ALGORITHMIC BIAS IN FORENSIC AI AND THE LEGAL STANDARDS FOR ADMISSIBILITY IN INDIA

Tanaya P Kamlakar [*]
Prerana Sanjay[**]

Abstract

The integration of Artificial Intelligence (*hereinafter*, "AI") in forensic practices particularly *facial recognition, predictive policing*, and *gait analysis* has begun to reshape the Indian criminal justice landscape. While these tools offer operational efficiency, they also pose significant risks of algorithmic bias and evidentiary unreliability. This paper critically evaluates the admissibility of AI–generated forensic evidence under the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023. It examines how caste, gender, religion, and socio-economic bias may become structurally encoded within algorithms, thereby violating constitutional protections under articles 14, 20(3), and 21. Drawing on jurisprudential developments from the United States, United Kingdom and European Union, the paper analyses global benchmarks on reliability, transparency and due process in AI– enabled evidence. It concludes by proposing detailed statutory and procedural reforms to ensure algorithmic accountability, evidentiary integrity, and judicial scrutiny, thereby aligning India's evidentiary framework with constitutional mandates and international best practices.

I Introduction

IN RECENT years, Indian law enforcement agencies have rapidly adopted AI – powered forensic technologies to aid criminal investigations. Tools such as facial recognition systems, predictive policing algorithms, and forensic gait analysis are being piloted or employed by police across various states.[1] These technologies bring undeniable potential benefits like expediting the identification of suspects through CCTV footage, forecasting crime hot-spots to allocate police resources, and matching surveillance images *via* biometric analysis. Policymakers tout such tools as means to modernize policing and improve the accuracy of criminal justice outcomes. Indeed, the Bharatiya Nagarik Suraksha Sanhita, 2023 (*hereinafter,* "BNSS") explicitly mandates greater use of forensic techniques in investigations, requiring forensic collection for serious offenses and even allowing trials to be conducted in electronic mode.[2] The

* Assistant Professor, Maharashtra National Law University Mumbai.

** Final Year Student, MNLU and Student Convener, Centre for Criminal Justice, MNLUM.

1 Press Information Bureau, "Integrating AI in India's Judiciary and Law Enforcement," (2025), *available at*: https://pib.gov.in/PressReleasePage.aspx?PRID=2106239 (last visited on Apr. 3, 2025); Snehil Singh, "Understanding The Gait Test And Its Impact On Criminal Trials" LiveLaw (Aug. 20, 2022), *available at*: https://www.livelaw.in/columns/gait-test-indian-evidence-act-section-45-gait-pattern-analysis-podiatry-knowledge-criminal-trials-202632 (last visited on Apr. 3, 2025).

2 The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ss. 176, 336–340.

Bharatiya Sakshya Adhiniyam, 2023 (*hereinafter,* "BSA") –similarly updates evidentiary rules to accommodate digital and expert evidence within a *"fair trial"* framework.[3]

However, alongside these promises of efficiency, a growing body of evidence reveals that AI–based forensic tools can replicate and even amplify societal biases.[4]Algorithmic bias – systematic error that unfairly prejudices outcomes against certain groups – has been documented in many AI systems. Facial Recognition Technology (*hereinafter,* "FRT"), for example, has shown significantly higher error rates for women and minority ethnic groups compared to others.[5] Predictive policing algorithms trained on historical crime data often reflect and reinforce pre-existing prejudices in policing, disproportionately flagging neighbourhoods or communities that have been historically over-policed, including marginalized caste and religious groups.[6] Even gait analysis, promoted as a cutting-edge identification method, is susceptible to subjectivity and inconsistency in the absence of standardized protocols.[7] These biases are not merely technical flaws. When deployed in criminal justice, they implicate fundamental rights to equality, non-discrimination, and fair trial.

This paper examines the use of AI-based forensic tools such as facial recognition, predictive policing, and gait analysis in the Indian criminal justice system. Part I explores their deployment and associated bias concerns. Part II analyses the admissibility of AI-generated evidence under the BSA and the BNSS, focusing on expert opinions, electronic records, and evidentiary reliability. Part III evaluates the constitutional implications, particularly under articles 14 and 21, in relation to opaque or

---

3 The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 45, 63, 65.

4 NITI Aayog, "National Strategy for Artificial Intelligence," (2018), pp. 41–43, *available at* : https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf(last visited on Mar. 3, 2025).

5 Buolamwini, J., and Gebru, T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," 81 *Proceedings of Machine Learning Research* at 1–15 (2018), *available at*: http://proceedings.mlr.press/v81/buolamwini18a.html (last visited on Apr. 3, 2025); Karishma Mehrotra, "Indian Faces Were Run Through Facial Recognition Tech Tools. Here's Why You Should Be Concerned" *Scroll.in*, July 26, 2021, *available at*: https://scroll.in/magazine/1001836/facial-recognition-technology-isnt-wholly-accurate-at-reading-indian-faces-find-researchers (last visited on Mar. 3, 2025).

6 Antara Vats, "Predictive Policing in India: A Constitutional Critique of Emerging Technologies in Criminal Justice" 38 International Review of Information Ethics (IRIE) 1 (2022), *available at*: https://informationethics.ca/index.php/irie/article/view/487 (last visited on Apr. 3, 2025); Ameya Bokil, *et.al.,* "Settled Habits, New Tricks: Casteist Policing Meets Big Tech in India" *TNI Longreads*, May 2021, *available at*: https://longreads.tni.org/stateofpower/settled-habits-new-tricks-casteist-policing-meets-big-tech-in-india (last visited on Apr. 3, 2025); Aryan, R., "Artificial Intelligence Driven Predictive Policing Tools: Reshaping Law Enforcement Practices," *White Black Legal,* (2025), *available at*: https://www.whiteblacklegal.co.in/details/artificial-intelligence-driven-predictive-policing-tools-reshaping-law-enforcement-practices-by—ritul-aryan (last visited on Mar. 3, 2025).

discriminatory algorithmic systems. Part IV offers comparative insights from the United States, United Kingdom, and European Union, highlighting reliability standards, disclosure norms, and equality safeguards. Part V proposes detailed reforms statutory, procedural, and institutional to ensure transparency, judicial scrutiny, and protection of fundamental rights in AI–driven investigations. The paper concludes that without robust legal safeguards, forensic AI may compromise fair trial guarantees, but with appropriate reforms, its benefits can be harnessed within constitutional boundaries.

II AI-based forensic tools in the Indian criminal justice system

Facial recognition technology in policing

FRT has seen wide deployment by Indian law enforcement in recent years. Police departments and security agencies use Automated Facial Recognition Systems (*hereinafter,* "AFRS") to compare photographs or CCTV images against databases of known individuals (*e.g.* photographic identification, driving license photos, or the growing national ID repositories) in order to identify suspects or find missing persons. The Union Ministry of Home Affairs has advocated for a centralized AFRS for crime detection, and several state police forces including those in Delhi, Telangana, Maharashtra, and Tamil Nadu have acquired facial recognition software for investigative use.[8] For instance, the Delhi Police deployed FRT to screen crowds during large-scale protests and to identify suspects from CCTV footage related to the 2020 Delhi riots and other incidents.[9] Similarly, the Indian Railways announced plans to implement FRT-based surveillance across hundreds of stations,[10] aiming to bolster security by automatically flagging individuals appearing on law enforcement watch lists.

---

7 Badiye, A., Kapoor, N., Kathane, P., and Krishan, K., "Forensic Gait Analysis," *StatPearls* (2020), *available at*: https://www.ncbi.nlm.nih.gov/books/NBK557684/ (last visited Mar. 3, 2025).

8 Internet Freedom Foundation, "Hyderabad Police force people to remove their masks before photographing them. We sent a legal notice. #Save Our Privacy", Internet Freedom Foundation, May 2021, *available at*: https://internetfreedom.in/hyderabad-police-force-people-to-remove-their-masks-before-photographing-them-we-sent-a-legal-notice-saveourprivacy/ (last visited on Apr. 3, 2025); Ameen Jauhar, "Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges" Vidhi Centre for Legal Policy, Aug. 10, 2021, *available at*: https://vidhilegalpolicy.in/research/indian-law-enforcements-ongoing-usage-of-automated-facial-recognition-technology-ethical-risks-and-legal-challenges/ (last visited on Mar. 3, 2025).

9 Internet Freedom Foundation, *supra* note 8.

10 Internet Freedom Foundation, "We will not be tracked! Indian Railways' plans to introduce FRT surveillance in train coaches is a big departure from the right to privacy" *Internet Freedom Foundation*, 2021, *available at*: https://internetfreedom.in/indian-railways-frt-surveillance/(last visited on Mar. 3, 2025).

Documented uses and efficacy

While authorities portray FRT as a powerful crime-fighting tool, empirical evidence about its accuracy in India is alarming. In 2018, the High Court of Delhi was informed that the facial recognition software (*hereinafter,* "FRS") used by Delhi Police had an accuracy rate of only 2% – essentially, 98% of matches were false positives.[11] The high court, perturbed by this finding, directed the police to upgrade the FRS.[12] Similarly, independent audits have underscored the unreliability of prevailing FRT systems on Indian populations. A 2021 study tested leading commercial facial recognition tools on Indian faces; *"the results were stark"* – the algorithms failed far more often for certain demographics, especially by gender.[13] On average, the software misidentified the gender of Indian women 14 times more frequently than that of Indian men (7% error rate for women versus 0.5% for men).[14] Such disparities echo earlier international studies that found facial recognition performance dropping precipitously for darker-skinned female faces.[15] In effect, the technology tends to be most accurate on lighter-skinned male faces: a demographic bias that is particularly concerning in India's diverse society.

The implications of these accuracy issues are profound. False negatives may allow dangerous suspects slip through, but false positives are even more troubling from a rights perspective, they mean innocent people (disproportionately from certain groups) risk misidentification as crime suspects. Notably, in the United States at least three Black men have been wrongfully arrested based on faulty facial recognition matches.[16]

---

11 Soumyarendra Barik, "Delhi Police in RTI Reply: 80% Match in Facial Recognition is Deemed Positive ID," *The Indian Express*, July 28, 2022, *available at*: https://indianexpress.com/article/cities/delhi/delhi-police-rti-reply-80-pc-match-facial-recognition-deemed-positive-id-8094324/ (last visited Mar. 3, 2025).

12 Press Trust of India, "Delhi police facial recognition software has only 2 per cent accuracy: HC told" *Business Standard*, Aug. 23, 2018, *available at*: https://www.business-standard.com/article/pti-stories/delhi-police-facial-recognition-software-has-only-2-per-cent-accuracy-hc-told-118082301289_1.html (last visited on Mar. 03, 2025); Press Trust of India, "Upgrade face recognition software: Delhi high court" *The Times of India*, Aug. 4, 2019, *available at:* https://timesofindia.indiatimes.com/city/delhi/upgrade-face-recognition-software-delhi-high-court/articleshow/70813797.cms (last visited on Mar. 3, 2025).

13 Karishma Mehrotra, *supra* note 5.

14 Smriti Parsheera and Gaurav Jain, "Cinderella's Shoe Won't Fit Soundarya: An Audit of Facial Processing Tools on Indian Faces," *available at*: https://doi.org/10.48550/arXiv.2112.09326, Dec. 17, 2021 (last visited Mar. 3, 2025).

15 Joy Buolamwini and Timnit Gebru, *supra* note 4.

16 Shawn Mulcahy, "Artificial intelligence is reshaping how police investigate crime" *The Washington Post*, Apr. 11, 2025, *available at*: https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/(last visited on Apr. 3, 2025); American Civil Liberties Union, "Williams v. City of Detroit," *available at:* https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest (last visited on Mar. 3, 2025).

While such cases have not yet come to light in India, the stark 2% accuracy revelation suggests that without caution, misidentifications are inevitable. Indeed, the use of Delhi's FRT system to identify participants in protests against the Citizenship Amendment Act raised concerns that it could erroneously target individuals from minority communities, given known biases and the context of communal profiling.[17]

Bias concerns

Algorithmic bias in facial recognition can stem from skewed training data (e.g. underrepresentation of certain skin tones or facial attributes) and from inherent prejudices in how the technology is applied (e.g. surveillance of specific neighbourhoods or groups). Studies in the United States and United Kingdom have repeatedly found that many FRT algorithms exhibit higher false match rates for people of colour and women.[18] In India, this translates into potential discrimination along lines of caste and religion as well, since those often correlate with distinct regional or ethnic appearance. For example, a system trained mostly on light-skinned North Indian male faces might perform poorly on dark-complexioned South Indian female faces – a disparity that can map onto historically marginalized communities. Civil society has raised alarms that use of FRT in policing may exacerbate existing biases; a 2021 analysis warned that such technology could reinforce police predispositions against minority communities and political dissidents.[19] The very decision of whom to include in watchlist databases or which events to surveil with FRT may reflect bias – for instance, over-policing of Dalit and Adivasi populations (documented in traditional policing) could carry into digital policing, putting those groups at higher risk of false matches.[20]

17 Internet Freedom Foundation, "Is the Illegal Use of Facial Recognition Technology by the Delhi Police Akin to Mass Surveillance? You Decide – Project Panoptic" Internet Freedom Foundation, 2021, *available at:* https://internetfreedom.in/is-the-illegal-use-of-facial-recognition-technology-by-the-delhi-police-akin-to-mass-surveillance-you-decide-project-panoptic/ (last visited on Mar. 17, 2025).

18 Joy Buolamwini and Timnit Gebru, *supra* note 4; Karishma Mehrotra, *supra* note 5.

19 Ameya Bokil, *et.al.*, *supra* note 6.

20 Rina Chandran, "Racist, Sexist, Casteist: Is AI Bad News for India?" *Context*, 2024, *available at*: https://www.context.news/digital-rights/racist-sexist-casteist-is-ai-bad-news-for-india (last visited on Apr. 3, 2025); Rishi Rajpurohit, "Building the Case for Restricted Use of Predictive Policing Tools in India" *Research Gate*, 2023, *available at*: https://www.researchgate.net/publication/376335081_Building_the_case_for_restricted_use_of_predictive_policing_tools_in_India(last visited on Apr. 3, 2025); Common Cause and Lokniti–Centre for the Study of Developing Societies, *"Status of Policing in India Report 2020-21: Volume I – Policing in Conflict-Affected Regions"*, *available at:* https://ruralindiaonline.org/en/library/resource/status-of-policing-in-india-report-2020-21-volume-i-policing-in-conflict-affected-regions/ (last visited on Mar. 3, 2025); Amnesty International, *India 2023: Human Rights Report*, *available at*: https://www.amnesty.org/en/location/asia-and-the-pacific/south-asia/india/report-india/ (last visited on Mar. 3, 2025).

Despite these issues, Indian law enforcement continues expanding FRT usage. There is currently no specific legislation regulating facial recognition. A private member's bill the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 has been proposed in Parliament to introduce safeguards,[21] but it remains to be seen if it will advance. As it stands, the deployment of FRT is governed only by general legal constraints and internal police directives. This gap underscores the importance of courts scrutinizing FRT evidence for reliability and bias before admitting it against an accused.

III Predictive policing systems

Predictive policing refers to the use of AI algorithms to analyse large volumes of historical crime data in order to predict future crime occurrences: whether by identifying likely crime locations known as "hotspots" or by flagging individuals who may be involved in criminal activity. In India, multiple state police agencies have experimented with predictive policing tools as part of "smart policing" initiatives.[22] For example, the Hyderabad City Police adopted a system in 2017 that analyses past crime trends to forecast vulnerable areas and times for offenses.[23] The Delhi Police too, under its Crime Mapping Analytics and Predictive System (CMAPS), began using data analytics to guide patrol deployments.[24] These efforts mirror systems like PredPol (now Geolitica) in the United States, aiming to optimize resource allocation by anticipating crime patterns.[25]

However, evidence from India and abroad indicates serious limitations and biases in predictive policing. Predictive policing in India often relies on inferior quality datasets and is deployed without adequate oversight, leading to reinforcement of police biases.[26] Historical crime data reflect decades of unequal policing –for instance, "habitual offender" databases and crime records may over-record petty offenses in underprivileged localities or among denotified tribes (once branded 'criminal tribes' in colonial times).[27] When algorithms train on such skewed data, they may

21 The Facial Recognition Technology (Regulation of Police Powers) Bill, 2023, Bill No. XX of 2023, *available at*: https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/facial%20recognition%20Priyanka-E1219202360805PM.pdf?source=legislation (last visited Mar. 3, 2025).

22 Antara Vats, *supra* note 6.

23 Internet Freedom Foundation, *supra* note 8.

24 *Ibid.*

25 Aaron Sankin and Surya Mattu, "Predictive Policing Software Terrible at Predicting Crimes" *The Markup*, Oct. 2, 2023, *available at*: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes(last visited on Apr. 03, 2025).

26 Antara Vats, *supra* note 6.

27 Common Cause and Lokniti–Centre for the Study of Developing Societies, *Status of Policing in India Report 2023*, *available at*: https://www.commoncause.in/wotadmin/upload/Report_2023.pdf (last visited on Mar. 3, 2025).

disproportionately predict crime in the same marginalized communities, creating a vicious cycle of over-policing.[28] Indeed, without safeguards, predictive policing ends up *"reinforcing and amplifying police biases in law enforcement."*[29]

One concrete manifestation is in preventive detentions. Section 170 of the BNSS, 2023 permits police to arrest, without a warrant, a person designed to commit a cognizable offense, in order to prevent that offense.[30] Predictive tools that claim to identify likely offenders could encourage police to make such pre-emptive arrests. Basing preventive detention on an algorithm's suspicion poses grave dangers to fundamental rights and criminal justice norms, especially if those algorithms are effectively opaque and unchallengeable.[31] An individual could be detained for a predicted crime that they never intended, owing to a computer's error or bias. This turns the presumption of innocence on its head, recalling critiques that predictive policing risks a *"self-fulfilling prophecy"* of criminalizing certain groups.[32]

Delhi's predictive policing system raises issues in the data underpinning the algorithm.[33]The crime data was incomplete and biased towards certain types of reported crimes, lacking socio-economic context, which could skew predictions towards policing poorer neighbourhoods while ignoring underreported crimes in affluent areas.[34]Internationally, experiences have shown that predictive policing often *over-predicts* in communities of colour (in the US) or immigrant neighbourhoods (in Europe), aligning with ingrained prejudices in policing data.[35] For instance, in Pasco County, Florida, US, a predictive policing program harassed residents with repeated police

28 Ameya Bokil, *et.al.*, *supra* note 6.

29 Antara Vats, *supra* note 6.

30 The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 170.

31 Antara Vats, *supra* note 6; Tim Lau, "Predictive Policing Explained" *Brennan Center for Justice*, Apr. 1, 2020, *available at:* https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained (last visited on Mar. 3, 2025).

32 KilianVieth-Ditlmann, "Algorithmic Policing: When Predicting Means Presuming Guilty" *AlgorithmWatch*, 2021, *available at:* https://algorithmwatch.org/en/algorithmic-policing-explained/ (last visited on Apr. 3, 2025).

33 Vidushi Marda and Shivangi Narayan, "Data in New Delhi's Predictive Policing System," *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT2020)*, *available at:* https://www.vidushimarda.com/storage/app/media/uploaded-files/fat2020-final586.pdf (last visited Feb. 17, 2025).

34 *Ibid.*

35 Tim Lau, *supra* note 31;Fair Trials, *Automating Injustice: The Use of Artificial Intelligence & Automated Decision-Making Systems in Criminal Justice in Europe*, Nov. 2021, *available at*: https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf (last visited on Feb. 3, 2025).

visits based on dubious algorithmic lists of potential offenders, leading to public outcry and eventual legal challenges.[36]

In India, public information on predictive policing deployments remains limited, partly due to lack of transparency. Nevertheless, civil society oversight has begun: the Internet Freedom Foundation served legal notice to Hyderabad Police in 2021 after reports that officers were stopping individuals on the street and compelling them to provide fingerprints or face scans "because an app predicted them as suspects" a practice the Internet Freedom Foundation decried as illegal profiling.[37] Likewise, scholars have cautioned that caste dynamics could creep into algorithmic policing. According to one report, caste-based surveillance (such as the tracking of Dalit and tribal communities) might be turbocharged by predictive analytics if not checked.[38] The combination of legacy biases (*e.g.,* the 'history sheets' of so-called habitual offenders, which disproportionately list marginalized caste individuals) with modern algorithms can result in a digital net that is seemingly neutral but effectively discriminatory.[39]

IV Gait analysis and other emerging forensic AI tools

Another AI-based technique making inroads in India is forensic gait analysis that is the examination of a person's walking pattern to establish identity. CCTV cameras often capture perpetrators from a distance or angles that obscure facial features, but investigators may attempt to match the suspect's gait (movement, posture, stride) with that of a known individual. Traditionally, gait identification could be done by human experts like forensic podiatrists or anatomists as an expert opinion. Increasingly, computer-vision algorithms are being developed to measure biometric features of gait for matching purposes, effectively creating a new form of biometric evidence. Countries like the UK, Netherlands, and Denmark have used forensic gait analysis in investigations for over a decade.[40]

---

36 Kathleen McGrory and Neil Bedi, "Pasco's Sheriff Uses Data to Guess Who Will Commit Crime. Then Deputies 'Hunt Down' and Harass Them" *Tampa Bay Times*, Sep. 3, 2020, *available* at: https://www.tampabay.com/news/pasco/2020/09/03/pascos-sheriff-uses-data-to-guess-who-will-commit-crime-then-deputies-hunt-down-and-harass-them/(last visited on Mar. 3, 2025).

37 Internet Freedom Foundation, "Hyderabad Police force" *supra* note 8.

38 Ameya Bokil, *et.al., supra* note 6.

39 AI Now Institute, "A New AI Lexicon: 'Caste'" *AI Now Institute*, 2021, *available at:* https://ainowinstitute.org/publication/a-new-ai-lexicon-caste (last visited on Feb. 3, 2025); Nikita Sonavane, "Casteist Carcerality: Everyday Policing of 'Habitual Offenders' in India" *History for Peace*, 2022, *available at:* https://www.historyforpeace.pw/post/casteist-carcerality-everyday-policing-of-habitual-offenders-in-india-nikita-sonavane (last visited on Mar. 18, 2025).

40 Mastrigt, Celie, *et al.*, "Critical review of the use and scientific basis of forensic gait analysis." *Science and Justice* 58.5 (2018): 357-363, *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6201773/ (last visited Feb. 4, 2025).

Indian courts have seen gait evidence in a few recent cases. In 2021, a Mumbai special court convicted a man for rape and murder in the *Saki Naka* case, relying in part on a gait analysis report that linked the accused to CCTV footage.[41] This was reported as possibly the first conviction in India using a "gait test" as evidence. Similarly, during the investigation into the 2017 murder of journalist Gauri Lankesh in Bengaluru, the Special Investigation Team used gait comparison of CCTV video to help identify suspects.[42] With CCTV surveillance pervasive in cities, police are increasingly turning to gait features when facial clarity is lacking. Gait analysis is thus gaining recognition in Indian courts as a form of expert forensic evidence.

At the same time, gait analysis illustrates the challenges of emerging forensic science. A person's gait is a behavioural biometric, not a fixed physical trait – it can vary with context, footwear, fatigue, or disguise.[43] Unlike fingerprints or DNA, there is no singular, unchanging "gait signature." Studies have found that even trained gait analysts can differ in their interpretations. In one experiment, multiple experts analyzing the same set of CCTV clips achieved only about 71% accuracy in identifying whether the suspect's gait matched the target, highlighting that conclusions involve probabilities, not certainties.[44] Moreover, no uniform protocol exists yet for gait comparison; methodologies vary, leading to a risk of subjectivity.[45] The UK recognized these concerns and in 2018 published a draft Code of Practice for Forensic Gait Analysis to standardize how experts approach such evidence.[46]In contrast, India currently lacks not only formal guidelines but even a comparable draft framework or accreditation standard for gait analysis.

Bias in gait analysis can emerge in subtler ways. If a computer model is used, any bias in training data could affect accuracy across different body types or cultural attire. Even human examiners are not free from unconscious prejudice, potentially seeing what they expect to see (confirmation bias) or being influenced by knowledge of a suspect's identity or background.[47] Thus, while gait evidence can be a useful corroborative tool, it is far from foolproof. Indian courts have treated it as an expert

41 *State of Maharashtra* v. *Mohan Kathwaru Chauhan*, SC/ST Special Case No. 380 of 2021; Snehil Singh, *supra* note 1.

42 *Ibid.*

43 Ashish Badiye, Prachi Kathane, and Kewal Krishan, *Forensic Gait Analysis* (Updated Nov. 7, 2022), in *Stat Pearls* [Internet] (StatPearls Publishing, Treasure Island (FL), Jan. 2025), *available at*: https://www.ncbi.nlm.nih.gov/books/NBK557684/ (last visited on Mar. 05, 2025)

44 Mastrigt, Celie, *et al., supra* note 40.

45 *Ibid.*

46 "Forensic gait analysis: a primer for courts." *The Royal Society*, 2017. *Available at*: https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf (last visited Feb. 5, 2025).

47 Mastrigt, Celie, *et al.*, *supra* note 40.

opinion under Section 45 of the Indian Evidence Act (Section 39, BSA), meaning it is only advisory and not conclusive.[48] In fact, a recent judgment of the High Court of Madras ruled that if CCTV footage is too unclear to permit a reliable gait analysis, the accused cannot be compelled to provide a fresh gait sample by re-enacting the walk, as that would effectively force him to generate self-incriminating evidence.[49] This reflects caution, acknowledging both technical limits and constitutional protections (like the right against self-incrimination under article 20(3)).

Beyond these three tools, other AI-driven forensic techniques are on the horizon in India: voice recognition and speaker identification, license plate recognition, and even "crime scene reconstruction" software.[50] Each brings analogous concerns of accuracy and fairness. As India embraces a new era of digital forensics, the legal system faces a critical question – how should courts determine whether algorithm-generated evidence is admissible and credible?

V Admissibility of AI-derived evidence under BSA 2023 and BNSS 2023

The BSA and the BNSS constitute the primary legal framework governing how evidence is collected, presented, and evaluated in criminal trials. Any AI-based forensic result, be it a facial recognition match or a predictive algorithm's output, must satisfy the requirements of these laws to be admissible in court. In essence, Indian law does not have special provisions exclusive to "algorithmic evidence." Instead, such evidence will be analogized to existing categories like expert opinion, electronic records, or scientific reports, and tested under general admissibility criteria of relevance and reliability.

---

48 The Bharatiya Sakshya Adhiniyam, 2023 (Act 49 of 2023), s. 39.

49 Mohamed Imranullah S., "When CCTV visuals are unclear, suspects cannot be forced to re-enact the crime for gait analysis, rules Madras High Court" *The Hindu*, June 20, 2024, *available at:* https://www.thehindu.com/news/national/tamil-nadu/when-cctv-visuals-are-unclear-suspects-cannot-be-forced-to-re-enact-the-crime-for-gait-analysis-rules-madras-high-court/article68310945.ece (last visited on Mar. 5, 2025).

50 Pragati Jain, Pragna Chinmayee, Kamaljeet Kaur, and Shefali Chaudhary, "Advancements in Forensic Voice Analysis: Legal Frameworks and Technology Integration" *Research Gate* (July 2024), *available at* : https://www.researchgate.net/publication/382537301_Advancements_in_Forensic_Voice_ Analysis_Legal_Frameworks_and_ Technology_Integration(last visited Apr. 5, 2025); Sergio Montazzolli Silva and Claudio Rosito Jung, "Real-Time License Plate Detection and Recognition Using Deep Convolutional Neural Networks" 71 *Journal of Visual Communication and Image Representation* 102773 (2020), *available at*: https://www.sciencedirect.com/science/article/abs/pii/S1047320320300237 (last visited Feb. 5, 2025); Snehalata U. Shenoy, Varad Nagar, and Akhith, "Artificial Intelligence-Based Techniques for Crime Scene Reconstruction and Investigation: An Overview" 14(4) *Journal of Forensic Research* (2023), *available at:* https://www.hilarispublisher.com/open-access/artificial-intelligencebased-techniques-for-crime-scene-reconstruction-and-investigation-an-overview-99302.html (last visited Feb. 5, 2025).

Expert opinion and electronic evidence based on the evidence act framework

Under the BSA there are two key routes through which AI-derived evidence might enter trial proceedings:-

Expert opinion

If the AI tool's findings are presented via a human expert who interprets or explains them, that testimony is treated as expert opinion evidence under the BSA. For example, a forensic analyst might testify that *"the facial recognition software identified 'X' as the person in the CCTV image with 90% confidence"* or that *"after analyzing the gait patterns, I conclude the suspect's gait is consistent with the person in the video."* Here, the witness is an expert relying on the AI tool's analysis as the basis of their opinion. Section 45[51] allows experts to testify on matters of science, identification of handwriting or fingerprints, etc., and by extension, algorithmic analyses can be included. In fact, gait analysis has been explicitly noted to fall under section 45 when done by a human expert.[52] The expert must be shown to have specialized knowledge in the field (e.g. a forensic data analyst or an AI specialist). However, crucially, expert opinions are not binding on the court; judges are free to accept or reject them after considering methodology and credibility.[53] This principle empowers judges to act as gatekeepers, scrutinizing whether the AI tool used is scientifically valid.

Electronic/digital evidence

If the output of an AI system is presented as an electronic record – for instance, a printout of a facial recognition match report, or a log file from predictive policing software – it must meet the admissibility criteria for electronic evidence. Section 63 of the BSA deems electronic records admissible as long as certain conditions are met to ensure integrity. For instance, proof that the record was produced from a computer in regular use and has not been altered.[54] Section 63 eases the admissibility of digital records, stating that electronic records shall have the same legal effect as paper records, subject to conditions for authenticity.[55] For AI outputs, this means a certificate under section 63(4) (by a person in charge of the computer system) would typically be required to attest that the data was reliably produced.[56] Additionally, the BSA brings examiners of electronic evidence (appointed under Section 79A of the IT

51 The Bharatiya Sakshya Adhiniyam, 2023 (Act 49 of 2023), s. 45.

52 Snehil Singh, *supra* note 1.

53 Examination Of Expert' Opinion: Relevancy, Admissibility, And The Framework," *Mondaq*, *available at*: https://www.mondaq.com/india/trials-amp-appeals-amp-compensation/1258928/examination-of-expert-opinion-relevancy-admissibility-and-the-framework (last visited Apr. 5, 2025)

54 The Bharatiya Sakshya Adhiniyam, 2023 (Act 49 of 2023), s. 63(2).

55 *Id.*, s. 63(1).

56 *Id.*, s. 63(4).

Act, 2000) on par with other experts, so that their opinions on electronic data (potentially including algorithm functioning) are relevant.[57] In practice, police might submit an AI result accompanied by a certificate from the system operator or a forensic lab analyst.

Importantly, whether *via* expert opinion or electronic record, the evidence must pass the test of relevance, and it must relate to a fact in issue or a relevant fact in the case and not be excluded by any other rule. For example, a predictive policing algorithm's assessment that *"'A' is likely to commit a burglary next week"* would not directly be relevant to proving 'A' committed the burglary charged it's more of a suspicion generator than proof of a past act. Using such a prediction as evidence of guilt would violate the basic relevance and also conflict with the presumption of innocence. Thus, courts are unlikely to admit a "predictive score" about a defendant as evidence of propensity, as it would be analogous to impermissible character evidence or profiling.[58] In an American context, this is akin to "similar fact" or bad character evidence rules, which Indian law also treats with caution.

Facial recognition matches and gait analysis are somewhat different because they purport to identify the defendant as the person in a scene which is directly relevant to identity of the offender, a key fact in issue. Here the question shifts from relevance to weight and reliability. The BSA does not list specific reliability thresholds for scientific evidence, but Indian courts have precedent of assessing the soundness of novel scientific techniques. Although India does not have a codified equivalent of the United States *Daubert* standard, judges have invoked general standards of scientific acceptance. In *State of Himachal Pradesh* v. *Jai Lal*, the Supreme Court held that expert opinion is only valuable when based on certain facts or data and the methodology is reliably applied to those facts otherwise the court may reject it.[59] This aligns with the logic of *Frye* (general acceptance test) and *Daubert* (reliability test) used in other jurisdictions, even if not formally adopted.

The BSA does attempt to modernize and consolidate principles regarding expert evidence. One notable change is that it brings digital and electronic experts to parity with other experts.[60] Earlier, some felt electronic evidence examiners' certificates were given special status. Now, all expert analysis, whether of DNA, handwriting, or computer data, is subject to the same scrutiny. This implicitly means an AI algorithm's result presented by an expert should be judged by the same yardsticks of relevance and probative value, and the court can insist that the underlying algorithm be explained to the extent necessary to test its veracity.

---

57 *Id.*, s. 39(2).

58 Antara Vats, *supra* note 6

59 *State of Himachal Pradesh* v. *Jai Lal*, AIR 1999 SC 3318.

60 The Bharatiya Sakshya Adhiniyam, 2023 (Act 49 of 2023), s. 39(2).

VI Criminal procedure and forensic collection

The BNSS, introduces some provisions that encourage use of technology in investigation and court procedure. Two are particularly noteworthy:

Mandatory forensic investigation for serious crimes

BNSS mandates that for offenses punishable with seven years or more, a forensic team must visit the crime scene, collect evidence, and record the process.[61] This indicates an institutional push to incorporate scientific methods, which could include AI tools, in building the evidentiary base of serious offences. For instance, if a CCTV camera captured part of a crime, forensic teams might use facial or gait recognition tools as part of evidence collection. The process must be recorded how the evidence was obtained should be documented, aiding later transparency. If an algorithm was used, ideally its use should be noted in the case diary or forensic report, which defense can later inspect.

Electronic mode for trials and evidence presentation

The BNSS explicitly allows trials, inquiries, and proceedings to be conducted in electronic mode,[62] and permits the production of electronic devices that may contain digital evidence for inspection.[63] This procedural openness implies that courts should be ready to handle digital forms of evidence directly. In an AI context, it could mean a court might view a software interface demonstration or consider digital forensic reports on-screen. The BNSS also allows taking voice samples and fingerprints even from persons who are not arrested (aiding building databases or eliminating suspects):[64] a sign of widening the investigatory toolkit.

When it comes specifically to admissibility in trial, Sections 218-21 of BNSS likely continue to allow certain forensic reports to be used as evidence without the examiner's presence (for efficiency), *e.g.*, reports under the *Criminal Identification* provisions or certified reports by government scientific experts. If an AI tool's output is part of such a report, it could be submitted under those provisions. However, typically, the defense has the right to demand the expert be summoned for cross-examination if the report is contested.

No specific clause in BNSS explicitly addresses algorithm transparency or bias. It is largely tech-neutral, assuming that evidence whether physical, biological, or digital will be handled with existing procedures of proof. Therefore, challenges to AI evidence admissibility will likely be raised through traditional means: opposing counsel may file

61 The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), s. 176(3).

62 *Id.*, s. 532.

63 *Id.*

64 *Id.*, s. 349.

an application to exclude evidence (akin to a *voir dire* or a preliminary objection) on grounds that it lacks reliability or would violate fair trial if admitted. For example, a defense could argue that a facial recognition match is so error-prone that it fails the threshold of relevance or would mislead the jury/judge unduly (similar to how "junk science" can be excluded). Indian judges, being the triers of fact in most criminal cases, have a measure of flexibility in weighing evidence – they might admit the evidence but assign little weight if they doubt its accuracy, rather than excluding it outright. However, in close cases, the mere presence of a purportedly scientific match might prejudice the judge unless caution is exercised. This makes it vital for the BSA's principles of evaluation to be rigorously applied.

One helpful existing safeguard is the requirement of corroboration. Generally, courts hesitate to convict solely on the basis of new or untested forensic techniques without corroboration from independent evidence. This was seen in the context of narco-analysis and brain-mapping tests – even when results were voluntarily obtained, courts treated them as needing corroboration since their scientific reliability is not absolute.[65] By analogy, an AI prediction or identification on its own should not suffice; it should be corroborated by traditional evidence (eyewitness, physical evidence, *etc.*), or at least the AI result should be verified by a human expert analysis before being given weight.

VII Constitutional doctrines: due process, fair trial, equality and privacy

The introduction of algorithmic tools in criminal justice engages core constitutional values in India. Even if domestic statutes formally permit a piece of evidence, its use might be impermissible if it violates fundamental rights of the accused or public. Four constitutional principles are particularly relevant: *first,* the right to equality, which guards against discriminatory treatment; *second,* the right to life and personal liberty, which has been interpreted to encompass due process of law and fair trial; from these emanate more specific rights like *third,* the right to a fair trial and procedural due process, *fourth* the right to privacy, and *fifth* the right against self-incrimination. We examine each in turn *vis-à-vis* AI forensic tools.

Equality before law and non-discrimination

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws.[66] A facially neutral practice can violate article 14 if it results in unfair discrimination against a class without reasonable justification. Algorithmic bias raises the spectre of indirect discrimination. If a policing algorithm systematically performs worse on certain racial, ethnic, or caste groups, using it could lead to those groups facing higher likelihood of misidentification, arrest, or scrutiny compared to others. This is an equality concern. The equal protection provision would demand that state

65 *Selvi* v. *State of Karnataka* (2010) 7 SCC 263.

agencies not employ technologies that have an unjustifiably disparate impact on protected groups such as Scheduled Castes, Scheduled Tribes, religious minorities, or women.

In jurisdictions like the UK., this logic has been applied through the public sector equality duty.[67] In the landmark case of *Bridges v. South Wales Police*, the UK Court of Appeal found that the police's use of live facial recognition was unlawful partly because the police failed to account for the technology's bias risks – their deployment did not satisfy the Public Sector Equality Duty to consider if the system created indirect discrimination by race or sex.[68] The court noted that the police had not assessed whether the algorithm's error rates were higher for women or ethnic minorities, calling the lack of such evaluation "obviously inadequate."[69] This resonates with article 14's mandate in India.

If an Indian court were faced with evidence that, say, a facial recognition match was the basis of the accused's identification, and it was shown that the algorithm has a known error rate bias such that it more frequently misidentifies people of the accused's community, a constitutional question of whether it is consistent with equality and non-discrimination to treat this as credible evidence arises. A strong argument can be made that knowingly relying on a biased tool amounts to state-sanctioned discrimination, unless the bias can be corrected or its impact neutralized through additional safeguards. For instance, if a tool is 10 times more likely to falsely match a tribal person than an upper-caste person, using that tool to generate leads against tribal persons might offend the equal protection guarantee, absent a strong justification and counter-balancing measures.

Moreover, article 14 also entails a broader concept of arbitrariness – state actions must not be arbitrary or irrational. An algorithm that produces results with no discernible scientific rigor or that is opaque and unexplainable could be challenged as arbitrary if used to deprive someone of liberty. The Supreme Court in *Shayara Bano* v. *Union of India* expanded article 14 to strike down the practice of instant triple talaq on the ground that it allowed unilateral divorce without due process or fairness, rendering it manifestly arbitrary under article 14.[70] This case established that even practices not explicitly discriminatory could be unconstitutional if they were unprincipled or capricious. If, for example, predictive policing was used to justify detaining individuals purely because a formula labelled them high-risk – this might be seen as an arbitrary

66 The Constitution of India, art. 14.

67 The Equality Act, 2010, s. 149.

68 *Bridges* v. *South Wales Police*, [2020] EWCA Civ 1058.

69 *Ibid.*

70 *Shayara Bano* v. *Union of India*, (2017) 9 SCC 1.

deprivation of liberty not based on individualized evidence, thus violating article 14 (and article 21).

Right to life and personal liberty (article 21) – due process and fair trial

Article 21 guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law.[71] Since *Maneka Gandhi* v. *Union of India*, "procedure established by law" has been read to imply a requirement of fundamental fairness and reasonableness – effectively importing a due process standard.[72] In criminal proceedings, this means the process leading to any deprivation (such as conviction and punishment) must be fair, just, and equitable. Fair trial is a core component of article 21, as affirmed in cases like *Zahira Habibullah Sheikh* v. *State of Gujarat*[73] and *Hussainara Khatoon* v. *State of Bihar*.[74] Additionally, the Supreme Court has held that the right to a fair trial is not just for the accused, but also for the victim and society, ensuring justice is done.[75] However, here our focus is on the accused's fair trial rights, which include the rights to present a defense, to challenge the prosecution's evidence, and to be tried by an impartial tribunal on the basis of reliable evidence.

Use of AI evidence poses at least two challenges to fair trial rights:

The ability of the defense to contest the evidence

If an AI algorithm is used in the investigative or evidentiary process, the defense must have a meaningful opportunity to challenge its findings. This implicates the principle of "equality of arms" – both sides should be able to examine and test evidence. In traditional forensic evidence, defense counsel can cross-examine the expert who conducted a test about potential errors or alternative interpretations. With AI, especially proprietary algorithms, there is a risk that the underlying method is a "black box" shielded from scrutiny.[76] For instance, if police use a commercial facial recognition software to identify a suspect, the vendor might claim trade secrecy over the algorithm, preventing disclosure of how it works or its detailed error rates. Admitting evidence from such a system without allowing the defense to inspect and challenge it would raise due process flags. The Sixth Amendment confrontation right in the US (not directly applicable in India, but a comparable fair trial concept) was

71 The Constitution of India, art. 21.

72 *Maneka Gandhi* v. *Union of India*, (1978) 1 SCC 248.

73 *Zahira Habibullah Sheikh (5)* v. *State of Gujarat* (2006) 3 SCC 374.

74 *Hussainara Khatoon* v. *Home Secretary, State of Bihar* (1980) 1 SCC 81.

75 *State of Punjab* v. *Gurmit Singh* (1996) 2 SCC 384.

76 Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI" 41 *Computer Law & Security Review* 105567 (2021), *available at* :https://www.sciencedirect.com/science/article/abs/pii/S0267364921000406 (last visited Apr. 05, 2025).

invoked in a New Jersey case where the court held that a defendant must be given access to the inner workings of the facial recognition software used to implicate him, including source code and error rates.[77] The NJ appellate court recognized that otherwise the defendant's due process rights would be violated.[78] By analogy, Indian courts under article 21 should ensure that if algorithmic results are used, the defense is provided sufficient information to test the evidence's reliability – whether by examining the algorithm, obtaining error rate statistics, or cross-examining those who operated it.

The Supreme Court in *Natasha Singh* v. *CBI* stated that fair trial includes the right to fair and proper opportunities to the accused to prove his innocence which extends to the right to effectively cross-examine prosecution witnesses and evidence.[79] If a machine's output is effectively functioning as a witness against the accused, *the ability to cross-examine that "witness" becomes a complex issue*. One cannot cross-examine a software program, but one can cross-examine the person who interpreted or input data into it, and one can examine the validity of the process. In *Melendez-Diaz v. Massachusetts*,[80] the US Supreme Court held that a forensic lab report (a certificate of drug analysis) was testimonial evidence, and the defendant had a right to demand the analyst's live testimony by extension, one might argue an AI report is "testimonial" and the defense can insist on examining the expert who relied on the AI.[81] Indian law, while not having a confrontation clause, has principles of natural justice under article 21 to similar effect.

The reliability of the evidence itself

The Supreme Court's decision in *Selvi* v. *State of Karnataka* addressed the admissibility of scientific techniques like narco-analysis, polygraph tests, and Brain Electrical Activation Profile (BEAP).[82] The court there not only grounded its decision in the right against self-incrimination but also noted the *questionable reliability* of these techniques.[83] The judgment stressed that involuntary administration of these tests violates due process, and even when voluntary, the results have to be evaluated carefully as they are not definitive.[84] By analogy, introducing evidence from an AI

77 *State* v. *Arteaga*, No. A-3078-21, slip op. at 19–20 (N.J. Super. Ct. App. Div. June 7, 2023).

78 *Ibid.*

79 *Natasha Singh* v. *Central Bureau of Investigation (State)* (2013) 5 SCC 741.

80 *Melendez-Diaz* v. *Massachusetts*, 557 U.S. 305 (2009).

81 Gabrielle M. Haddad, "Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom" 23 *Vanderbilt Journal of Entertainment and Technology Law* 1007 (2021), *available at:* https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1051&context=jetlaw (last visited Apr. 6, 2025).

82 *Supra* note 64.

83 *Ibid.*

84 Snehil Singh, *supra* note 1.

system known to have significant error rates might contravene the requirement of a fair, rational trial process. If a court were to convict someone largely on an FRT match that has, say, a 10% false match rate, one could argue this falls below the threshold of proof "beyond reasonable doubt," which is a facet of fair trial. In *K.M. Nanavati* v. *State of Maharashtra*, the standard of proof beyond reasonable doubt was held sacrosanct in criminal cases – algorithmic evidence with high uncertainty could undermine this standard unless accompanied by strong corroboration.[85]

Additionally, unequal access to technology can raise fairness issues. The state might have sophisticated AI tools at its disposal, whereas defendants especially indigent ones do not. Article 21, read with article 39A – right to legal aid, would demand that defendants be given resources to challenge such evidence perhaps by appointing independent experts or providing access to the software for independent testing. Failure to do so could tilt the playing field, making the trial unfair.

VIII Privacy and surveillance concerns

The right to privacy, recognized as a fundamental right under article 21 in *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*, has significant implications for the use of AI in surveillance and evidence gathering.[86] Puttaswamy established that privacy covers personal autonomy and control over personal data, and any state infringement on privacy must satisfy the test of legality, necessity, and proportionality.

Facial recognition and predictive policing inherently involve surveillance and data processing that can infringe privacy.[87] Live facial recognition scans individuals in public, capturing and processing their biometric data without consent. Predictive policing may involve monitoring people's activities or locations to feed the algorithm. Under Puttaswamy, such actions amount to a search or surveillance that intrudes on the right to privacy of movement and anonymity in public spaces – a concept that courts are grappling with globally. For an intrusion to be valid, there must be a law authorizing it, and it must be necessary and proportionate to a legitimate aim.[88]

Currently, India lacks a comprehensive law specifically authorizing facial recognition surveillance or algorithmic predictions. The absence of a clear statutory framework with safeguards for these technologies can render their indiscriminate use constitutionally suspect. In *PUCL* v. *Union of India*,[89] the Supreme Court read procedural safeguards into the Telegraph Act to protect privacy, noting that unregulated

85 *K.M. Nanavati* v. *State of Maharashtra*, AIR 1962 SC 605.

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

87 U.S. Department of Justice, *Artificial Intelligence and Criminal Justice*, Dec. 2024, *available at:* https://www.justice.gov/olp/media/1381796/dl (last visited on Apr. 06, 2025).

88 *Supra* note 85.

89 *People's Union for Civil Liberties (PUCL)* v. *Union of India* (1997) 1 SCC 301.

surveillance invites abuse. By analogy, deploying FRT broadly to identify people in crowds without statutory oversight could be challenged as an illegal invasion of privacy. The necessity and proportionality prongs would require the state to show that using FRT or predictive systems is necessary to achieve a pressing security goal and that there were no less intrusive means, and that the measure is narrowly tailored. If the technology is riddled with errors or biases, its proportionality is undermined because the benefits are diminished while the privacy harm is large.

Privacy concerns also intersect with fair trial rights: if evidence is gathered in a manner that violated someone's privacy, should it be admissible? Indian law does not have an exclusionary rule as stringent as the US Fourth Amendment's exclusionary rule for illegal searches, but courts have shown discomfort with evidence obtained through gross rights violations.[90] In context, if police used an unconstitutional mass surveillance tool to identify a suspect (for example, using facial recognition on everyone at a peaceful protest, violating their privacy and perhaps chilling freedom of expression/assembly), a court might in theory exclude the resulting identification to discourage such methods which would be a judicially created remedy, as neither BSA nor BNSS explicitly address this. At minimum, the courts would likely subject such evidence to heightened scrutiny of reliability given the covert way it was obtained.

Furthermore, data privacy aspects arise. AI tools often rely on large datasets like databases of faces, or crime data. Collecting and using personal data like faces, biometrics, past criminal records including those of acquitted persons, etc. must comply with privacy principles. The Digital Personal Data Protection Act, 2023 provides certain exemptions for law enforcement, but also requires fair and reasonable processing.[91] If an algorithm processes personal data in a biased or secretive way, individuals might have a privacy-based claim. A convict might argue their data was processed unlawfully by an AI, leading to their implication.

Thus, from a constitutional perspective, surveillance-oriented AI tools should have a lawful basis and be used in a proportionate manner. Judicial oversight might be constitutionally required in the long run, to prevent a drift towards a techno-surveillance state. Article 14 and 21 combined create a framework where any state action that is opaque, untested, or discriminatory could be struck down as violating due process or equality. The courts, as guardians of fundamental rights, may not permit a conviction to rest on evidence that fails these constitutional benchmarks.

---

90 E. Prema and Shanmuga Sundaram Angamuthu, "Fruits of the Poisonous Tree – Exclusionary Rule and Its Application in India" (May 11, 2023), *available at* :https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4685782 (last visited Apr. 06, 2025).

91 The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17.

IX Right against self-incrimination

Though not explicitly mentioned in the prompt, article 20(3)[92] is an important doctrine in the context of forensic evidence.[93] Reaffirming the principle laid down earlier, the court has consistently maintained that involuntary investigative procedures such as Brain Electrical Activation Profile or narco-analysis violate both mental privacy and the right against self-incrimination.[94]The judgment distinguished between physical evidence such as fingerprints, DNA, voice samples which are non-testimonial and can be compelled, versus testimonial/communicative acts which cannot be.[95]

Applying this to AI forensic tools, if the use of the tool requires the accused's participation in a way that is testimonial, then article 20(3) is implicated. For instance, being forced to speak certain phrases for a voice recognition test, or as the High Court of Madras case held that to walk for a gait analysis re-enactment could be argued as compelled evidence.[96] The reasoning likely is that making the suspect perform to produce evidence is akin to making him testify especially because gait, while physical, is also a manifestation of behaviour, potentially classified as non-testimonial physical evidence. The lines can blur, but courts will be cautious in compelling any action from the accused for feeding an algorithm unless clearly non-testimonial and authorized by law.

Under BNSS, police can take fingerprints, iris scans, photographs, and voice samples from accused– these have been held to be physical evidence and thus permissible.[97] Gait might be analogous to voice as it is a physical characteristic that can be measured, but if it involves an element of performing an act related to the crime i.e., re-enacting the crime scene walk, it edges toward testimonial. So, any procedure employing AI must respect the line drawn by article 20(3). An AI cannot be used as a backdoor to compel what a human interrogator could not; for example, you cannot force a suspect to wear AR glasses that track eye movements to see if they recognize a crime scene.

Constitutional doctrines demand that the use of AI in criminal justice be balanced against individual rights. Evidence from AI tools must not only be handled in compliance with statutes but must also survive scrutiny for fairness, transparency, and non-discrimination. This is an evolving area – Indian courts have yet to directly rule on algorithmic bias, but the principles from analogous cases provide guidance that they

92 "No person accused of any offence shall be compelled to be a witness against himself."

93 The Constitution of India, art. 20(3).

94 *Supra* note 64.

95 *Ibid.*

96 *Supra* note 49.

97 *State of Bombay* v. *KathiKalu Oghad*, AIR 1961 SC 1808.

are unlikely to give a free pass to "machine evidence" without ensuring it meets the same constitutional muster as human-gathered evidence. To better appreciate how these concerns are being handled elsewhere and what lessons can be learned, we turn to comparative perspectives.

X Comparative perspectives on AI forensic admissibility

As India grapples with regulating AI in criminal justice, valuable insights can be drawn from experiences in other jurisdictions. The United States and United Kingdom in particular have seen early litigation and policy responses to algorithmic evidence, while the European Union is establishing normative frameworks addressing AI risks. These comparative perspectives highlight common challenges – mainly around accuracy, transparency, and fundamental rights and demonstrate potential legal standards and safeguards.

United States – Daubert reliability and due process

In the U.S., the admissibility of scientific or technical evidence in court is governed by standards stemming from Rule 702 of the Federal Rules of Evidence[98] and the landmark Supreme Court case *Daubert* v. *Merrell Dow Pharmaceuticals*.[99] Under Daubert (and later cases *Joiner*, *Kumho Tire*),[100] judges act as "gatekeepers" who must ensure expert testimony rests on a reliable foundation and is relevant. They consider factors like whether the theory or technique has been tested, peer reviewed, has a known error rate, and has gained general acceptance. This framework has direct bearing on AI evidence: any result produced by an algorithm would likely be presented through an expert witness explaining the tool. That testimony can be challenged under Daubert. Indeed, an algorithm's match or score is only as admissible as the algorithm is demonstrably reliable.

American courts have started to see such challenges. For example, in a recent Ohio murder case, a judge excluded facial recognition evidence on the grounds of concerns over reliability and transparency, effectively preventing a conviction that relied on that match.[101] This indicates that at least some courts, applying Daubert, are not convinced that FRT has met the reliability threshold, especially if the defense cannot thoroughly probe how the match was generated. Similarly, in cases involving

98 Federal Rules of Evidence, Rule 702.

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

100 *General Electric Co.* v. *Joiner*, 522 U.S. 136 (1997); *Kumho Tire Co.* v. *Carmichael*, 526 U.S. 137 (1999).

101 Lars Daniel, "Judge Throws Out Facial Recognition Evidence In Murder Case" *Forbes*, Jan. 29, 2025, *available at*: https://www.forbes.com/sites/larsdaniel/2025/01/29/judge-throws-out-facial-recognition-evidence-in-murder-case/ (last visited on Apr. 7, 2025).

probabilistic DNA genotyping software such as TrueAllele[102] or STRmix,[103] which use algorithms to interpret complex DNA mixtures, US courts have sometimes been cautious. In *United States* v. *Gissantaner*, a federal judge excluded TrueAllele results because the defense was denied access to its source code, making it impossible to challenge reliability – the judge noted that without transparency the evidence did not satisfy Daubert's test of scientific scrutiny.[104] This resonates strongly with the earlier mentioned New Jersey case,[105] where an appellate court mandated source code disclosure for facial recognition used in an investigation.[106] Such decisions underscore a vital principle that if the prosecution wants to use algorithmic evidence, it must be prepared to expose the algorithm to adversarial testing.

From a due process standpoint, United States courts and scholars have voiced worries about "black box" algorithms. In *State* v. *Loomis*,[107] the Wisconsin Supreme Court confronted the use of a proprietary risk assessment algorithm (*hereinafter,* "COMPAS") at sentencing. The defendant argued that he couldn't challenge COMPAS's validity because its inner workings were secret, violating due process. The court allowed COMPAS in that instance but with cautionary conditions that it cannot be the determinative factor in sentencing and must be accompanied by warnings of its limitations.[108] While that was a sentencing (not guilt) context, it reflects awareness of the opacity problem. If we translate that to evidentiary use, one can conceive a rule that algorithmic results should never be the sole basis of a conviction and juries/ judges should be instructed about their potential errors – a practice some United States courts might adopt, akin to how eyewitness IDs are now often accompanied by jury instructions about their fallibility.

---

102 Cybergenetics, "TrueAllele Casework System," *Cybergenetics*, *available at*: https:// www.cybgen.com/products/casework/(last visited on Apr. 08, 2025).

103 STRmix™, "Probabilistic Genotyping Software for Forensic DNA Interpretation," *STR mix*, *available at:* https://www.strmix.com/ (last visited on Feb. 8, 2025).

104 *United States* v. *Gissantaner*, 990 F.3d 457 (6th Cir. 2021).

105 *Supra* note 76.

106 Karen Gullo, "Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him" *Electronic Frontier Foundation*, June 7, 2023, *available at:* https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition (last visited on Apr. 08, 2025).

107 *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

108 NAACP, "Artificial Intelligence and Predictive Policing: Issue Brief," *NAACP*, 2021, *available at*: https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief (last visited on Mar. 8, 2025).

Additionally, the United States has seen legislative and executive actions. Some cities have banned police use of facial recognition entirely, citing civil rights concerns.[109] While that doesn't directly create a courtroom standard, it reflects a normative stance that the tech is too flawed for use. The state of Maine enacted a law strictly limiting use of facial recognition by law enforcement.[110] At the federal level, guidelines from the National Institute of Standards and Technology and the FBI encourage testing facial recognition systems for accuracy across demographics.[111] Though not law, these set expectations that could play into court evaluations of whether using a particular algorithm was reasonable.

The United States practice highlights the importance of reliability standards (Daubert) and the confrontation right. Defense access to algorithms and data is increasingly being recognized by courts as necessary for fairness.[112] India, which doesn't have an identical evidentiary provision, can still derive the principle that any novel forensic tech must be independently validated and open to challenge.

Legal challenges and regulatory efforts in the United Kingdom

The UK's experience, especially with facial recognition, has revolved around judicial review and regulatory oversight rather than evidentiary rulings in criminal trials. The aforementioned case of *Bridges*[113]was a watershed moment wherein Ed Bridges, a private citizen, challenged the police's use of live AFR in public spaces as a violation of privacy[114] and data protection and equality laws. The Court of Appeal held the use unlawful on three grounds:

Insufficient legal basis

There was no clear law governing when and how AFR could be used, hence it was not "in accordance with law."[115]

109 ACLU of Massachusetts, "Boston Becomes Largest City on East Coast to Ban Face Surveillance" *ACLU of Massachusetts*, June 24, 2020, *available at*: https://www.aclum.org/en/press-releases/boston-becomes-largest-city-east-coast-ban-face-surveillance (last visited on Apr. 8, 2025); Matt O'Brien and Janie Har, "Public Safety, Civil Rights Groups Battle Over Face ID Tech" *KCRA News*, May 13, 2019, *available at:* https://www.kcra.com/article/public-safety-civil-rights-groups-battle-face-id-tech/27459724 (last visited on Mar. 08, 2025).

110 Maine Revised Statutes, Title 25, Part 14, Ch. 701.

111 Patrick Grother, Mei Ngan and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," NIST Interagency Report 8280, Dec. 2019, available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (last visited on Apr. 08, 2025); Kimberly J. Del Greco, "Facial Recognition Technology: Ensuring Transparency in Government Use," FBI, *available at:* https://www.fbi.gov/news/speeches-and-testimony/facial-recognition-technology-ensuring-transparency-in-government-use (last visited on Apr. 08, 2025).

112 *Supra* note 104.

113 *Supra* note 67.

114 The European Convention on Human Rights, 1950, art. 8.

115 *Id.,* art. 8(2).

Privacy and data protection

The use was not strictly necessary and proportionate, and the Data Protection Impact Assessment was inadequate.[116]

Public sector equality duty

As noted earlier, the police failed to adequately consider the risk of indirect discrimination (bias against race/sex).[117]

While Bridges was about live use and not a specific prosecution, its effect has been to halt or heavily scrutinize facial recognition deployments by UK police. The London Metropolitan Police and South Wales Police had to pause and improve their frameworks. If a facial recognition identification were to be introduced as evidence in a UK court today, Bridges suggests that the defense could argue its collection was unlawful or its reliability suspect, given that even the police hadn't proven it free of bias. The UK also has the Forensic Science Regulator (*hereinafter,* "FSR"), a body that issues codes of practice for forensic methods. In 2021, the FSR was put on a statutory footing, meaning labs must comply with its standards. The FSR has been examining algorithmic tools including probabilistic genotyping and gait analysis. The publication of the *Draft Forensic Gait Analysis Code of Practice*[118] in 2018 is an example of proactive standard-setting. The draft acknowledges gait analysis limitations and provides recommended methodology to improve consistency. Such codes, while not law, would likely be considered by courts in weighing expert evidence: an expert who did not follow the code might be deemed less credible.

On the legislative side, the UK does not yet have an AI-specific law, but data protection law imposes constraints on automated processing, especially if it produces legal effects which identification and risk scores arguably do.[119] There's also an ongoing push for algorithmic transparency in the public sector: The UK Equality and Human Rights Commission in 2020 warned that biased algorithms in policing could breach the Equality Act.[120]

---

116 Hunton Andrews Kurth LLP, "UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in *Bridges* v. *South Wales Police*" *Privacy and Information Security Law Blog*, Aug. 11, 2020, *available at:* https://www.hunton.com/privacy-and-information-security-law/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police (last visited on Mar. 09, 2025).

117 *Ibid.*

118 United Kingdom, Forensic Science Regulator, *Forensic Gait Analysis: Consultation Draft*, 2018, available at: https://assets.publishing.service.gov.uk/media/5b3500d140f0b60b48621ced/2018_Forensic_Gait_Analysis_Consultation_Draft.pdf (last visited on Feb. 9, 2025).

119 United Kingdom, *Data Protection Act*, 2018 (2018 c.12), read with the *United Kingdom General Data Protection Regulation (UK GDPR).*

120 Equality and Human Rights Commission, *Civil and Political Rights in Great Britain*, March 2020, available at: https://www.equalityhumanrights.com/sites/default/files/2021/civil-and-political-rights-in-great-britain-march-2020.pdf(last visited on Mar. 9, 2025).

In criminal trials, UK law has traditionally relied on the discretion of judges to exclude evidence if its admission would have an adverse effect on fairness.[121] So, if an AI identification was obtained through methods that make the trial unfair a judge could exclude it under that provision. While no reported case yet shows such an exclusion specifically for an algorithmic match, the mechanism exists and could be invoked similarly to how evidence from an improperly conducted identification parade is thrown out.

Additionally, British courts have an interesting approach to expert evidence reliability after *R* v. *Luttrell*[122] and some subsequent cases, they allow novel expert evidence if the field is sufficiently well-developed and the expert is qualified.[123] If one tried to introduce, say, a novel AI algorithm's result through an expert, the court might consider if the technique has achieved recognition in its field. If not, the judge could refuse to admit it as lacking foundation.

XI Human rights and emerging AI regulations in the European Union

The EU as a whole, through the European Court of Human Rights (*hereinafter,* "ECtHR") and EU institutions, provides a broader rights-based perspective. While criminal procedure is largely national, the European Convention on Human Rights (*hereinafter,* "ECHR") influences standards. Article 6 of ECHR guarantees fair trial,[124] and article 8 guarantees privacy.[125] ECtHR jurisprudence (*S. and Marper* v. *UK*[126] on DNA databases, *Big Brother Watch* v. *UK*[127] on surveillance) emphasizes that surveillance technologies must have strict controls to prevent rights violations. If an AI tool leads to unfairness like one side cannot challenge evidence, or it encroaches privacy without oversight, an accused could in theory appeal to the ECtHR after domestic remedies, claiming violation of article 6 or 8. This external check means European countries tread carefully; for instance, France's highest administrative court in 2020 sets as illegal any drone equipped with camera and flying low enough, as such a drone would allow the police to detect individuals by their clothing or a distinctive sign – signalling that even beneficial tech can be illegal without safeguards.[128]

---

121 *Police and Criminal Evidence Act*, 1984 (1984 c. 60), s. 78.

122 *R* v. *Luttrell*, [2004] EWCA Crim 1344 (CA).

123 *Atkin* v. *Atkin*, [2005] EWCA Civ 1241.

124 The European Convention on Human Rights, 1950, art. 6.

125 *Id.,* art. 8.

126 *S. and Marper* v. *United Kingdom*, [2008] ECHR 1581.

127 *Big Brother Watch* v. *United Kingdom*, [2021] ECHR 581.

128 European Digital Rights (EDRi), "France: First Victory Against Police Drones" *EDRi*, May 26, 2020, *available at:* https://edri.org/our-work/france-first-victory-against-police-drones/ (last visited on Mar. 9, 2025).

The EU has also enacted the AI Act, a regulation that classifies AI systems by risk and impose requirements.[129] Notably, *real-time remote biometric identification systems* are slated to be banned in principle in public spaces, with narrow exceptions for serious crimes and even that with safeguards. This means that, across the EU, police use of facial recognition might be heavily curtailed or standardized by law. For forensic AI tools that are not outright banned, the AI Act will require things like transparency to users, accuracy standards, and accountability. For example, if predictive policing software is considered "high-risk" (likely, since it affects fundamental rights), providers will have to ensure a certain level of explainability and bias testing.[130] Over time, these regulatory standards could indirectly set a bar for admissibility – a defense lawyer in say Germany could point out that a tool wasn't certified under the AI Act compliance procedures, hence it's not reliable enough.

Comparatively, the EU's approach is more pre-emptive regulation, whereas the US/UK rely on courts. But all point towards a consensus that transparency and oversight are key.

One illustrative European example – The Netherlands had implemented a system called SyRI (*hereinafter,* "System Risk Indication") to detect welfare fraud using algorithms.[131] In 2020, a Dutch Court struck it down as violating privacy and the right to equal treatment because it was too opaque and intrusive.[132] While that was a civil context, it demonstrates judicial scepticism of inscrutable algorithmic government tools, emphasizing that rule of law requires intelligibility and proportionality. For criminal justice, one can expect similar reasoning – an EU judge might say if a person is convicted based significantly on an algorithm's output that the person or even the judge cannot comprehend, that undermines the fairness of the process.

International human rights bodies like the UN Human Rights Council have also weighed in. A report by the UN High Commissioner for Human Rights urged a moratorium on use of AI that poses serious risks to human rights (specifically naming facial recognition) until adequate safeguards are in place.[133] Though not binding, this reflects a cautious global attitude.

---

129 *Artificial Intelligence Act*, 2024, Regulation (EU).

130 *Supra* note 35.

131 District Court of The Hague (Netherlands), *NJCM* v. *Netherlands*, ECLI:NL:RBDHA:2020:1878, Judgment of Feb. 5, 2020, *available at:* https://www.escr-net.org/wp-content/uploads/2020/09/ecli_nl_rbdha_2020_1878.pdf (last visited on Mar. 9, 2025).

132 *Ibid.*

133 United Nations Human Rights Council, *Report of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age*, U.N. Doc. A/HRC/51/17 (Sept. 12, 2022), *available at:* https://docs.un.org/en/A/HRC/51/17 (last visited on Mar. 9, 2025).

XII Policy recommendations and reforms

In light of the above analysis, it is clear that India's legal framework needs to evolve to safely integrate AI into forensic processes while upholding constitutional values. The BSA 2023 and the BNSS 2023 presents a timely opportunity to incorporate specific provisions or interpretative guidelines addressing algorithmic evidence. We offer the following policy recommendations aimed at legislators, judicial authorities, and law enforcement agencies:

Amend the BSA 2023 to codify reliability safeguards

Introduce a provision (or an explanation to the relevant sections on expert evidence) explicitly requiring courts to ascertain the scientific validity of any AI-based forensic technique before relying on it. This could mirror the Daubert factors: requiring that the proponent of the evidence demonstrate the tool's error rate, whether it has been independently validated, and that it is generally accepted in the scientific community. For example, a new illustration to Section 45 could be added: *"(Illustration) A proposes to introduce a facial recognition match report to identify Z as the culprit. The court should consider the reliability of the facial recognition system used, including its known accuracy and potential biases, before such opinion can be given weight."* While judges can do this under inherent powers, codification will ensure consistency.

Statutory obligation of algorithmic transparency

The Parliament should consider an amendment to the BNSS or an adjunct law that when prosecution seeks to use evidence generated by an algorithm, the source code or detailed technical information such as developmental methodology, training data characteristics, error rates, bias assessments, must be disclosed to the court and made available to the defense. Provisions can protect sensitive information by allowing in camera inspections or protective orders, but the defense should have the right to get an independent expert analyse the algorithm. Without such disclosure, the evidence should be presumptively inadmissible due to violating fair trial rights.

Independent testing and certification of forensic AI tools

The government should establish a body or empower the existing NCRB/BPRD or a new Forensic Science Regulator role to test and certify AI tools used in criminal justice. Before a facial recognition software or predictive policing algorithm is deployed by police, it should undergo evaluation on Indian demographic data to gauge accuracy across different communities. Certification results (pass/fail, accuracy metrics) should be published. Courts could then take judicial notice if a tool is certified or not. Using non-certified tools in collecting evidence should be discouraged, or if used, their outputs treated with caution. This is akin to how Breathalyzer models in drunken driving cases often must be approved by labs.

Judicial training and guidelines

The Supreme Court, perhaps *via* the e-committee or a special bench should formulate practice directions on handling digital evidence from AI systems. Judges at trial and appellate level need to be literate in basic AI concepts like false positives, training data bias, overfitting, *etc.* The National Judicial Academy can include courses on this. Moreover, the Supreme Court could draw from comparisons to craft guidelines similar to the guidelines laid for DNA evidence in some jurisdictions emphasizing that whenever AI evidence is presented, judges must ensure the accused had opportunity to challenge it and that they record reasons why they find it reliable (or not). This will promote higher scrutiny uniformly.

Reforming line-up and identification procedures

Just as there are detailed rules for conducting an identification parade for suspects, there should be standard operating procedures (*hereinafter,* "SOPs") for using facial recognition in investigations. For instance, if a system throws up a match, it should be verified through human examiners and perhaps a second algorithm before action is taken. The SOP should mandate that an FRT match alone can never be the sole basis of arrest or charge – it must be treated as an intelligence lead to be corroborated. These SOPs can be issued by the Ministry of Home Affairs to police forces, and courts should insist on compliance. Much like non-compliance with arrest memorandum requirements can cast doubt on prosecution.

XIII Strengthen expert evidence provisions in BNSS

The BNSS could incorporate a procedure akin to a *pre-trial evidentiary hearing* for complex scientific evidence. On defense application, courts could hold a "*voir dire*" on algorithmic evidence where experts from both sides testify on its reliability and the judge decides if it can be considered. Although India mostly has bench trials, such a procedure ensures the issues are thrashed out transparently. BNSS already allows courts to summon experts or seek reports; this can be expanded to technical referees to help understand novel evidence.

Ensuring equality and non-discrimination

The legislature should explicitly include in the BSA and special laws that evidence obtained or processed in a manner that is consciously or unconsciously discriminatory is inadmissible as it offends public policy similar to evidence obtained by inducement is disallowed. Short of a statute, courts can use article 14 to similar effect, but a statute would put police on notice that bias means no usable evidence. Additionally, investigative agencies should be required to conduct and submit "Algorithmic Impact Assessments" for any AI tool they use, which includes an evaluation of potential bias outcomes and steps taken to mitigate them. This mirrors the equality impact assessment concept from Bridges[134] and would align with fundamental rights by design.

134 *Supra* note 67.

Data protection and privacy compliance

Any deployment of AI for surveillance or evidence should comply with data protection principles. It would be prudent for the Data Protection Board of India (once constituted under the new DPDP Act)[135] to issue a code of practice for law enforcement use of AI, mandating minimal data retention, purpose limitation (*e.g.*, facial recognition data of innocents must be deleted promptly), and breach notification if misidentifications occur. If police violate these and collect evidence, that could be a basis for exclusion under a strengthened right to privacy framework.

Legislating use-specific laws

In the absence of a comprehensive policy, a targeted law regulating facial recognition by law enforcement could be enacted like some United States jurisdictions have. It should define when it can be used, require prior authorization, set accuracy benchmarks, and enforce audit logs for each use to later review if it was valid. It should also give individuals a remedy if they were falsely implicated by FRT – such as the right to obtain information on whether FRT was used on them and to challenge wrongful matches.

Promote algorithmic diversity and local databases

From a policy perspective, to reduce bias, the government should invest in creating diverse Indian training datasets for algorithms with proper ethical collection so that tools trained on Indian faces or crime data perform better for all groups. Reliance on foreign-trained models has been problematic.[136] Collaboration with Indian research institutes to develop transparent AI forensics where source code can be open or auditable would decrease the black box issue. Such home-grown solutions could be more easily scrutinized in court.

Exclude or minimize use of high-risk AI

Echoing the EU's approach, the most risk-prone AI applications like purely predictive policing that identifies individuals should perhaps be prohibited or heavily restricted. The police can use AI to predict places or times for preventive patrolling with oversight, but generating lists of "persons likely to commit crime" should be banned as it is too reminiscent of colonial preventive detention abuses and cannot be squared with the presumption of innocence. A policy decision could be taken to that effect by the Ministry of Home Affairs, and courts should frown upon any evidence stemming solely from such predictions (as fruit of a poisonous tree, so to speak).

Continuous judicial oversight committees

Establish a standing committee under the National Human Rights Commission or a special Parliamentary committee to monitor law enforcement AI use. This body could

135 Digital Personal Data Protection Act, 2023, s. 18.

136 Karishma Mehrotra, *supra* note 5.

periodically review systems for bias and recommend suspension if issues arise, acting as a watchdog that keeps executive enthusiasm in check with rights concerns.

Implementing these recommendations would require concerted effort but would significantly bolster the accountability and fairness around forensic AI. They aim to fill the gaps in our current laws that, as we saw, do not explicitly account for the distinct challenges posed by algorithms. Ultimately, the goal is not to reject technology's assistance in law enforcement, but to embed it within a robust legal and ethical framework so that increases in efficiency do not come at the cost of justice or constitutional rights.

XIV Conclusion

The march of technology in the form of AI-driven forensic tools is transforming the landscape of criminal investigation and adjudication in India. As we have explored, innovations like facial recognition, predictive policing, and gait analysis carry great promise for bolstering law enforcement capabilities, yet they also harbour the peril of entrenching biases and undermining fundamental rights if left unchecked. The legal system stands at a critical juncture: it must craft doctrines and rules now to govern these technologies, rather than retroactively responding to injustices after they occur.

Under the BSA, 2023 and the BNSS, 2023, India has the opportunity to usher its evidentiary and procedural law into the digital age. This requires recognizing that an algorithm's imprimatur does not automatically equate to truth – courts must interrogate the reliability of AI evidence just as rigorously as they would a human expert's credentials or a witness's testimony. In fact, greater rigor is warranted, given the obscurity and complexity that often shroud algorithmic processes. Our analysis of constitutional principles – equality, due process, fair trial, privacy makes it evident that blindly accepting AI outputs can violate the very pillars of justice. Article 14 demands that technology not be a new gateway for discrimination; Article 21 demands that no person lose liberty on the basis of unchallengeable or unjust evidence. The Indian judiciary's past decisions, from *Maneka Gandhi* to *Selvi* to *Puttaswamy*, all emphasize that fairness and reason must temper even the most well-intentioned state action.

Comparative experiences urge India to be proactive. The United States has taught us the value of reliability standards and defense access to algorithmic evidence.[137] The UK has highlighted the need for clear legal frameworks and the risks of overlooking bias.[138] European norms underscore that some high-risk uses of AI simply have no place in a rights-respecting society absent stringent controls. Rather than viewing these as obstacles, India should treat them as a roadmap for responsible AI integration.

137 *Supra* note 104.

138 *Supra* note 67; *Supra* note 114.

In practical terms, this means investing in robust oversight: independent certification of tools, judicial training, and perhaps most importantly, legislative foresight to amend laws in step with technological advancement. Policy recommendations outlined herein, such as mandating transparency and bias audits, are not anti-technology they are pro-justice. They will help ensure that when an AI tool points the finger, it does so justifiably, and that the courts and defendants can examine that pointing finger from all angles.

The challenge of algorithmic bias is essentially to prevent historical prejudices from being repackaged in futuristic form. If a facial recognition system disproportionately misidentifies members of a certain community, it resurrects the spectre of that community being unfairly targeted only now with a veneer of scientific objectivity. The law's role is to peel back that veneer. By imposing legal standards for admissibility that factor in accuracy and fairness, courts can filter out the noise of unreliable technology, admitting only evidence that genuinely assists in ascertaining truth.

As India implements the BSA and BNSS, a clear message should be sent that the criminal justice system is not a testing ground for unproven gadgets, especially not at the expense of individual rights. Instead, it will embrace useful AI tools on its own terms i.e. the terms defined by the Constitution and principles of justice. With thoughtful reforms, India can strike the delicate balance between innovation and rights. The power of forensic AI can be harnessed to deliver justice more efficiently, while steadfastly guarding against the infusion of bias and error. In doing so, Indian law will reaffirm an age-old tenet in the new age: the ends of justice are best served when advanced technology is coupled with advanced safeguards.