INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE IN FORENSIC INVESTIGATION: LEGAL AND ETHICAL CHALLENGES IN INDIA

AUTHORED BY - RAJDEEP MALIK
Course: LL.B Semester IV
College: Bareilly College, Bareilly U.P.
Affiliation: Mahatma Jyotiba Phule Rohilkhand Universit, Bareilly, U.P.

Abstract

Artificial intelligence is entering forensic investigation while India is remaking criminal justice around electronic records, digital proceedings, forensic collection, and technology-enabled policing. AI can help investigators sort digital evidence, compare faces and voices, detect cyber patterns, and reduce laboratory delay. Yet the same systems may be inaccurate, biased, opaque, excessive, or trained on data that should not have been collected. This paper argues that India should treat forensic AI as a high-risk criminal justice technology. The Bharatiya Sakshya Adhiniyam, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, and constitutional doctrine on privacy and self-incrimination provide a foundation, but not a complete regime. The core issue is not whether AI may assist investigation. It is how AI can be used without weakening legality, dignity, fairness, transparency, and the presumption of innocence.

Key words: Artificial intelligence; forensic investigation; electronic evidence; Bharatiya Sakshya Adhiniyam; privacy; self-incrimination; facial recognition; algorithmic bias; India; criminal justice.

Introduction

Forensic investigation has always depended on the tools of its time. Fingerprints, DNA profiling, call detail records, CCTV footage, mobile extraction, and cyber forensics each changed how crime is investigated and proved. Artificial intelligence adds a sharper shift because it does not merely store evidence. It classifies, compares, ranks, infers, and recommends. It may help an analyst locate files in a seized laptop, match faces across video

ISSN: 2582-6433

feeds, isolate a voice from noisy audio, flag manipulated media, read number plates, or connect scattered online activity.

The Indian context makes the debate urgent. The new criminal laws place electronic and digital records at the centre of investigation and trial. The Bharatiya Sakshya Adhiniyam, 2023 recognises electronic and digital records as documents and gives them legal effect subject to the conditions for admissibility of electronic records[1]. The Bharatiya Nagarik Suraksha Sanhita, 2023 contemplates electronic communication, audio-video recording of search and seizure, electronic-mode proceedings, and forensic collection in serious offences[2]. Official government material describes the reform as an attempt to digitise the process from FIR to case diary, charge-sheet, trial, and judgment, while also expanding the category of documents to include emails, server logs, smartphones, websites, locational evidence, and messages stored on devices[3].

These changes create a fertile environment for forensic AI. Once police stations, laboratories, prosecutors, and courts handle more digital material, automated tools become attractive. The difficulty is that criminal law is a rights-sensitive field where error has human consequences. A false facial-recognition match may bring an innocent person into the criminal process. A biased tool may push investigators toward already over-policed communities. An opaque model may influence an expert report without allowing meaningful cross-examination. The central research question is therefore: what legal and ethical standards should govern AI-assisted forensic investigation in India?

Scope and Methodology

This paper uses doctrinal legal research and policy analysis. It studies Indian constitutional principles, evidence law, criminal procedure, data protection, and technology policy to evaluate how AI can be integrated into forensic investigation. It focuses on legal and ethical challenges rather than technical design alone.

[1] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 2(d), 2(e), 57, 61, 63, India Code (enforced July 1, 2024), https://www.indiacode.nic.in/handle/123456789/20063; see also Section 63, India Code, https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00049_2023-47_1719292804654&orderno=63

[2] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (enforced July 1, 2024), https://www.indiacode.nic.in/handle/123456789/21615.

[3] Press Information Bureau, Union Home Minister and Minister of Cooperation, Shri Amit Shah Introduces the Bhartiya Nyaya Sanhita Bill 2023, the Bharatiya Nagarik Suraksha Sanhita Bill, 2023 and the Bharatiya Sakshya Bill, 2023 in the Lok Sabha (Aug. 11, 2023), https://pib.gov.in/PressReleasePage.aspx?PRID=1947941.

ISSN: 2582-6433

The paper uses the expression "forensic AI" broadly. It includes machine-learning and automated decision-support systems used to collect, process, compare, interpret, or present evidence in a criminal investigation. This includes AI-supported digital forensics, facial recognition, voice comparison, image enhancement, deepfake detection, predictive triage of seized devices, biometric comparison, and automated pattern analysis. The term does not mean that AI itself is a legal witness. In Indian criminal process, the relevant legal question remains whether the output can be proved through lawful collection, proper custody, valid certification, expert explanation, and fair testing in court.

AI and the Changing Nature of Forensic Investigation

Traditional forensic science often examines a physical trace: a fingerprint, bloodstain, bullet mark, handwriting sample, or chemical residue. Modern investigation increasingly examines data trails. Phones record location, apps preserve chats, servers generate logs, cameras capture movement, and social media produces metadata. AI matters because this volume is too large for manual review alone. A single smartphone may contain years of messages, images, browsing history, deleted files, app databases, and cloud records. AI can reduce search time by clustering files, recognising objects, transcribing speech, detecting anomalies, and prioritising material for human review.

This usefulness should not be dismissed. Delay in forensic examination can weaken prosecution and defence alike. Victims may wait for trial, accused persons may remain under suspicion, and courts may face technical evidence without adequate expert assistance. NITI Aayog's national AI strategy frames India's AI ambition around "AI for All," inclusive growth, human capability, and solutions to access, affordability, and shortage of expertise[4]. Those goals are relevant to forensic science, where expertise and infrastructure are uneven across states.

But forensic AI differs from many ordinary administrative uses of AI. The harm from error is severe. A person wrongly identified by a machine may be arrested before the mistake is discovered. A probabilistic match score may be treated as conclusive proof. AI therefore must not become an invisible shortcut from suspicion to guilt. It should remain an investigative aid requiring validation, human judgment, and legal scrutiny.

[4] NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll 4, 12, 16, 75 (2018), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

ISSN: 2582-6433

Indian Legal Framework

Electronic Evidence Under the Bharatiya Sakshya Adhiniyam

The Bharatiya Sakshya Adhiniyam, 2023 is the starting point because most AI outputs will be derived from electronic or digital records. The statute defines "document" to include electronic and digital records and defines evidence to include such records produced for court inspection[5]. Section 61 states that electronic or digital records cannot be denied admissibility merely because of their digital form, while section 63 sets conditions for admissibility[6]. The BPRD ready reckoner explains that the BSA places electronic and digital evidence on equal footing with traditional documentation, subject to section 63[7].

The older Supreme Court doctrine under section 65B of the Indian Evidence Act, 1872 remains highly instructive. In Anvar P.V. v. P.K. Basheer, the Court held that electronic records by way of secondary evidence must satisfy the special certificate requirement and cannot be proved through general oral evidence when the statutory conditions apply[8]. In Shafhi Mohammad v. State of Himachal Pradesh, the Court softened that requirement where the party seeking to rely on electronic evidence was not in possession of the device[9]. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, a larger bench restored the centrality of the certificate and clarified the procedure for electronic evidence[10]. Together, these cases show that Indian evidence law is cautious about electronic material because authenticity, integrity, and source matter.

AI complicates this framework. A section 63 certificate can speak to the production of a computer output, the device, ordinary use, and proper functioning. It may not explain the model architecture, training data, error rate, validation study, confidence score, or limits of an AI-generated conclusion. If an AI tool says that two faces are likely the same person, the court needs a route to examine reliability, input quality, error rates, population validation, and independent human assessment.

---

[5] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 2(d), 2(e), India Code, https://www.indiacode.nic.in/handle/123456789/20063.

[6] Id. §§ 61, 63; Section 63, India Code, https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00049_2023-47_1719292804654&orderno=63.

[7] Bureau of Police Research & Development, Ready Reckoner Highlighting the Use of Technology in New Criminal Laws 34 to 43 (2024), https://bprd.nic.in/uploads/pdf/20240129040422119463 4UseofTechnology.pdf.

[8] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473, https://aphc.gov.in/docs/imp_judgements/Anvar%20PV%20case.pdf.

[9] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 S.C.C. 801, https://narcoticsindia.nic.in/Judgments/Shafhi_Mohammad_vs_The_State_Of_Himachal_Pradesh_on_30_January_2018.pdf.

[10] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1, https://digiscr.sci.gov.in/admin/judgement_file/judgement_pdf/2020/volume%207/Part%20I/Arjun%20Panditrao%20Khotkar%20_%20Kailash%20Kushanrao%20Gorantyal%20And%20Ors._1701334263.pdf.

ISSN: 2582-6433

Criminal Procedure and Technology-Enabled Investigation

The BNSS deepens the role of technology in criminal process. Government materials state that the new framework contemplates e-FIR, electronic service, digital proceedings, audio-video recording, and forensic examination in serious offences[11]. The BPRD ready reckoner identifies provisions for audio-video recording of search and seizure, production of communication devices likely to contain digital evidence, electronic police reports, electronic supply of documents, and electronic-mode proceedings[12] . These provisions can improve transparency and chain of custody if implemented carefully.

At the same time, digitisation increases sensitive data in state custody. A search of a phone or cloud account may reveal far more than the alleged offence, including intimate communications, medical data, political opinions, photographs, contacts, location history, and privileged material. AI can make the intrusion deeper because it rapidly searches, classifies, and infers. Investigative necessity must therefore be applied more strictly when AI is used to mine personal data.

Privacy, Data Protection, and State Power

The constitutional foundation is Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench unanimously recognised privacy as a fundamental right under Article 21 and Part III of the Constitution[13]. Puttaswamy does not make privacy absolute. It allows lawful restrictions, but those restrictions must satisfy legality, legitimate state aim, necessity, and proportionality. Criminal investigation is undoubtedly a legitimate state aim, yet proportionality requires more than invoking public safety. The state must show legal authority, rational connection, minimal intrusion, and safeguards against abuse.

The Digital Personal Data Protection Act, 2023 adds a statutory privacy layer for digital personal data. India Code describes it as recognising both the right of individuals to protect personal data and the need to process such data for lawful purposes[14]. Forensic AI must respect that balance. Investigators may have lawful grounds to process data for crime investigation, but broad retention of biometric databases, training datasets, or extracted device images can exceed the moral limits of investigation.

[11] Press Information Bureau, supra note 3.
[12] Bureau of Police Research & Development, supra note 7, at 10 to 31
[13] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1; Supreme Court Observer, Fundamental Right to Privacy, https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/.
[14] Digital Personal Data Protection Act, No. 22 of 2023, India Code (Aug. 11, 2023), https://www.indiacode.nic.in/handle/123456789/22037?locale=en

ISSN: 2582-6433

The Information Technology Act, 2000 is also relevant because it gives legal recognition to electronic records and electronic signatures, defines electronic records, and establishes the background legal architecture for digital authentication[15]. It does not regulate forensic AI as such. The gap is that AI-generated forensic inferences require standards beyond the legal validity of electronic records.

Self-Incrimination and Scientific Techniques

AI-based forensic investigation may intersect with Article 20(3), which protects an accused from being compelled to be a witness against himself. The Supreme Court has long distinguished between testimonial compulsion and physical or identifying material. In State of Bombay v. Kathi Kalu Oghad, the Court held that giving fingerprints, handwriting, or specimen signatures is not the same as giving testimonial evidence based on personal knowledge[16]. In Ritesh Sinha v. State of Uttar Pradesh, the Court held that a Magistrate may order a person to provide a voice sample for investigation, while recognising that statutory clarity was needed[17]. However, Selvi v. State of Karnataka draws an important constitutional line. The Court held that involuntary narcoanalysis, polygraph examination, and brain electrical activation profile tests violate personal liberty and protection against self-incrimination, and that even voluntary results are not automatically admissible as evidence[18]. Selvi matters for AI because scientific language cannot override autonomy. If a technology extracts or infers mental content, behavioural vulnerability, or intimate identity information, courts should ask whether it resembles physical identification or testimonial intrusion.

Major Legal Challenges

Admissibility and Probative Value

The first challenge is admissibility. Indian law can admit electronic records if statutory conditions are met, but AI outputs require a second question: what is their probative value? A court may admit an AI-assisted report and still give it little weight if the system is unvalidated, poorly explained, or applied to low-quality input. A facial-recognition match from blurred

[15] Information Technology Act, No. 21 of 2000, §§ 2(t), 3, 3A, 4, 5, 7, India Code, https://www.indiacode.nic.in/handle/123456789/1999.
[16] State of Bombay v. Kathi Kalu Oghad, A.I.R. 1961 S.C. 1808, https://juris-codex.com/supreme-court/1961/the-state-of-bombay-v-kathi-kalu-oghad-and-others.html.
[17] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 S.C.C. 1, https://api.sci.gov.in/pdfdate/index1.php?filename=supremecourt%2F2010%2F27352%2F27352_2010_1_1501_15521_Judgement_02-Aug-2019.pdf&dno=273522010&dt=2019-08-02.
[18] Selvi v. State of Karnataka, (2010) 7 S.C.C. 263, https://api.sci.gov.in/jonew/judis/36303.pdf.

ISSN: 2582-6433

CCTV footage should not be treated like a clean fingerprint. The court must ask what the algorithm measured, how similar the inputs were, what the false positive rate is, and whether a human examiner reviewed the result.

This distinction between admissibility and weight should be made explicit. AI should not be excluded merely because it is AI, just as electronic evidence is not excluded merely because it is electronic. But the party relying on AI-assisted evidence should disclose enough information for the opposing party and the court to test reliability. At minimum, the record should include the tool used, version, input data, preprocessing steps, output, confidence score, human review notes, audit logs, known limitations, and chain of custody.

Chain of Custody and Integrity

Forensic AI depends on the integrity of both input and process. If the seized device is not properly imaged, metadata is altered, files are uploaded without logging, or the AI tool modifies an image while enhancing it, the evidentiary chain weakens. The BPRD ready reckoner recognises the need for safe storage and transfer of electronic evidence and warns against leakage, deletion, corruption, alteration, modification, or transposition of digital records[19]. This is especially important where tools are cloud-based or vendor-operated.

The best practice should be forensic reproducibility. A defence expert should be able, where legally appropriate, to examine the same input and understand how the output was generated. If exact reproduction is impossible because the model is proprietary or has changed, the evidence should be treated cautiously. Criminal justice cannot rest on a black box that says "trust me."

Algorithmic Opacity and Cross-Examination

The right to cross-examine is weakened when neither the witness nor the investigator can explain the system. NITI Aayog's responsible AI paper expressly identifies transparency as a principle and notes that deep learning systems may become opaque, creating the "black box" problem[20]. In criminal trials, opacity is not only an engineering issue. It is a rule-of-law issue. An accused person must be able to challenge the evidence against him. If the state relies on an AI output but refuses meaningful disclosure on grounds of trade secrecy or security, courts must balance confidentiality against the right to a fair trial.

[19] Bureau of Police Research & Development, supra note 7, at 41 to 43.
[20] NITI Aayog, Responsible AI: Principles for Responsible AI 41 to 48 (Feb. 2021), https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf.

ISSN: 2582-6433

This does not always require full source-code disclosure. Courts can use layered disclosure: model documentation, validation summaries, independent audit reports, test performance, error rates, and expert testimony. In high-stakes cases, in camera review or court-appointed technical experts may be appropriate. The core principle is simple: no forensic conclusion should become decisive if the accused cannot reasonably test it.

Privacy and Surveillance

Facial recognition is the clearest privacy problem. Project Panoptic records 170 installed FRT systems, 118 RTIs filed, and a total financial outlay of ₹1,513.26 crore; it also notes that facial recognition is not 100% accurate and may cause false positives and false negatives[21]. When such systems are used for investigation, they can shift from targeted forensic comparison to mass surveillance. Comparing a suspect's face with footage from a particular crime scene is one thing. Scanning crowds, protests, railway stations, or public databases to generate suspects is far more intrusive.

The Puttaswamy proportionality test should govern such use. Law enforcement should have clear statutory authority, a defined purpose, limited retention, independent oversight, and remedies for wrongful identification. Mere administrative convenience cannot justify continuous biometric surveillance. Privacy is not the enemy of investigation. It is the condition that keeps investigation within constitutional boundaries.

Bias and Discrimination

AI systems learn from data, and data often reflects social inequalities. If a facial-recognition system is trained mainly on some demographic groups, it may perform worse on others. If historical policing data reflects disproportionate surveillance of communities, predictive or patterning tools may reproduce that imbalance. NITI Aayog's responsible AI principles expressly include equality, inclusivity, and non-discrimination, and warn that AI can amplify unfair bias at scale[22].

In India, bias must be understood through local realities: caste, religion, gender, region, language, class, disability, and uneven access to documentation. A model that works well in a laboratory may fail in a crowded street with poor lighting, low-resolution footage, and diverse appearances. Ethical forensic AI therefore requires India-specific validation.

[21] Project Panoptic, Panoptic FRT Tracker, https://panoptic.in/
[22] NITI Aayog, supra note 20, at 29 to 40.

ISSN: 2582-6433

Accountability and Vendor Dependence

Forensic AI often involves private vendors. This creates a "many hands" problem: the police collect data, a vendor processes it, an expert interprets it, a prosecutor presents it, and a judge evaluates it. If the system fails, responsibility can become diffuse. NITI Aayog identifies accountability as a responsible AI principle and recognises this difficulty[23].

Indian criminal justice needs clear allocation of responsibility. Police agencies should remain accountable for the lawful collection and use of evidence. Vendors should be contractually bound to validation, security, audit cooperation, confidentiality, and non-reuse of forensic data. Experts should not merely repeat tool outputs; they should explain methodology and limitations. Courts should insist that the prosecution identify every material step in the AI-assisted evidentiary process.

Ethical Challenges

The ethical problem with forensic AI is not that machines are always worse than humans. Human investigators can also be biased or careless. The problem is that AI can give old errors a new appearance of scientific certainty. A computer-generated score can look objective even when built on poor data. A "match" can sound final even when it is only a probability. Ethical use therefore requires humility.

Human oversight is necessary but not sufficient. A human officer who simply accepts the machine's recommendation is not exercising meaningful judgment. Oversight must be competent, documented, and independent. The human reviewer must know what the system can and cannot do. The reviewer should record why the AI output was accepted, rejected, or treated as inconclusive. In serious cases, AI should trigger further investigation, not replace it.

Consent and dignity also matter. In forensic contexts, consent is often complicated because the individual faces state authority. A person asked to provide a biometric sample or device password may not feel free to refuse. Selvi's insistence on autonomy in the context of scientific techniques should influence AI governance. Even where compulsion is legally permitted, the process should be bounded by necessity, judicial authorisation, and safeguards against humiliation or fishing expeditions.

[23] Id. at 49 to 55.

ISSN: 2582-6433

There is also an ethical duty to protect victims and witnesses. AI tools used for image analysis, sexual offence investigations, child sexual abuse material detection, or voice and face comparison may process intensely sensitive data. Leakage can cause a second injury. Forensic laboratories and police units need strict access controls, encryption, deletion schedules, and penalties for misuse.

Recommendations

India should adopt a risk-based legal framework for AI in forensic investigation. It should classify forensic AI as high-risk and require pre-deployment validation, India-specific bias testing, cybersecurity review, documentation, auditability, and approval by an independent technical-legal body.

Second, evidence law should develop explicit standards for AI-generated or AI-assisted evidence. Section 63 of the BSA is necessary but not enough. Courts should require disclosure of model identity, version, purpose, input quality, confidence score, limitations, validation data, and human review. Where the AI system is proprietary, courts should use protective orders or independent experts rather than accepting secrecy as a complete answer.

Third, police and forensic laboratories should adopt standard operating procedures for AI tools. These SOPs should cover lawful acquisition of data, imaging, hashing, secure upload, access logs, cloud processing, retention, deletion, expert review, and reporting language. Reports should avoid overstating conclusions and should state similarity level, comparison conditions, system limits, and corroboration.

Fourth, privacy safeguards should be built into procurement. No police agency should purchase or deploy forensic AI without clauses on data minimisation, non-retention by vendors, prohibition on secondary use, localisation where necessary, breach reporting, audit rights, and deletion after the lawful purpose ends. Public procurement should not become a back door for permanent biometric databases.

Fifth, courts should strengthen defence access to technical evidence. Fair trial requires that the accused can challenge not only the final report but the method behind it. Legal aid systems may also need technical forensic support, because AI evidence will otherwise deepen inequality between the state and the defence.

ISSN: 2582-6433

Finally, India should invest in public forensic capacity. Dependence on opaque private tools can weaken sovereignty, accountability, and trust. Public laboratories, universities, and forensic science institutions should develop validated tools, open benchmarks, and training modules for judges, prosecutors, defence lawyers, police, and forensic scientists. AI should help build a more reliable justice system, not merely a more automated one.

Conclusion

Artificial intelligence can improve forensic investigation in India, but only if it is governed as a constitutional technology. The new criminal laws recognise the centrality of electronic records and digital process. India's AI policy recognises safety, equality, privacy, transparency, accountability, and human values. Supreme Court doctrine recognises privacy, limits coercive scientific techniques, and insists on careful proof of electronic evidence. These principles already point toward a balanced model.

The future of forensic AI should not be framed as a choice between innovation and rights. A system that produces unreliable, biased, or unchallengeable evidence is not innovative in any meaningful legal sense. It is a threat to justice. The proper aim is responsible forensic intelligence: tools that assist investigators, respect privacy, preserve human dignity, disclose their limits, and remain answerable in court. In India, where criminal justice reform and digital transformation are moving together, this is the moment to set those standards. If law waits until wrongful arrests and wrongful convictions expose the weaknesses, the cost will be paid by individuals whose liberty cannot be restored by a software update.

Reference

1. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 2(d), 2(e), 57, 61, 63, India Code (enforced July 1, 2024), see also Section 63, India Code.
2. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (enforced July 1, 2024).
3. Press Information Bureau, Union Home Minister and Minister of Cooperation, Shri Amit Shah Introduces the Bhartiya Nyaya Sanhita Bill 2023, the Bharatiya Nagarik Suraksha Sanhita Bill, 2023 and the Bharatiya Sakshya Bill, 2023 in the Lok Sabha (Aug. 11, 2023).
4. NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll 4, 12, 16, 75 (2018).
5. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 2(d), 2(e), India Code.
6. Id. §§ 61, 63; Section 63, India Code.
7. Bureau of Police Research & Development, Ready Reckoner Highlighting the Use of Technology in New Criminal Laws 34 to 43 (2024).

ISSN: 2582-6433

8. Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473.
9. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 S.C.C. 801.
10. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1.
11. Press Information Bureau, supra note 3.
12. Bureau of Police Research & Development, supra note 7, at 10 to 31.
13. Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1; Supreme Court Observer, Fundamental Right to Privacy. 14. Digital Personal Data Protection Act, No. 22 of 2023, India Code (Aug. 11, 2023).
14. Information Technology Act, No. 21 of 2000, §§ 2(t), 3, 3A, 4, 5, 7, India Code.
15. State of Bombay v. Kathi Kalu Oghad, A.I.R. 1961 S.C. 1808.
16. Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 S.C.C. 1.
17. Selvi v. State of Karnataka, (2010) 7 S.C.C. 263.
18. Bureau of Police Research & Development, supra note 7, at 41 to 43.
19. NITI Aayog, Responsible AI: Principles for Responsible AI 41 to 48 (Feb. 2021).
20. Project Panoptic, Panoptic FRT Tracker.
21. NITI Aayog, supra note 20, at 29 to 40.
22. Id. at 49 to 55.