assertion without data does not amount to evidence.

<sup>16</sup>AIR 1980 SC 531: (1980) 1 SCC 704.

<sup>17</sup>ibid; the Court's own comparative power is now preserved in the Bharatiya Sakshya Adhiniyam 2023, s 72 (formerly Indian Evidence Act 1872, s 73).

point this article returns to, from the opposite direction, when it considers how England has handled genuinely human facial-comparison opinion in *R v Atkins* in Part.

## V. BNSS SECTION 330 AND THE EROSION OF CROSS-EXAMINATION

Section 330 BNSS, headed “No formal proof of certain documents”, requires the prosecution and the accused to list every document filed and to admit or deny its genuineness within a prescribed period.<sup>18</sup> Its second proviso is the operative text for present purposes: “no expert shall be called to appear before the Court unless the report of such expert is disputed by any of the parties to the trial.”<sup>19</sup> Where genuineness is not disputed, sub-section (3) permits the document to be read into evidence without proof of the signature of the person by whom it purports to be signed.<sup>20</sup>

The provision sits alongside section 329 BNSS, the successor to section 293 of the repealed Code of Criminal Procedure 1973, which independently allows the reports of specified government scientific experts, chemical examiners, serologists, and the like, to be used as evidence without the expert's formal examination unless the court directs otherwise.<sup>21</sup> Section 330's proviso is broader: on its text it applies to any expert report filed as a document in the proceeding, not only to the government scientific experts enumerated in section 329.

The efficiency logic of section 330's proviso is sound for the evidentiary world it was written for. Where a forensic science laboratory's ballistics or chemical-analysis report reflects a well-understood, externally validated methodology, a defence lawyer or a rival expert can meaningfully read the report, evaluate the methodology on its face, and make an informed decision about whether contesting it is worth the trial's time. Non-disputation, in that world, functions as a considered waiver: the defence looked,

---

<sup>18</sup>Bharatiya Nagarik Suraksha Sanhita 2023, s 330(1).

<sup>19</sup>*ibid* s 330(1), second proviso.

<sup>20</sup>*ibid* s 330(3).

<sup>21</sup>Bharatiya Nagarik Suraksha Sanhita 2023, s 329.

understood, and chose not to fight. The shortcut converts an informed silence into an evidentiary shortcut, and little of substance is lost.

That assumption collapses precisely where the methodology is inaccessible to the party being asked to accept or dispute it. A defence lawyer confronted with a one-line report stating that a probe photograph was “matched” to a database image at a stated confidence score has nothing on the face of the report to evaluate: no error rate, no account of the matching algorithm, no record of how the specific deployment conditions, lighting, camera angle, image resolution, compare to the conditions under which the tool was validated, if it was validated at all. To “dispute” such a report meaningfully, counsel would already need to know what section 330 is designed to let the report substitute for: an examination of the expert.

The proviso thus creates a structural, not merely tactical, trap; silence born of opacity is treated identically to silence born of informed concession, and the shortcut is most likely to operate exactly where it is least justified. This is not a hypothetical concern: as Part VI shows, an English court has already found, in the starkest terms available, that treating a machine's output as reliable by default can reverse the practical burden of proof and produce a documented, systemic miscarriage of justice, without any algorithm, machine learning, or proprietary trade secret being involved at all.

It is worth adding that even where a report is disputed and the expert is duly called, section 330's proviso is satisfied by the mere fact of the witness's appearance. It does not ask, and cannot by its terms ask, whether the witness who appears is the opinion-holder that *Ramesh Chandra Agrawal* requires.

If the technician who operated the software takes the stand, the letter of section 330 is complied with regardless of whether that witness can satisfy the second *Ramesh Chandra Agrawal* precondition, that the evidence rests on principles she can herself vouch for as reliable. Compliance with the calling requirement and satisfaction of the underlying opinion-holder requirement identified in Part II are two different things, and section 330 secures only the first.

## VI. THE BLACK-BOX PROBLEM: WHAT KIND OF WITNESS IS A TECHNICIAN?

Consider the archetype the title of this article names. A police officer or forensic-cell operator runs a probe image through a facial-recognition system, of the kind the National Crime Records Bureau has sought to establish through its Automated Facial Recognition System procurement, and of the kind at issue in the pending *Rahim* litigation, or enters case data into a proprietary predictive-risk tool.<sup>22</sup> That witness can typically testify, from personal knowledge, to a narrow band of facts: which image or dataset was fed into the system, which database was queried, what score or rank the system returned, and what standard operating procedure was followed in reviewing the output.

She typically cannot testify, not because she is evasive, but because the information was never given to her, to the composition and provenance of the training data, the architecture or feature-weighting of the underlying model, the tool's validated false-match and false-non-match rates under conditions resembling the case at hand, or the logic by which a raw similarity score is converted into a reported "identification" or "risk level".

Measured against the three *Ramesh Chandra Agrawal* preconditions, this witness's position is uncomfortable. She may satisfy the first precondition in a loose sense: computer-vision-based identification and actuarial risk-scoring are recognised fields, even if the particular tool is proprietary. She plainly satisfies the third precondition, in the narrow sense that she is qualified to operate the interface she was trained to operate. It is the second precondition, that the evidence be based on principles the witness can show to be reliable, that she cannot satisfy, because she does not know the principles; she knows the interface.

---

<sup>22</sup>On the National Crime Records Bureau's Automated Facial Recognition System procurement and its constitutional exposure under *Puttaswamy*, see Panoptic, 'NCRB's National Automated Facial Recognition System' (Case Study) <https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system> accessed 8 September 2026.

On a faithful application of *Jai Lal*'s requirement that the witness “furnish the Judge with the necessary scientific criteria for testing the accuracy of the conclusions”, this witness cannot discharge the function that justifies treating her testimony as opinion evidence in the first place. She can report that the machine said X. She cannot explain why the machine said X, or how confident a factfinder should be that X is correct.

It is worth pausing to distinguish why she cannot, because “cannot explain” is not a single problem, and the distinctions matter for what, if anything, can be done about it. Jenna Burrell's influential taxonomy of algorithmic opacity distinguishes three analytically separate sources: opacity as intentional corporate or state secrecy; opacity as technical illiteracy on the part of the person interpreting or applying the system; and an opacity intrinsic to the character of machine-learning models themselves, which resist full human interpretation regardless of anyone's willingness to explain them.<sup>23</sup>

All three are present, in different measures, in the archetype this article describes. The vendor's refusal to disclose its matching architecture on trade-secret grounds is Burrell's first form, the problem Part V examines through *State v Loomis* and Rebecca Wexler's critique of it. The operator-witness's own inability to explain what she was never taught is Burrell's second form, the specific gap this Part has just identified against *Ramesh Chandra Agrawal*'s second precondition. The third form is the deepest, and the one Indian doctrine is least equipped to address, because it survives even complete good faith: a modern deep-learning facial-matching model distributes its decision logic across millions of weighted parameters learned from training data, in a form that resists reduction to the kind of criteria demanded in *Jai Lal*, criteria that even the model's own designers may be unable to articulate.

Disclosure cures the first form of opacity and training cures the second, but the third form has no comparable cure; there may simply be no discrete “scientific criteria for testing the accuracy of the conclusions” of the kind traditional expert evidence

---

<sup>23</sup>Jenna Burrell, 'How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) Big Data & Society 1, 1-2.

assumes every reliable opinion must rest on. This distinguishes the algorithmic case sharply from older forms of instrumental or documentary evidence; a chemical assay or a fingerprint comparison rests on a method that is, at least in principle, fully specifiable and auditable even if the particular witness cannot specify it; a deep neural network's matching logic may not be specifiable by anyone, at any level of access, in the form section 39 doctrine has always assumed an opinion must be defensible in.

Three doctrinal boxes present themselves as homes for this testimony, and none fits cleanly. The first is section 39 opinion evidence itself, considered above and found wanting: the witness holds no opinion in the *Jai Lal/Ramesh Chandra Agrawal* sense, because she cannot defend the reasoning behind the output she reports. The second is documentary or real evidence, treating the system-generated match report as analogous to a photograph, admissible through section 330 BNSS's "no formal proof" mechanism as a plain record of what a device produced. This, too, understates what the report actually is.

A photograph is a comparatively raw perceptual record; a facial-recognition match is already an inferential judgment, an identity claim, generated by a process that weighs, ranks and selects among candidates according to criteria no one on the record has disclosed. Treating that inferential output as a bare "document" for section 330 purposes smuggles an undefended opinion into evidence under cover of a category built for records that need no defending.

The third candidate is closer to the mark but has no settled place in Indian doctrine: the possibility that the machine itself performs an act functionally equivalent to assertion, and that the human witness is merely its conduit rather than its source. American scholarship on this problem, associated most closely with Andrea Roth's work on "machine testimony", argues that legal systems built around a hearsay/opinion architecture designed for human declarants have no settled doctrinal home for an assertion whose real source is a machine's programming,

whether the product of human coding or of machine learning, rather than the testifying witness's own knowledge.<sup>24</sup>

Indian evidence law has, if anything, less of a doctrinal home for this problem than the Federal Rules of Evidence that Roth is writing against: section 39(2) BSA's Examiner of Electronic Evidence route addresses the authenticity of stored data, and section 63 BSA's certification regime (discussed in Part VIII) addresses the integrity of a record, but neither engages the reliability of an inference the machine itself draws from authenticated data.

The result of trying all three boxes is not that algorithmic opinion evidence is inadmissible as a matter of principle, nothing in this article suggests that Indian courts should categorically exclude facial-recognition or risk-assessment evidence, but that Indian courts currently admit it, when they admit it, by defaulting into whichever box counsel happens to invoke, without a doctrine calibrated to what the evidence actually is, or to which of Burrell's three forms of opacity is operating in a given case. That is the gap this article's title names: an opinion is offered to the court, but no witness who appears before the court holds it in the sense section 39, as construed in *Jai Lal* and *Ramesh Chandra Agrawal*, requires.

## VII. COMPARATIVE ANCHOR I: RELIABILITY AND CONFRONTATION IN THE UNITED STATES

American law offers no ready-made transplant for this problem, but it offers two independent doctrinal traditions that each grapple with a piece of it, and whose limitations are as instructive as their achievements. The first is the reliability-gatekeeping tradition running from *Frye v United States*<sup>25</sup> through *Daubert v Merrell Dow Pharmaceuticals Inc*<sup>26</sup> to *Kumho Tire Co v Carmichael*<sup>27</sup>. *Frye* asked only whether a technique had gained “general acceptance” in the relevant scientific community, a

---

<sup>24</sup>Andrea Roth, 'Machine Testimony' (2017) 126 Yale LJ 1972, 1976–77, 2001–22.

<sup>25</sup>293 F 1013 (DC Cir 1923).

<sup>26</sup>509 US 579 (1993).

<sup>27</sup>526 US 137 (1999).

majoritarian proxy for reliability that *Daubert* displaced, for the federal courts, with a judge-administered gatekeeping inquiry under Federal Rule of Evidence 702.

*Daubert* identified a non-exhaustive set of factors relevant to that inquiry: whether the theory or technique can be and has been tested; whether it has been subjected to peer review and publication; its known or potential rate of error, and the existence of standards controlling its operation; and its degree of acceptance within the relevant scientific community.<sup>28</sup> The error-rate factor is the one most directly relevant here: it is precisely the figure that an operator-witness of the kind described in Part IV is typically unable to supply for the tool's performance under conditions resembling the case at trial.

*Kumho Tire* then extended the gatekeeping obligation beyond strictly “scientific” testimony to testimony resting on “technical, or other specialized knowledge”, holding that the nature of the gatekeeping inquiry, not the label attached to the witness, determines whether *Daubert* applies.<sup>29</sup> An algorithmic-tool operator's know-how is exactly the kind of technical-but-not-classically-scientific expertise *Kumho* contemplated; under the American framework, her testimony would not escape gatekeeping merely because no one calls her a scientist.

India has no codified equivalent of this gatekeeping stage. Section 39 BSA contains no pre-trial reliability hearing, no requirement that error rates or validation methodology be disclosed before an expert's opinion is led, and no statutory proxy for peer review or general acceptance. *Ramesh Chandra Agrawal*'s three preconditions are India's closest functional analogue, but they operate through the ordinary appreciation of evidence at or after trial rather than as a threshold admissibility filter, and, as Part III showed, they are most likely to be tested only where a party disputes the report, which section 330 BNSS makes structurally less likely for exactly the evidence that most needs testing. India's gap, in other words, is not merely that it lacks *Daubert*; it is that it lacks even the weaker, case-by-case version of the inquiry that *Ramesh Chandra Agrawal*

---

<sup>28</sup>*Daubert* (n 23) 592–94.

<sup>29</sup>*Kumho Tire* (n 24) 141, 147–50.

already supplies, because the procedural gateway of section 330 discourages the report from ever being tested at all.

The second American tradition is the Sixth Amendment confrontation-clause line running from *Crawford v Washington*<sup>30</sup> through *Melendez-Diaz v Massachusetts*<sup>31</sup> to *Bullcoming v New Mexico*<sup>32</sup>. *Crawford* held that testimonial hearsay is inadmissible against a criminal defendant unless the declarant is unavailable and the defendant had a prior opportunity to cross-examine. *Melendez-Diaz* applied that rule to forensic laboratory certificates, holding that a report prepared to serve as evidence at trial is testimonial and cannot be introduced through a live witness's bare recitation of its contents; the accused is entitled to confront the analyst who actually made the certification.<sup>33</sup>

*Bullcoming* then confronted directly the argument most relevant to this article: New Mexico had sought to introduce a blood-alcohol report through a “surrogate” analyst, qualified with respect to the general operation of the testing machine and the laboratory's procedures, but not personally involved in performing or observing the specific test, on the theory that the certifying analyst who signed the report was a “mere scrivener” transcribing the machine's output.

The Supreme Court rejected the argument, holding that the surrogate's general familiarity with the machine could not substitute for the personal knowledge of the analyst who actually conducted the test, because surrogate testimony of that order does not permit meaningful cross-examination about what the analyst actually did and observed.<sup>34</sup>

*Bullcoming*'s ‘scrivener’ is the closest doctrinal cousin the American reports offer to the technician described in Part IV of this article. In both cases a single, identifiable human being appears in the courtroom or on the record; in both cases the knowledge

---

<sup>30</sup>541 US 36 (2004).

<sup>31</sup>557 US 305 (2009).

<sup>32</sup>564 US 647 (2011).

<sup>33</sup>*Melendez-Diaz* (n 28).

<sup>34</sup>*Bullcoming* (n 29), Syllabus and majority opinion.

that would actually explain the report's reliability belongs to someone, or something, else entirely. The American solution, excluding the surrogate's testimony and requiring the analyst with genuine personal knowledge, works for *Bullcoming* because that knowledge, though absent from the courtroom, exists intact in one identifiable analyst who could in principle be produced.

For the facial-recognition or predictive-risk operator, no equivalent person exists to be produced: on Burrell's taxonomy, the knowledge that would explain the algorithm's output is dispersed across a private vendor's engineering team, its training pipeline, and, for the third, intrinsic form of opacity, potentially across no single mind at all.<sup>35</sup> *Bullcoming* solves a location problem, so one must find the right witness. The algorithmic case is, at least in its third and deepest form, a non-existence problem, in that there may be no witness, located or not, who holds the knowledge section 39 and *Ramesh Chandra Agrawal* require.

The Wisconsin Supreme Court's decision in *State v Loomis*<sup>36</sup> is the clearest illustration of how easily even this developed apparatus can be worked around where Burrell's first, intentional form of opacity is in play. Eric Loomis was sentenced partly on the strength of a COMPAS risk-assessment score; the tool's developer, Northpointe, treated its scoring methodology as a trade secret and refused to disclose how the risk factors were weighted.<sup>37</sup>

Loomis argued that this opacity denied him due process by preventing any meaningful challenge to the tool's scientific validity. The Wisconsin Supreme Court disagreed, holding that consideration of a COMPAS score at sentencing does not violate due process provided the sentencing court is given, and observes, certain

---

<sup>35</sup>cf Rebecca Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 Stan L Rev 1343, 1346–47, describing how commercial vendors of criminal-justice software resist disclosure of the source of an algorithm's output even where that output is central to the prosecution's case.

<sup>36</sup>2016 WI 68, 881 NW 2d 749 (Wis 2016).

<sup>37</sup>Loomis (n 33) paras 6–8, 51–52.

“limitations and cautions” about the tool's contested accuracy and its use of group-based statistics.<sup>38</sup>

The court declined to compel disclosure of the underlying algorithm. As Wexler has argued in a wider critique of trade-secret assertions in criminal proceedings, a rule that treats commercial secrecy as a reason to relax rather than heighten scrutiny is largely ahistorical, disproportionately burdens defendants, and is not required even by the internal logic of trade-secret law itself, which has long accommodated protective orders and in-camera disclosure precisely to avoid this kind of binary choice between full publication and total opacity.<sup>39</sup>

*Loomis* demonstrates something important for the Indian context that the comparative material in Parts VI and VII will sharpen further: it is not enough for a jurisdiction to possess a reliability-gatekeeping doctrine and a confrontation right if courts are willing, as the Wisconsin Supreme Court was, to treat proprietary opacity as a matter going to the weight a factfinder gives the evidence rather than to its admissibility, or to the threshold question of whether a genuine gatekeeping hearing must occur at all.

## VIII. COMPARATIVE ANCHOR II: ENGLAND AND WALES, FROM ‘MECHANICAL RELIABILITY’ TO THE POST OFFICE HORIZON SCANDAL

If the American material shows two doctrines straining, imperfectly, against algorithmic opacity, English law offers something rarer and more sobering: a fully litigated, publicly inquired-into demonstration of what happens when a legal system resolves the opacity question the other way, by presuming, rather than requiring proof, that a machine's output is reliable. The starting point is *Castle v Cross*<sup>40</sup>, where the Divisional Court held that first-hand evidence of what a mechanical measuring device displays or prints out is “real evidence” admissible at common law, and that,

---

<sup>38</sup>*ibid* para 8.

<sup>39</sup>Wexler (n 32) 1346, 1396–1429.

<sup>40</sup>[1984] 1 WLR 1372 (DC).

in the absence of evidence to the contrary, “the courts will presume that [mechanical instruments] were in order at the material time.”<sup>41</sup>

The House of Lords extended that reasoning directly to a computer-based breath-alcohol analyser in *Director of Public Prosecutions v McKeown and Jones*<sup>42</sup>, holding that a police officer's evidence of what an Intoximeter's visual display and printout showed was itself admissible real evidence, without any witness needing to explain the device's internal computation at all.

For a short period, Parliament had pointed the presumption the other way. Section 69 of the Police and Criminal Evidence Act 1984 provided that a statement in a document produced by a computer was not admissible unless it was shown, among other things, that the computer was operating properly throughout the relevant period, placing the burden of proving reliability on the party seeking to rely on the computer's output.

In 1997, however, the Law Commission recommended the repeal of section 69 without replacement, reasoning that computer error was rare enough, and difficult enough for the prosecution to prove, that requiring proof of proper functioning served no useful purpose.<sup>43</sup> Parliament accepted the recommendation in the Youth Justice and Criminal Evidence Act 1999, and the effect, on repeal, was that the older common-law presumption from *Castle v Cross* and *McKeown* simply reasserted itself for computer-generated evidence: absent evidence to the contrary, an English court would now presume that a computer had operated correctly, and it fell to the defendant, typically without access to the system that produced the evidence against him, to prove otherwise.

The consequences of that presumption are now a matter of public record. From 1999, Post Office Limited prosecuted several hundred sub-postmasters, sub-postmistresses and counter staff for theft, fraud and false accounting, relying on branch-account

---

<sup>41</sup>Castle (n 37), as summarised in *Director of Public Prosecutions v McKeown and Jones* [1997] UKHL 4, [1997] 1 WLR 295, 302 (Lord Hoffmann).

<sup>42</sup>[1997] UKHL 4, [1997] 1 WLR 295.

<sup>43</sup>Law Commission, Evidence in Criminal Proceedings: Hearsay and Related Topics (Law Com No 245, 1997) Part XIII.

shortfalls generated by its Horizon computerised accounting system. In *Bates v Post Office Ltd (No 6: Horizon Issues)*<sup>44</sup>, Fraser J found, after extensive technical evidence, that Horizon contained bugs, errors and defects capable of causing precisely the kind of apparent shortfall on which the prosecutions had relied, and that it was therefore unsafe to treat Horizon data as inherently reliable.<sup>45</sup>

The Court of Appeal drew out the evidential consequence in *Hamilton v Post Office Ltd*<sup>46</sup>, quashing the convictions of thirty-nine of forty-two appellants as an abuse of process. Holroyde LJ found that by “constantly asserting” that Horizon was reliable and refusing to countenance any suggestion to the contrary, the Post Office had “effectively sought to reverse the burden of proof”: it treated an unexplained accounting shortfall as an incontrovertible loss and proceeded, in substance, as though it were for the accused to prove that no loss had occurred, which, denied disclosure of material capable of undermining Horizon's reliability, they were structurally unable to do.<sup>47</sup>

The lesson worth drawing out for present purposes is not simply that Horizon was buggy software poorly deployed; it is that the presumption of mechanical reliability, once combined with an institutional party controlling both the system and the disclosure process, was sufficient by itself to produce what is now widely described as the largest single series of wrongful convictions in English legal history, and it did so with a fully deterministic, rule-based accounting system, not a machine-learning model.

Every one of Horizon's outputs was, in principle, fully specifiable and auditable code; the defect was institutional and evidentiary, not intrinsic to the technology in Burrell's third sense. If a presumption of reliability applied to a deterministic system could inflict this much damage before anyone thought to test it, the case for withholding any comparable presumption from a genuinely opaque, non-deterministic facial-

---

<sup>44</sup>[2019] EWHC 3408 (QB).

<sup>45</sup>Bates (n 41) para 968.

<sup>46</sup>[2021] EWCA Crim 577.

<sup>47</sup>Hamilton (n 43) para 137.

recognition or predictive-risk model, where even good-faith disclosure may not yield a testable explanation, is considerably stronger.

The United Kingdom government has, since the Post Office scandal, opened a formal call for evidence on whether the presumption that computers are reliable should be reformed or abolished.<sup>48</sup> India, which has not yet had its own Horizon-scale scandal, has the comparatively rare opportunity to draw the lesson before rather than after the fact: nothing in section 39 BSA or section 330 BNSS presently forecloses an Indian court from drifting, case by case, toward the same presumption of reliability the English common law applied for two decades, and the structural incentives, institutional prosecutorial control of the system, an efficiency-minded shortcut provision in section 330, and no codified reliability gate, are already in place.

It is worth closing this Part with a contrast rather than only a warning, because English law also shows how the traditional opinion-evidence framework can be preserved, carefully, for a problem that superficially resembles this article's hypothetical but is not the same. In *R v Atkins*<sup>49</sup>, the Court of Appeal considered the permissible limits of “facial mapping” evidence, a qualified human expert's comparison of a suspect's features against CCTV footage.

The Court held that such an expert may properly express a conclusion on a qualitative “sliding scale”, from evidence lending “no support” to evidence lending “powerful support” to a match, provided the conclusion is not dressed up as a statistical probability the expert cannot actually justify, and provided the jury is directed clearly that the opinion reflects the expert's own trained, subjective judgment rather than a scientific certainty.<sup>50</sup>

*Atkins* works, on its own terms, precisely because it preserves an opinion-holder in the fullest sense: a human being who reached her own conclusion through trained

---

<sup>48</sup>'Government Considers Ending 'Computer Is Right' Rule Following Horizon Scandal' (Legal Cheek, January 2025) [www.legalcheek.com/2025/01/government-considers-ending-computer-is-right-rule-following-horizon-scandal/](https://www.legalcheek.com/2025/01/government-considers-ending-computer-is-right-rule-following-horizon-scandal/) accessed 8 September 2026.

<sup>49</sup>[2009] EWCA Crim 1876, [2010] 1 Cr App R 8.

<sup>50</sup>*Atkins* (n 46) paras 14–31; see also *R v Gardner* [2004] EWCA Crim 1639, affirming the general admissibility of expert facial-comparison evidence.

perception, who can be cross-examined about how she reached it, and whose evidence is expressly bounded by an acknowledgment of its own subjectivity. None of that architecture transfers to an automated matching system.

A facial-recognition algorithm does not offer a hedged, self-consciously subjective “sliding scale” opinion that a jury can be warned to treat with appropriate caution; it offers a number, dressed in the language of statistical confidence, precisely the kind of claim *Atkins*'s safeguards were designed to prevent a merely human expert from making without justification. Transplanting *Atkins*'s tolerance for a human expert's bounded, avowedly subjective opinion onto a machine's unbounded, avowedly statistical one would not extend the doctrine; it would invert its entire rationale.

## IX. COMPARATIVE ANCHOR III: THE EUROPEAN UNION'S EX-ANTE MODEL

Where American law addresses algorithmic opacity chiefly at the point of trial, and English law shows what happens when a legal system fails to address it at all, European Union law increasingly addresses it before a tool is ever deployed. Article 22(1) of the General Data Protection Regulation gives a data subject the right not to be subject to a decision “based solely on automated processing” that produces legal or similarly significant effects, and Article 15(1)(h) entitles a data subject, in such cases, to “meaningful information about the logic involved.”<sup>51</sup>

The Court of Justice of the European Union gave that entitlement real content in *OQ v Land Hessen (SCHUFA Holding)*<sup>52</sup>, holding that a credit-scoring probability value generated by a credit reference agency constitutes automated individual decision-making within the meaning of Article 22(1), even though the agency itself does not make the final lending decision, wherever a third party relies heavily on that value to decide whether to contract with the data subject.<sup>53</sup>

---

<sup>51</sup>Regulation (EU) 2016/679 (General Data Protection Regulation), arts 15(1)(h), 22(1).

<sup>52</sup>Case C-634/21, Judgment of the Court (First Chamber), 7 December 2023, EU:C:2023:957.

<sup>53</sup>SCHUFA (n 49) paras 44–52.

The Court's reasoning is the point of comparative interest here: it held that reading Article 22 narrowly would leave a “lacuna in legal protection”, because the party who actually makes the downstream decision, the lender, typically does not itself possess, and cannot itself supply, meaningful information about the scoring logic; only the party that built the score can.<sup>54</sup>

That reasoning maps with unusual precision onto this article's own hypothetical: the police officer who acts on a facial-recognition match, like the lender who acts on a SCHUFA score, does not possess and cannot supply the information that would make the underlying inference testable; only the system's designer does, and unless the law reaches back to that designer, the gap in protection the CJEU identified in a civil, data-protection context reproduces itself, with substantially higher stakes, in a criminal trial.

It is worth being precise about how far the comparison travels. *SCHUFA* is a data-protection access right, not a rule of criminal evidence; it entitles a data subject to information about an automated decision's logic, not to have that decision excluded, or even weighed differently, in subsequent litigation. Nor is the CJEU's answer obviously the only reasonable one: the Wisconsin Supreme Court, confronting a structurally near-identical opacity problem in *Loomis*, reached the opposite institutional response, tolerating Northpointe's refusal to disclose COMPAS's scoring logic and treating judicial “limitations and cautions” as an adequate substitute for genuine transparency.

Two mature courts, faced with comparable gaps between who acts on an algorithmic output and who understands it, have reached opposite conclusions about where the resulting risk should fall. That disagreement is itself instructive for India: it shows that this is a genuinely open institutional choice, not a settled question with one importable answer, and that the choice India makes, through Parliament, the courts, or both, will have to be defended on its own terms rather than assumed from precedent.

---

<sup>54</sup>*ibid* paras 68–73.

The European Union's more recent Artificial Intelligence Act goes further than GDPR's access-based model, regulating certain law-enforcement uses of algorithmic tools before deployment rather than leaving disclosure to be litigated case by case. Article 5(1)(h) of the Regulation prohibits the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law-enforcement purposes, subject only to narrowly defined and independently or judicially authorised exceptions, namely locating a specific missing or trafficked person, preventing a specific and imminent threat to life or a terrorist attack, or identifying a suspect in specified serious offences.<sup>55</sup>

Article 5(1)(d) separately prohibits the use of an AI system to assess or predict the risk of a person committing a criminal offence "solely" on the basis of profiling or personality-trait assessment, without objective, verifiable facts directly linked to criminal activity, a provision that speaks directly to the predictive-risk half of this article's hypothetical, and whose legislative history draws explicitly on earlier domestic litigation, including a Dutch court's 2020 invalidation of the government's own algorithmic welfare-fraud detection system, *System Risico Indicatie* ('SyRI'), for insufficient transparency about the risk indicators it relied on.<sup>56</sup>

Where a biometric identification or law-enforcement risk-assessment tool is not prohibited outright, it is generally classified "high-risk" under Annex III of the Regulation, which imposes, before the tool may lawfully be placed in service, obligations of risk management, data governance, technical documentation, record-keeping and logging, human oversight, and demonstrated accuracy and robustness.<sup>57</sup>

The structural lesson for India is not that it should transplant the Artificial Intelligence Act's specific prohibitions; that is a legislative and constitutional choice for Parliament, not a doctrinal conclusion this article can draw from evidence law alone. It is that the

---

<sup>55</sup>Regulation (EU) 2024/1689 (Artificial Intelligence Act), art 5(1)(h).

<sup>56</sup>Regulation (EU) 2024/1689, art 5(1)(d); *NJCM v The State of the Netherlands (SyRI)* (The Hague District Court, 5 February 2020) ECLI:NL:RBDHA:2020:1878, holding the SyRI legislation incompatible with art 8 of the European Convention on Human Rights principally for lack of transparency and insufficient safeguards for judicial scrutiny.

<sup>57</sup>Regulation (EU) 2024/1689, arts 8–15 and Annex III, point 6.

European model relocates the opinion-holder problem this article has traced through Indian, American and English doctrine to an earlier point in time.

Rather than waiting for a trial court to discover, case by case, that no witness before it can supply *Jai Lal's* “necessary scientific criteria for testing the accuracy of the conclusions”, the European approach requires that documentation to exist, logged, retained, and available for scrutiny, before the tool is ever used to generate evidence at all. That is the ex-ante mirror of the ex-post problem this article has been describing, and it is the model Part IX draws on most directly in proposing a doctrinal fix for Indian law.

## X. THE INDIAN STATUTORY AND CONSTITUTIONAL OVERLAY

Indian law is not without a template for treating machine-sourced material differently from ordinary opinion or documentary evidence; it has simply not yet extended that template to inferential outputs. Section 63 BSA, the successor to section 65B of the repealed Indian Evidence Act 1872, governs the admissibility of electronic records and was held mandatory, not merely directory, by the Supreme Court in *Anvar P.V. v P.K. Basheer*<sup>58</sup> and reaffirmed, after a period of conflicting authority, by a three-judge bench in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*.<sup>59</sup>

Section 63 goes further than its predecessor: where section 65B(4) of the 1872 Act required only a single certificate from a person occupying “a responsible official position in relation to the operation of the relevant device”, section 63(4) BSA requires a two-part certificate in a prescribed schedule format, including a hash value of the record, and contemplates certification by both the person in charge of the device and, where applicable, an independent expert.<sup>60</sup>

---

<sup>58</sup>(2014) 10 SCC 473, holding that secondary electronic evidence 'shall not be admitted in evidence unless the requirements under Section 65B are satisfied', and overruling the contrary position in *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.

<sup>59</sup>(2020) 7 SCC 1, overruling *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801 and reaffirming *Anvar P.V.* (n 55) on the mandatory nature of the certificate requirement.

<sup>60</sup>Bharatiya Sakshya Adhiniyam 2023, s 63(4) and Schedule.

Parliament has thus already shown itself willing, in the specific context of machine-sourced material, to depart from the ordinary opinion/documentary dichotomy and to legislate a bespoke authentication regime calibrated to the particular risks that electronic records present, in substance, a modest, domestic precursor to the ex-ante disclosure model examined comparatively in Part VII. The Supreme Court has since upheld section 63(4)'s validity against a manifest-arbitrariness challenge, while declining to settle who, exactly, must sign as the provision's certifying expert, leaving open precisely the question this article presses in the reliability context.

Section 63's dual-certification model is a template, not a ready-made solution, and the distinction matters. What it authenticates is that a record is what it purports to be, that the data has not been altered, that the chain of custody is documented, that the hash value matches. What it does not do, and was never designed to do, is authenticate that an *inference* drawn from that data, a facial match, a risk score, is itself reliable. That is a different question in kind, closer to the reliability inquiry *Daubert* and *Ramesh Chandra Agrawal* pose than to the authenticity inquiry section 63 answers.

The structural lesson worth drawing from section 63, however, is precisely that a dual-signatory model, a certificate from the operator responsible for running the system, matched with a certificate from an independent person genuinely competent on the science, is not a foreign transplant for Indian evidence law. It is a device Parliament has already built for a related problem, and it can be adapted, in substance rather than mere form, to the reliability problem this article identifies, without needing to look further than India's own statute book for the structural precedent.

The constitutional overlay supplied by *Justice K.S. Puttaswamy (Retd) v Union of India*<sup>61</sup> reinforces the same point from a different direction. *Puttaswamy*'s three-part test, that a state intrusion on privacy be backed by law, pursue a legitimate aim, and be proportionate, was developed to police the *collection* of biometric and other personal data, and it is that framework the pending *Rahim* petition invokes against the Delhi Police's deployment of facial-recognition and biometric tools at protest sites, alleging

---

<sup>61</sup>Puttaswamy (n 4).

the absence of statutory backing and of any privacy-impact assessment for the technology in question.<sup>62</sup>

The point worth drawing out, without pre-judging a matter that remains sub judice, is structural rather than substantive, and it is sharpened by the comparative material in Parts VI and VII: the same institutional failure that makes a surveillance deployment constitutionally suspect at the collection stage, the absence of a documented legal basis, a proportionality assessment, or a validation record, of the kind the European Union's Artificial Intelligence Act now requires before deployment, is very likely to reappear downstream, at the evidentiary stage, as the absence of a witness who can satisfy *Ramesh Chandra Agrawal*'s second precondition, in exactly the way the absence of any comparable requirement allowed Horizon's presumed reliability to go untested in England for two decades.

A tool procured and deployed without any requirement to document its error rates or validation methodology cannot, later, generate a witness competent to disclose what was never created or preserved in the first place. Constitutional opacity at intake, evidentiary opacity at trial, and the absence of ex-ante documentation are three expressions of one underlying failure.

Finally, the fair-trial dimension of the problem is not merely borrowed from a foreign constitutional text India does not share. Article 21 of the Constitution guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law, and it is settled, since *Maneka Gandhi v Union of India*<sup>63</sup>, that such procedure must itself be just, fair and reasonable. The requirement that expert testimony be tested, that a court not simply accept a conclusion but be furnished with reasoning it can independently interrogate, is precisely how *Jai Lal* and *Ramesh Chandra Agrawal* give content to a fair procedure in the specific context of expert evidence.

---

<sup>62</sup>Indian MP Asks the Supreme Court to Halt Police Facial Recognition at Protests' (n 3).

<sup>63</sup>(1978) 1 SCC 248.

Section 330 BNSS's structural discouragement of contesting opaque reports, for the reasons given in Part III, puts pressure on that same guarantee, even though Indian constitutional doctrine locates it in Article 21's due-process reading rather than in a free-standing confrontation clause of the kind the Sixth Amendment supplies, or in the access-based logic that grounds Article 22 GDPR.

## **XI. TOWARD A DOCTRINAL FIX**

None of what precedes suggests that algorithmic tools should be excluded from Indian courtrooms, or that facial-recognition and predictive-risk evidence is inherently untrustworthy. The argument is narrower and, for that reason, more tractable: Indian evidentiary doctrine has not yet built a category calibrated to what this evidence actually is, and until it does, courts will keep sorting it into section 39's opinion-evidence box by habit rather than by reasoned fit. Five modest, achievable steps, drawing respectively on India's own section 63 precedent and on the comparative lessons of Parts V to VII, would close much of the gap identified above.

First, a front-end reliability certificate for algorithmic opinion tools, modelled structurally on section 63(4) BSA's dual-signatory format but different in substance, and informed by the European Union's Annex III documentation model examined in Part VII. Where section 63(4) certifies that a record is authentic, the proposed certificate would require a person with genuine technical, not merely operational, competence to certify the tool's documented error rates, its validation methodology, and the conditions under which it was tested, before its output is tendered as opinion evidence.

This extends section 39's "specially skilled" requirement to the tool as well as to the human interface: a witness cannot be "specially skilled" in a process she has never been shown the workings of, and a certificate of this kind forces the disclosure that *Ramesh Chandra Agrawal's* second precondition already demands but which section 330's shortcut currently lets go untested.

Second, a purposive reading of section 39(1) itself. Consistent with *Jai Lal* and *Ramesh Chandra Agrawal*, courts should treat "specially skilled" as requiring that the witness before the court possess the special skill relevant to the specific opinion offered, not

merely the skill required to operate an interface, the same discipline that *R v Atkins* enforces for human facial-mapping experts in England, and that this article has argued cannot simply be waived because the witness in question operates a machine rather than her own trained eye.

Operating software competently is not the special skill section 39 contemplates; understanding, and being able to defend, why the software's output should be believed is. Trial courts should test operator-witnesses against the reliable-principles precondition as a matter of course when algorithmic opinion evidence is tendered, rather than only when defence counsel happens to press the point, a discipline that matters most exactly where, as Part III showed, the defence is least equipped to press it.

Third, undisclosed or proprietary methodology should, as a matter of law, be treated as rendering a report “disputed” for the purposes of section 330 BNSS's second proviso. The shortcut should not be available where the party against whom the report is used could not, on the report's face, have meaningfully evaluated it in order to decide whether to dispute it. This reverses the default identified in Part III: opacity itself, rather than only an affirmative objection, would trigger the requirement to call the expert.

It should be said plainly that this reform only partially cures the underlying defect, given the scrivener problem examined through *Bullcoming* in Part V, calling the operator-witness does not by itself supply an opinion-holder if no such person exists to be called. But it at least ensures that the question is put to the test in open court, rather than resolved by the shortcut's silent default, and it forecloses the specific mechanism, an institutional party's unchallenged assertion of reliability, that Part VI showed converting an evidentiary presumption into a systemic miscarriage of justice in England.

Fourth, and expanding on the second condition to a point the comparative material makes newly urgent, this is a matter for coordinated executive and legislative attention, not only judicial interpretation, and it should operate before deployment as well as at trial. As the technology is procured and deployed by the Ministry of Home

Affairs, the National Crime Records Bureau, and state police forces, conditions of empanelment or approval for evidentiary use should require independent third-party validation studies, documented and deployment-specific error rates, and, following the European Union's Annex III model rather than waiting for a case to expose the gap, as *Bates* and *Hamilton* eventually did in England, mandatory logging and record-keeping obligations built into the tool's design and procurement contract, with results made available to the defence in a form sufficient to support meaningful cross-examination.

Genuine trade-secret interests in source code can be protected through the kind of protective-order and in-camera mechanisms Wexler has argued trade-secret law itself already accommodates, following the direction the Court of Justice took in *SCHUFA* rather than the deference the Wisconsin Supreme Court extended to Northpointe's blanket refusal in *Loomis*.<sup>64</sup> The 23rd Law Commission of India, chaired by Justice Dinesh Maheshwari, or Parliament directly, would be well placed to give this recommendation statutory form, whether through a dedicated amendment to section 39 BSA or through delegated rule-making tied to the procurement standards the National Crime Records Bureau already sets for tools such as the Automated Facial Recognition System.<sup>65</sup>

Fifth, and perhaps most importantly given the comparative material canvassed above, Indian courts and legislators should resist ever allowing section 330's efficiency logic to harden, case by case, into anything resembling the English common-law presumption that a machine's output is reliable unless the defence proves otherwise. *Castle v Cross* and *McKeown* were not reckless decisions; each addressed a narrow, comparatively well-understood device, a speedometer, a breath analyser, and neither court could reasonably have foreseen that the same reasoning would, two decades

---

<sup>64</sup>Wexler (n 32) 1396–1429.

<sup>65</sup>'Dinesh Maheshwari' in *Wikipedia, The Free Encyclopedia* [https://en.wikipedia.org/wiki/Dinesh\\_Maheshwari](https://en.wikipedia.org/wiki/Dinesh_Maheshwari) accessed 8 September 2026, recording his appointment as Chairperson, 23rd Law Commission of India, with effect from 15 April 2025. On the Automated Facial Recognition System's procurement history, see Panoptic (n 19).

later, help sustain the wrongful prosecution of hundreds of sub-postmasters on the strength of an accounting system's unexamined output.

India's advantage is that it can see the endpoint of that reasoning before adopting its starting premise. Section 63 BSA's dual-certification model is, if maintained and if extended in substance, not merely in form, from authenticity to reliability, a structural safeguard against ever needing to ask, a decade from now, how an Indian court came to presume that a facial-recognition algorithm's output was correct simply because no one had yet proved it wrong.

## XII. CONCLUSION

Robert Williams's arrest, the Post Office's prosecution of hundreds of its own sub-postmasters, and the petition pending before the Supreme Court of India in *AA Rahim MP v Union of India* are separated by continents, legal systems, and, in Horizon's case, decades, but they describe the same structural failure approached from different directions. In Detroit, a technology deployed without adequate validation produced a wrongful arrest that never had to survive cross-examination, because the case collapsed before trial.

In England, a presumption that machines are reliable, applied for two decades to a deterministic accounting system nobody thought to test, produced what is now recognised as the widest single miscarriage of justice in that jurisdiction's history. In New Delhi, a technology is being challenged before it has even generated the evidence a criminal trial would eventually have to test. Indian evidence law has, for the moment, the rare advantage of confronting this problem before rather than after it has produced its own Horizon.

The difficulty identified in this article is categorical before it is technological. Section 39 BSA and section 330 BNSS were written, and have been faithfully interpreted, for a world in which an "expert" is a person who studied a subject, formed a defensible view, and could be made to defend it under cross-examination. A police technician who runs a proprietary facial-recognition or predictive-risk tool without access to its internal logic is not that person, however genuinely she believes the result she reports, and however sincerely a trial court trusts her.

Section 39's own case law, *Jai Lal*, *Ramesh Chandra Agrawal*, *Murari Lal*, already contains the resources to say so, if courts are prepared to ask the question directly rather than accept the label “expert” at face value. Section 330's cross-examination shortcut, meanwhile, was built for a world in which non-disputation reflects informed choice, not structural inability to evaluate what is being waived. The comparative record, American doctrine straining against opacity it cannot fully dissolve, English law's documented collapse into an unearned presumption of reliability, and the European Union's still-unsettled experiment with regulating the problem before it reaches a courtroom at all, shows that no mature system has solved this cleanly, and that the choice India makes cannot simply be borrowed.

Until Indian evidence law names the category this article has tried to describe, opinion evidence without an opinion-holder, courts will keep sorting algorithmic testimony into section 39's box by habit, and section 330 will keep waiving cross-examination for exactly the reports that most need it. The reform this article proposes does not ask judges to become computer scientists. It asks the law to stop assuming that behind every opinion offered to a court, someone actually stands ready to defend it.

### **XIII. BIBLIOGRAPHY**

#### **A. Statutes and Legislative Instruments**

1. Bharatiya Sakshya Adhiniyam 2023.
2. Bharatiya Nagarik Suraksha Sanhita 2023.
3. Indian Evidence Act 1872.
4. Code of Criminal Procedure 1973.
5. Information Technology Act 2000.
6. Police and Criminal Evidence Act 1984.
7. Youth Justice and Criminal Evidence Act 1999.
8. Regulation (EU) 2016/679, General Data Protection Regulation.
9. Regulation (EU) 2024/1689, Artificial Intelligence Act.

## B. Cases

### 1. Indian Cases

- *Justice K.S. Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
- *State of Himachal Pradesh v Jai Lal* AIR 1999 SC 3318: (1999) 7 SCC 280.
- *Ramesh Chandra Agrawal v Regency Hospital Ltd* (2009) 9 SCC 709.
- *Murari Lal v State of Madhya Pradesh* AIR 1980 SC 531: (1980) 1 SCC 704.
- *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473.
- *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.
- *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
- *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.
- *Pune Bar Assn v Union of India* 2026 SCC OnLine SC 1297.
- *R v B* (2024) 1 HCC (Mad) 531.
- *Maneka Gandhi v Union of India* (1978) 1 SCC 248.
- *AA Rahim MP v Union of India*, Diary No 45049 of 2026, Supreme Court of India, pending.

### 2. American Cases

- *Frye v United States* 293 F 1013 (DC Cir 1923).
- *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US 579 (1993).
- *Kumho Tire Co v Carmichael* 526 US 137 (1999).
- *Crawford v Washington* 541 US 36 (2004).
- *Melendez-Diaz v Massachusetts* 557 US 305 (2009).
- *Bullcoming v New Mexico* 564 US 647 (2011).
- *State v Loomis* 2016 WI 68, 881 NW 2d 749 (Wis 2016).

### 3. English Cases

- *Castle v Cross* [1984] 1 WLR 1372 (DC).

- *Director of Public Prosecutions v McKeown and Jones* [1997] UKHL 4, [1997] 1 WLR 295.
- *Bates v Post Office Ltd (No 6: Horizon Issues)* [2019] EWHC 3408 (QB).
- *Hamilton v Post Office Ltd* [2021] EWCA Crim 577.
- *R v Atkins* [2009] EWCA Crim 1876, [2010] 1 Cr App R 8.
- *R v Gardner* [2004] EWCA Crim 1639.

#### 4. European Union and European Cases

- *OQ v Land Hessen (SCHUFA Holding)* Case C-634/21, Judgment of the Court, 7 December 2023, EU:C:2023:957.
- *NJCM v The State of the Netherlands (SyRI)* The Hague District Court, 5 February 2020, ECLI:NL:RBDHA:2020:1878.

#### C. Books, Articles, Reports, and Online Sources

1. Civil Rights Litigation Initiative, University of Michigan Law School and American Civil Liberties Union, 'Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on Facial Recognition Technology' (ACLU, 28 June 2024) [www.aclu.org/press-releases/civil-rights-advocates-achieve-nations-strongest-police-department-policy-facial](https://www.aclu.org/press-releases/civil-rights-advocates-achieve-nations-strongest-police-department-policy-facial) accessed 8 September 2026.
2. Reason, 'Faulty Facial Recognition Tech Got Him Arrested. Now He's Getting a \$300,000 Payout' (23 July 2024) <https://reason.com/2024/07/23/faulty-facial-recognition-tech-got-him-arrested-now-hes-getting-a-300000-payout/> accessed 8 September 2026.
3. 'Indian MP Asks the Supreme Court to Halt Police Facial Recognition at Protests' (IDTechWire, 28 July 2026) <https://idtechwire.com/indian-mp-asks-the-supreme-court-to-halt-police-facial-recognition-at-protests/> accessed 8 September 2026.
4. 'India's Supreme Court to Hear Challenge to Police Facial Recognition at Protests' (IDTechWire, 14 August 2026) <https://idtechwire.com/indias->

- [supreme-court-to-hear-challenge-to-police-facial-recognition-at-protests/](#) accessed 8 September 2026.
5. J.P. Associates, 'Bharatiya Sakshya Adhiniyam, 2023' (Mondaq, 2023) [www.mondaq.com/india/new-technology/1417594/bharatiya-sakshya-adhiniyam-2023](http://www.mondaq.com/india/new-technology/1417594/bharatiya-sakshya-adhiniyam-2023) accessed 8 September 2026.
  6. Panoptic, 'NCRB's National Automated Facial Recognition System' (Case Study) <https://panoptic.in/case-study/ncrbs-national-automated-facial-recognition-system> accessed 8 September 2026.
  7. Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) 3(1) *Big Data & Society* 1.
  8. Andrea Roth, 'Machine Testimony' (2017) 126 *Yale Law Journal* 1972.
  9. Alan Merry and Alexander McCall Smith, *Errors, Medicine and the Law* (Cambridge University Press 2001).
  10. Rebecca Wexler, 'Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System' (2018) 70 *Stanford Law Review* 1343.
  11. Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997).
  12. 'Government Considers Ending "Computer Is Right" Rule Following Horizon Scandal' (Legal Cheek, January 2025) [www.legalcheek.com/2025/01/government-considers-ending-computer-is-right-rule-following-horizon-scandal/](http://www.legalcheek.com/2025/01/government-considers-ending-computer-is-right-rule-following-horizon-scandal/) accessed 8 September 2026.
  13. 'Supreme Court Rejects Challenge To S.63(4) BSA Mandating Hash Value Disclosure For Electronic Evidence' (LiveLaw, 28 May 2026) accessed 10 September 2026.
  14. 'Dinesh Maheshwari' in *Wikipedia, The Free Encyclopedia* [https://en.wikipedia.org/wiki/Dinesh\\_Maheshwari](https://en.wikipedia.org/wiki/Dinesh_Maheshwari) accessed 8 September 2026.