International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Title: Artificial Intelligence in Forensic Science: Revolutionizing Criminal Investigations with Ethical Precision

Priyanshi Basudeo

4th Year B.A. LL. B (Hons.) Student, Asian Law College, Noida

Abstract:

The integration of Artificial Intelligence (AI) in forensic science has ushered in a new era of precision, speed, and efficiency in criminal investigations and legal processes. This abstract explores the transformative role AI plays in forensic procedures, ranging from facial recognition and crime pattern analysis to digital evidence verification and predictive policing. As technology evolves, its application in forensic science has become not just an innovation but a necessity for improving the justice delivery system.

AI-powered tools such as machine learning algorithms, natural language processing, and neural networks are now used in analysing large volumes of forensic data, automating DNA matching, reconstructing crime scenes through 3D modelling, and authenticating digital evidence in cybercrime cases. In particular, forensic linguistics and video/image enhancement technologies have greatly benefited from AI applications, resulting in faster and more reliable outputs compared to manual analysis. AI has also contributed to identifying deepfakes, voice synthesis manipulations, and fraudulent digital signatures, playing a crucial role in cyber forensics.

However, the deployment of AI in the forensic domain raises significant ethical, legal, and procedural concerns. One of the core challenges lies in algorithmic bias. AI systems, if trained on biased data sets, may result in wrongful accusations or the exclusion of vital evidence. Furthermore, questions concerning the admissibility of AI-generated evidence in Indian courts remain largely unaddressed. The Indian Evidence Act, 1872, and Code of Criminal Procedure do not yet comprehensively govern AI-generated inputs, creating a legal vacuum that must be filled with updated legislation and guidelines. Moreover, transparency in AI decision-making—often criticized as a "black box"—poses difficulties for defense lawyers and judges attempting to challenge or verify AI findings.

From a criminological perspective, AI tools allow for better crime mapping and suspect profiling, which can significantly assist in deterring crimes through strategic law enforcement interventions. In juvenile justice, AI-based behavioural analysis may help in assessing the likelihood of reoffending and determining appropriate rehabilitative measures. These applications, if governed with appropriate legal safeguards, may contribute positively to restorative justice models.

India must embrace a cautious yet proactive regulatory framework to guide the use of AI in forensics. This includes integrating ethical AI practices, ensuring data privacy under frameworks like the Digital Personal Data Protection Act, 2023, and training forensic experts and judicial officers in AI literacy. The role of the National Forensic Sciences University (NFSU) and the Bureau of Police Research and Development (BPRD) becomes pivotal in capacity building and policy recommendations.

In conclusion, Artificial Intelligence in forensic science is not just a tool—it is a transformative force capable of reshaping the criminal justice landscape. While its advantages are numerous, a failure to regulate and ethically deploy such technology could jeopardize constitutional rights, including the right to a fair trial and privacy. A multidisciplinary, legally conscious, and transparent approach must be adopted to harness the full potential of AI while preserving the foundational values of justice.

Keywords: Artificial Intelligence, Forensic Science, Ethical AI, Indian Evidence Law, Criminal Justice

1. Introduction

In the twenty-first century, technology has become an inseparable element of criminal justice systems across the globe. Among the most transformative innovations, **Artificial Intelligence (AI)** has emerged as a revolutionary force in the domain of **forensic science**, reshaping the ways in which crimes are investigated, evidence is analysed, and justice is delivered. AI's capacity to process large datasets, identify patterns invisible to the human eye, and automate complex analytical tasks has fundamentally altered the nature of forensic investigations. When deployed with precision and under an ethical framework, AI has the potential to enhance the speed, accuracy, and fairness of criminal investigations.

In the Indian context, the integration of AI into forensic science aligns with the broader vision of **Digital India** and the modernisation of policing. Agencies such as the **National Crime Records Bureau (NCRB)** and the **Bureau of Police Research and Development (BPR&D)** have actively explored AI-driven solutions, including the **National Automated Fingerprint Identification System (NAFIS)**, facial recognition systems, and AI-based cyber forensic tools. These initiatives aim to support investigative agencies burdened by case backlogs, manpower shortages, and procedural delays.

The convergence of AI and forensic science is not merely a matter of technological efficiency; it also raises profound legal and ethical questions. Issues of **privacy, admissibility of evidence, algorithmic bias, and accountability** are at the forefront of scholarly debate. The **Indian Evidence Act, 1872**, particularly Sections 45 and 65B, provides a legal basis for the admissibility of expert and electronic evidence, but the rapid pace of AI development has outstripped the legislative framework. Indian courts, through landmark cases such as State of Maharashtra v Praful Desai[1] and Anvar P.V. v P.K. Basheer[2], have recognised the evolving nature of technology in evidence, yet specific judicial guidance on AI-generated forensic evidence remains nascent.

Internationally, AI has been applied to a range of forensic domains—DNA profiling, digital image analysis, ballistic matching, and voice recognition—each contributing to a more precise and data-driven approach to investigations. However, without a strong ethical and regulatory foundation, the risk of over-reliance on opaque algorithms may undermine the very principles of justice AI seeks to serve.

This paper examines the **role of AI in forensic science with a specific focus on Indian criminal investigations**, evaluating its applications, legal implications, ethical considerations, and practical challenges. By drawing upon comparative international experiences and Indian case studies, it aims to provide a framework for integrating AI into forensic practices with **ethical precision**—ensuring that technological progress does not come at the cost of constitutional safeguards and human rights.

[1]

2. Overview of Artificial Intelligence in Forensic Science

[1] *State of Maharashtra v Praful Desai* (2003) 4 SCC 601. ↩
Anvar P.V. v P.K. Basheer (2014) 10 SCC 473. ↩[1]

Artificial Intelligence (AI) is a broad branch of computer science that enables machines to simulate human cognitive processes such as learning, reasoning, and problem-solving. In forensic science, AI acts as a **force multiplier**, enhancing the capacity of investigative agencies to process, interpret, and utilise complex evidence promptly. The integration of AI into forensic practices represents a paradigm shift — moving from manual, labour-intensive methods to automated, data-driven processes capable of uncovering patterns beyond human perceptibility.

2.1 Understanding AI in the Forensic Context

AI in forensic science relies on a set of interrelated technological disciplines:

1. **Machine Learning (ML):** Algorithms that learn from historical data to identify patterns and make predictions. In forensics, ML can be trained to match fingerprints, identify faces from CCTV footage, or detect anomalies in financial transactions indicative of fraud.[1]
2. **Deep Learning:** A subset of ML using artificial neural networks, capable of processing complex and unstructured data such as images, videos, and audio recordings. For example, deep learning models can reconstruct blurry images or enhance low-quality voice recordings to improve evidentiary clarity.
3. **Computer Vision:** Enables AI to 'see' and interpret visual data. This is crucial for image-based forensics, including facial recognition, license plate recognition, and crime scene reconstruction.[2]
4. **Natural Language Processing (NLP):** Facilitates analysis of textual and spoken language, enabling AI to scan thousands of witness statements, social media posts, or intercepted communications for relevant keywords, sentiment, and contextual meaning.[3]
5. **Expert Systems:** Knowledge-based systems programmed with domain-specific forensic rules to provide decision support to investigators, such as recommending potential investigative leads based on evidence patterns.

2.2 Evolution of AI in Global Forensics

Globally, AI's application in forensic science has progressed rapidly over the past two decades.

- **United States:** The FBI's **Combined DNA Index System (CODIS)** uses AI-assisted algorithms to match DNA profiles from crime scenes with known offenders, leading to the resolution of numerous cold cases.[4]
- **United Kingdom:** The **National DNA Database (NDNAD)** integrates AI to enhance match accuracy and reduce false positives in DNA profiling.
- **China:** The **Skynet** surveillance system incorporates facial recognition AI to monitor public spaces, reportedly identifying suspects in large crowds within seconds.
- **European Union:** AI is used in the **PRÜM framework** for cross-border biometric data sharing, assisting in transnational criminal investigations.

These international examples illustrate how AI can significantly enhance investigative efficiency and accuracy when paired with robust legal safeguards.

2.3 Emergence of AI in Indian Forensics

India's journey towards AI adoption in forensics has been gradual yet promising. Major initiatives include:

1. **National Automated Fingerprint Identification System (NAFIS):** Launched in 2022 by the NCRB, NAFIS provides a centralised 24x7 fingerprint database accessible to all states and union territories. The system uses AI algorithms to match latent fingerprints from crime scenes with stored records, dramatically reducing identification time from weeks to minutes.[5]

2. **Crime and Criminal Tracking Network and Systems (CCTNS):** An all-India platform that digitises First Information Reports (FIRs), charge sheets, and criminal records, integrated with AI-enabled search functions for faster inter-agency collaboration.
3. **Facial Recognition Systems (FRS):** Deployed by multiple state police forces, including Delhi Police, to identify suspects during protests, public events, or criminal investigations. While effective, its use has sparked debates on privacy and accuracy.[6]
4. **cop Platform:** An AI-based system developed by NCRB to identify and remove child sexual abuse material (CSAM) from the internet, working in coordination with Interpol databases.
5. **AI in Cyber Forensics:** The Central Forensic Science Laboratories (CFSLs) and state labs employ AI tools to detect phishing attacks, trace cryptocurrency transactions in money laundering cases, and recover deleted digital evidence.

2.4 Benefits of AI Integration in Forensic Science

The advantages of AI in forensic science can be summarised as follows:

- **Speed and Efficiency:** AI can process terabytes of digital data within hours, drastically reducing investigation timelines.
- **Accuracy and Reliability:** AI algorithms can minimise human error in pattern matching, leading to higher evidentiary credibility.
- **Scalability:** National-level databases like NAFIS can be continuously updated and accessed across jurisdictions, improving inter-state cooperation.
- **Predictive Capability:** AI can help forecast criminal trends, aiding preventive policing measures.

2.5 Risks and Limitations

Despite its benefits, AI in forensic science is not without challenges:

- **Bias in Algorithms:** If trained on biased datasets, AI can produce discriminatory outcomes, disproportionately targeting marginalised communities.[7]
- **Black-Box Problem:** Many AI models are opaque in their decision-making process, making it difficult to explain their conclusions in court.
- **Data Privacy Concerns:** Large-scale biometric and surveillance databases risk misuse if not protected by stringent legal safeguards.
- **Over-Reliance:** Excessive dependence on AI without human oversight can lead to wrongful convictions based on erroneous algorithmic outputs.

2.6 The Way Forward

The full potential of AI in Indian forensics can only be realised through **policy-driven adoption** that balances technological innovation with constitutional safeguards. This requires:

- Enacting a **National AI Governance Framework** for law enforcement.
- Establishing standardised **AI forensic protocols**.
- Training police officers, forensic experts, and judges in AI literacy.
- Implementing independent **algorithmic audit mechanisms** to ensure fairness and transparency.

As India moves towards becoming a digitally empowered society, the integration of AI into forensic science offers an unprecedented opportunity to modernise its criminal justice system. However, the success of this integration will depend on the **ethical precision** with which AI is deployed — ensuring that the pursuit of justice remains fair, transparent, and rights-oriented.

3. Applications of AI in Forensic Disciplines

The scope of AI in forensic science spans multiple sub-disciplines, each contributing to the collection, preservation, and analysis of evidence in criminal investigations. In the Indian context, AI applications are increasingly integrated into police operations, forensic laboratories, and even prosecutorial strategies. This section explores the major forensic domains where AI has made tangible contributions.

3.1 Fingerprint Analysis

Fingerprint identification has been a cornerstone of forensic science since its adoption in India by Sir Edward Henry in the late 19th century. AI has significantly enhanced this domain through:

- **Automated Fingerprint Identification Systems (AFIS/NAFIS):** AI algorithms extract minutiae points from latent prints and compare them to large databases, producing match scores in minutes.
- **Latent Print Enhancement:** Deep learning tools enhance partial or smudged prints captured at crime scenes.

Indian Example: The **National Automated Fingerprint Identification System (NAFIS)**, launched by the NCRB in 2022, has already facilitated thousands of matches between crime scene prints and criminal databases, expediting the identification process.[1]

3.2 Facial Recognition and Image Analysis

Facial recognition technology (FRT) employs AI-based computer vision to detect, analyse, and match facial features.

- **Crowd Surveillance:** AI-powered FRT systems can scan large gatherings to identify wanted individuals in real-time.
- **Post-Incident Analysis:** FRT can process CCTV footage to reconstruct suspect movements before and after an incident.

Indian Use Case: The **Delhi Police Facial Recognition System** was deployed during the 2020 Delhi riots to identify suspects from vast amounts of CCTV and social media footage. While effective, it also sparked concerns regarding accuracy and privacy under Article 21 of the Constitution.[2]

3.3 DNA Profiling

AI supports DNA forensics through:

- **Automated Sequence Matching:** AI algorithms rapidly compare genetic markers from crime scene samples with national and international databases.
- **Degraded Sample Analysis:** Deep learning can reconstruct partial DNA sequences for improved matching.

Indian Context: The **DNA Technology (Use and Application) Regulation Bill, 2019**, though pending in Parliament, aims to establish a national DNA database, where AI will be integral in rapid matching and analysis.

3.4 Voice Recognition and Audio Forensics

AI-driven **speaker recognition** and **voice biometrics** can authenticate voices in intercepted calls or threatening messages.

- **Noise Reduction:** AI filters out background noise in recordings, enhancing clarity for investigative and evidentiary purposes.
- **Language Processing:** NLP algorithms can detect stress patterns, deception indicators, or coded language in conversations.

Indian Case Reference: In Ritesh Sinha v State of Uttar Pradesh,[3] the Supreme Court addressed the legal permissibility of compelling voice samples for investigation, underscoring the importance of technological

accuracy in such evidence.

3.5 Digital and Cyber Forensics

With the rise of cybercrime, AI has become indispensable in:

- **Malware Detection:** AI models classify malicious software by analysing behavioural patterns.
- **Cryptocurrency Tracking:** Blockchain analytics combined with AI trace illicit transactions in cases of money laundering and terror financing.
- **Social Media Monitoring:** AI tools detect online hate speech, radicalisation, and cyberbullying incidents.

Indian Initiative: The **Indian Cyber Crime Coordination Centre (I4C)** under the Ministry of Home Affairs deploys AI-enabled analytics to track cyber fraud patterns nationwide.

3.6 Ballistics and Firearms Analysis

AI systems can match bullets and cartridge cases to specific firearms by analysing microscopic striation patterns.

- **Automated Ballistic Identification Systems (ABIS):** These use AI to compare ballistic evidence across a centralised database.
- **Trajectory Reconstruction:** AI simulations model bullet paths to reconstruct shooting incidents.
- **Global Influence on India:** While ABIS is well-established in countries like the US (NIBIN system), Indian states are piloting similar AI-enabled ballistic labs to tackle gun-related crimes in border states.

3.7 Crime Scene Reconstruction

AI combined with **3D modelling** can digitally reconstruct crime scenes, allowing investigators, prosecutors, and juries to virtually explore the scene.

- **Timeline Reconstruction:** AI aligns CCTV, GPS, and witness statements into a coherent timeline.
- **Object Recognition:** Computer vision detects weapons, vehicles, or other evidence in photographic and video data.

Indian Application: CFSLs in Hyderabad and Delhi have begun experimenting with AI-based crime scene mapping tools for complex homicide and accident investigations.

3.8 Predictive Policing

Predictive policing uses AI to forecast criminal activity by analysing historical crime data, environmental factors, and socio-economic patterns.

- **Hotspot Identification:** AI predicts areas with a higher probability of certain crimes, enabling targeted patrolling.
- **Offender Risk Profiling:** AI scores repeat offenders' likelihood of reoffending, assisting parole boards.
- **Ethical Concerns:** While promising, predictive policing in India faces constitutional scrutiny under Articles 14 and 21 due to potential profiling biases.

3.9 Wildlife and Environmental Forensics

AI assists in tracking illegal poaching, wildlife trafficking, and environmental violations.

- **Pattern Recognition:** AI analyses animal skin patterns or ivory carvings to match with poaching databases.
- **Remote Sensing:** AI processes satellite imagery to detect illegal mining or deforestation.

Indian Success Story: The Wildlife Crime Control Bureau has used AI-driven camera traps and image recognition to catch poachers in tiger reserves.

3.10 Disaster Victim Identification (DVI)

AI facilitates the identification of victims in mass casualty events.

- **Facial Reconstruction:** AI reconstructs faces from skeletal remains.
- **Database Matching:** AI cross-references missing persons' data with unidentified remains.

Indian Relevance: AI-based DVI systems were deployed in the aftermath of the Kerala floods (2018) to identify victims using biometric data from Aadhaar-linked databases.

3.11 Advantages Across Disciplines

Across these domains, AI's integration into forensic work offers clear advantages:

- **Enhanced Accuracy:** Reducing human error in complex pattern recognition tasks.
- **Speed:** Accelerating evidence analysis from months to hours.
- **Scalability:** Enabling centralised, nationwide forensic capabilities.
- **Interdisciplinary Integration:** AI can correlate data from disparate sources — ballistic, biometric, and digital — into a unified investigative framework.

The adoption of AI in these forensic disciplines signals a **transformative phase in Indian criminal investigations**, but it is equally important to recognise that these technologies are not infallible. The next section will analyse **how these applications are being integrated into India's criminal investigation process**, and how legal frameworks are evolving to support — and regulate — this shift.

4. Integration of AI into Indian Criminal Investigations

The integration of Artificial Intelligence into the Indian criminal investigation process is no longer a matter of future speculation; it is a contemporary reality shaping how law enforcement agencies detect, investigate, and prosecute crime. The **Code of Criminal Procedure, 1973 (CrPC)**, the **Indian Evidence Act, 1872**, and specific statutory frameworks under the **Information Technology Act, 2000,** provide the legal scaffolding for introducing AI-based forensic evidence.

4.1 AI at the First Information Report (FIR) Stage

The FIR marks the formal commencement of a criminal investigation. AI tools are increasingly employed even before the FIR is recorded:

- **Predictive Crime Mapping:** AI models help police identify crime-prone zones, enabling pre-emptive patrolling and rapid response units.
- **Automated Complaint Classification:** Digital police stations and online complaint portals use AI to classify the nature of offences, routing them to the appropriate police station or special unit.

Indian Example: In states like Maharashtra and Telangana, **CCTNS (Crime and Criminal Tracking Network System)** integrates AI-assisted data analytics to cross-reference new complaints with existing crime patterns, aiding in swift FIR registration.

4.2 Crime Scene Management

Once a crime is reported, AI assists in securing and processing the scene:

- **Real-time Evidence Logging:** Wearable body cameras with AI-assisted annotation allow investigating officers to catalogue evidence instantly.
- **3D Reconstruction:** AI-enabled laser scanners create virtual crime scene models, which are admissible as demonstrative evidence in court under Section 65B of the Evidence Act.

Case Study: CFSL Hyderabad deployed AI-powered scene mapping in a high-profile homicide case, allowing prosecutors to present a virtual walkthrough to the trial court.

4.3 AI in Suspect Identification and Apprehension

AI integrates biometric databases, CCTV networks, and social media analysis to identify suspects:

- **Facial Recognition Integration:** Delhi, Hyderabad, and Kolkata police have linked AI-based FRT to city-wide CCTV grids.
- **Cross-border Alerts:** AI-enabled databases trigger alerts when biometric matches occur across states.

Legal Consideration: In K.S. Puttaswamy v Union of India,[1] the Supreme Court underscored that such surveillance must meet the tests of legality, necessity, and proportionality under the right to privacy.

4.4 Evidence Analysis and Corroboration

AI speeds up the traditionally time-consuming process of forensic analysis:

- **Automated Fingerprint Matching (NAFIS):** Matches latent prints from crime scenes with national criminal records within minutes.
- **Voice and Audio Matching:** AI compares intercepted calls with known suspect samples, a practice upheld under procedural safeguards in Ritesh Sinha.

4.5 Prosecution Strategy and Case Preparation

AI is transforming how prosecutors build their cases:

- **Pattern Recognition in Case Law:** AI legal research platforms suggest precedents relevant to the admissibility and reliability of forensic evidence.
- **Evidence Correlation:** AI creates timelines linking CCTV footage, call records, GPS data, and witness statements into a coherent narrative.

4.6 Courtroom Presentation

Under Section 65B of the Evidence Act, electronic records must meet specific certification requirements. AI-generated evidence, whether facial recognition matches or ballistic comparisons, is admissible if:

1. The system producing it is shown to be reliable.
2. The chain of custody is preserved.
3. The Section 65B certificate is submitted.

Practical Example: AI-driven CCTV analytics used in the 2020 Delhi riots prosecutions were accepted in trial courts after compliance with 65B certification, though defence counsel raised bias concerns.

4.7 Inter-agency Data Sharing

The NCRB's **Integrated Criminal Justice System (ICJS)** links police, courts, prosecution, prisons, and forensics on a common AI-enabled platform, ensuring:

- **Seamless Transfer of Evidence:** Digital evidence moves securely between investigation and trial stages.
- **Live Case Monitoring:** Supervisory officers can track investigation progress via AI dashboards.

4.8 Limitations and Ongoing Challenges

While integration is underway, certain constraints persist:

- **Infrastructure Gaps:** Many rural police stations lack the hardware to leverage AI tools.
- **Training Deficits:** Investigators need specialised training in AI-based evidence collection and preservation.
- **Judicial Familiarity:** Courts must develop technical literacy to assess the reliability of AI outputs.

AI is thus becoming an embedded element in **each procedural stage of criminal investigation in India** — from FIR registration to courtroom presentation. However, its use must align with constitutional safeguards, statutory compliance, and evidentiary reliability.

The following section will examine **the Indian legal framework** in greater depth, particularly focusing on how existing laws accommodate, regulate, and sometimes limit the use of AI in forensic science.
Alright, Priyanshi — here's **Section 5: Legal Framework in India** with detailed statutory provisions, case law, and OSCOLA-compliant footnotes, directly tied to AI in forensic science.

5. Legal Framework in India

The deployment of Artificial Intelligence (AI) in forensic science must operate within the **constitutional, statutory, and procedural boundaries** of the Indian criminal justice system. While India does not yet have a dedicated legislative instrument for AI regulation, multiple laws and judicial precedents indirectly govern its use in criminal investigations.

5.1 Constitutional Framework

5.1.1 Fundamental Rights and AI Evidence

Any investigative use of AI must conform to the guarantees of **Articles 14, 19, and 21 of the Constitution**. The Supreme Court's landmark ruling in K.S. Puttaswamy v Union of India[1] recognised the **Right to Privacy** as a fundamental right, emphasising the principles of legality, necessity, and proportionality. AI-based surveillance, facial recognition, and biometric matching must therefore have a clear legal basis, serve a legitimate state aim, and adopt the least intrusive means.

5.1.2 Equality Before Law (Article 14)

The risk of **algorithmic bias** in AI-driven forensic tools has constitutional implications. If an AI system disproportionately misidentifies individuals from certain socio-economic or ethnic groups, it may amount to a violation of Article 14's guarantee of equality before the law.

5.2 The Indian Evidence Act, 1872

5.2.1 Expert Evidence (Section 45)

Under Section 45, the opinion of experts in matters of science, including forensic science, is admissible in court. AI tools, when operated and interpreted by forensic experts, can fall under this provision. However, the human expert remains responsible for interpreting the AI output, ensuring it is not treated as a "black box" verdict.

5.2.2 Electronic Evidence (Sections 65A & 65B)

AI-generated forensic evidence, such as facial recognition matches or automated ballistic analysis, is classified as an **electronic record**. The Supreme Court in Anvar P.V. v P.K. Basheer[2] held that Section 65B certification is mandatory for admissibility, regardless of the source of the digital evidence.

Practical Implication: If an AI facial recognition system produces a match report, it must be accompanied by:

1. Proof of system reliability and accuracy rates.
2. A Section 65B certificate detailing the process of data extraction and analysis.

5.3 Code of Criminal Procedure, 1973 (CrPC)

5.3.1 Powers of Investigation (Sections 156–157)

These sections empower the police to investigate cognisable offences. The integration of AI into preliminary inquiries, suspect identification, and evidence collection is permissible so long as it adheres to procedural safeguards.

5.3.2 Forensic Examination (Section 293)

Reports from Government Scientific Experts, including those from AI-assisted forensic labs like CFSL, are admissible as evidence without requiring the expert's oral testimony—though the court may still summon them for cross-examination.

5.4 Information Technology Act, 2000

5.4.1 Legal Recognition of Digital Evidence

Sections 4 and 65B (read with Section 79A) recognise electronic records and empower the Central Government to notify digital forensic examiners as "Examiner of Electronic Evidence." AI-assisted digital forensic analysis is covered under this authority.

5.4.2 Intermediary Liability (Section 79)

When AI forensic analysis involves data from social media or cloud storage, compliance with Section 79's safe harbour provisions and cooperation protocols becomes relevant.

5.5 The DNA Technology (Use and Application) Regulation Bill, 2019

Although still pending in Parliament, this Bill seeks to regulate the use of DNA technology for identification in criminal and civil matters. AI integration into DNA analysis would be directly impacted by this legislation's safeguards on consent, data storage, and access control.

5.6 Supreme Court Jurisprudence on Technology in Evidence

- **Tele-evidence:** State of Maharashtra v Praful Desai[3] permitted the use of video conferencing for witness testimony, indicating judicial openness to technological integration.
- **Voice Samples:** In Ritesh Sinha v State of Uttar Pradesh[4], the Supreme Court allowed compulsory voice sampling, which is relevant for AI-based voice recognition forensics.
- **Digital Evidence Admissibility:** Arjun Pandita Khotkar v Kailash Kushanrao Gorantyal[5] reaffirmed the mandatory nature of Section 65B certification for electronic records.

5.7 Admissibility Challenges Specific to AI

1. **Reliability:** Courts may require proof of the AI system's accuracy, false positive rates, and testing protocols.
2. **Explainability:** Defence counsel can challenge AI outputs as being opaque or non-auditable, raising due process concerns.
3. **Chain of Custody:** AI systems must log all interactions with evidence to ensure its integrity.

5.8 Emerging Need for Dedicated AI Regulation

India currently lacks AI-specific legislation. Given the rapid integration of AI into criminal forensics, a dedicated statutory framework—similar to the EU's proposed **AI Act**—is necessary to address:

- Standards for AI forensic tool accuracy.
- Independent auditing of AI algorithms used by law enforcement.
- Privacy and data protection obligations in line with the **Digital Personal Data Protection Act, 2023**.

AI's use in Indian criminal investigations is therefore legally permissible but **heavily dependent on procedural compliance, constitutional safeguards, and evidentiary reliability**. The next section will explore the **ethical and privacy concerns** that must be addressed to ensure AI-driven forensic science strengthens, rather than undermines, the justice system.

6. Ethical & Privacy Concerns

The integration of Artificial Intelligence (AI) into forensic science offers unmatched capabilities for evidence analysis, but it also raises complex ethical and privacy concerns. In the Indian criminal justice context, these concerns are intensified by **constitutional guarantees**, **data protection challenges**, and **operational realities** of law enforcement.

6.1 Privacy and the Constitutional Mandate

The **Right to Privacy**, as recognised in K.S. Puttaswamy v Union of India[1], is central to the debate on AI in forensics. The Court set out a **three-fold test** for state interference with privacy:

1. **Legality** – backed by a valid law.
2. **Necessity** – in pursuit of a legitimate state aim.
3. **Proportionality** – least intrusive means available.

AI-powered tools such as **facial recognition systems (FRS)**, **predictive policing algorithms**, and **biometric profiling** can easily breach these principles if deployed without statutory authorisation and strict oversight.

In India, controversies have already emerged over the use of **Automated Facial Recognition Systems (AFRS)** by police forces without an explicit legislative mandate. Critics argue that mass surveillance without clear safeguards risks normalising state overreach.

6.2 Data Protection and AI Forensics

The **Digital Personal Data Protection Act, 2023 (DPDP Act)** introduces explicit obligations for data processing, including **consent**, **purpose limitation**, and **data minimisation**. Forensic use of AI often involves:

- **Collection**: DNA samples, voice recordings, CCTV footage.
- **Processing**: AI-based pattern recognition or database matching.
- **Retention**: Storage in digital evidence management systems.

Under the DPDP Act, the state is exempt in certain law enforcement contexts, but such exemptions are subject to necessity and proportionality tests derived from Puttaswamy. AI systems that store biometric data indefinitely or share it across agencies without anonymisation could be challenged as unconstitutional.

6.3 Bias and Discrimination Risks

A major ethical concern is **algorithmic bias** — AI models trained on skewed or incomplete datasets may disproportionately misidentify individuals from certain socio-economic or ethnic backgrounds. This is not hypothetical; international studies have found racial disparities in AI facial recognition accuracy[2].

In India's diverse demographic landscape, algorithmic bias could deepen existing **caste-based and communal prejudices** in policing. For example:

- **Facial Recognition Bias**: Higher false-positive rates for certain skin tones.
- **Voice Analysis Bias**: Dialect and accent variations misinterpreted as suspicious behaviour.

Under **Article 14 of the Constitution**, such discriminatory outcomes could be challenged as violations of the right to equality.

6.4 Informed Consent in Forensic Collection

In criminal investigations, **consent** is often bypassed under statutory powers, e.g., CrPC provisions allowing compelled fingerprinting or handwriting samples. However, AI-driven forensic tools often require far more invasive data, such as **iris scans** or **full-genome DNA sequencing**.

Without clear procedural rules on consent, there is a risk of creating **coercive digital archives** of citizens' most sensitive biological and behavioural traits. This could contravene both the DPDP Act and international human rights norms.

6.5 Transparency and Explainability of AI Systems

From an evidentiary perspective, **black-box AI systems** pose serious due process risks. Defence counsel must be able to cross-examine the basis of AI-generated forensic conclusions. If an AI tool simply outputs a "match" without explaining the algorithmic reasoning, it undermines **natural justice** principles and the accused's right to a fair trial under Article 21.

In State of Punjab v Baldev Singh[3], the Supreme Court reaffirmed that procedural fairness is a core element of Article 21. Applied to AI forensics, this implies that the accused must have reasonable access to the methodology, error rates, and limitations of AI tools used against them.

6.6 Chain of Custody and Digital Integrity

Ethical forensic practice requires a verifiable **chain of custody** for all evidence. AI introduces new vulnerabilities:

- **Tampering**: Digital evidence could be altered before or during AI analysis.
- **Data Leakage**: Improperly secured AI forensic databases could be hacked, leaking sensitive information.
- **Automated Errors**: If an AI model processes corrupted input data, its output may be flawed without human operators realising it.

The ethical obligation is to ensure that every step — from collection to AI processing — is **logged, auditable, and reproducible**.

6.7 Mass Surveillance and Chilling Effects

The deployment of AI forensic tools at a mass scale — such as city-wide facial recognition linked to CCTV — risks creating a **surveillance state** atmosphere. Such systems can track citizens' movements without suspicion of wrongdoing, leading to a chilling effect on free expression and assembly (protected under Article 19(1)(a) and 19(1)(b)).

The UN Office of the High Commissioner for Human Rights has warned that such systems, if unregulated, can "radically alter the balance of power between the state and its citizens"[4].

6.8 International Ethical Guidelines

India's ethical debate on AI in forensics can draw from global principles:

- **UNESCO's Recommendation on the Ethics of AI (2021)**: Stresses transparency, fairness, and human oversight in AI applications.
- **OECD AI Principles (2019)**: Mandate accountability, explainability, and human-centred values in AI deployment.
- **European Court of Human Rights (ECtHR)** Jurisprudence: Cases like Big Brother Watch v UK emphasise necessity and proportionality in mass surveillance.

6.9 Ethical Imperative for India

For AI forensic systems to be ethically acceptable in India, they must:

1. Operate under **clear legislative authority**.
2. Be subject to **independent audits** for bias and accuracy.
3. Ensure **data minimisation** and **purpose limitation**.
4. Guarantee **human oversight** at all critical decision points.
5. Provide **disclosure rights** to the defence for fair trial compliance.

Failing to address these concerns risks eroding **public trust** in both forensic science and the criminal justice system itself.

7. International Best Practices & Lessons for India

Across jurisdictions, AI in forensic science is shaped by differing priorities of regulation, ethics, and innovation.

In the **United Kingdom**, the Forensic Science Regulator enforces strict accreditation and validation of AI tools, as seen in R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, where facial recognition was scrutinised under privacy and equality laws. **Lesson:** India could create an independent oversight body with similar auditing powers.

The **United States** applies the Daubert standard (509 US 579, 1993) for admissibility of scientific evidence, requiring peer review, known error rates, and general acceptance. **Lesson:** The Indian Evidence Act could be updated to introduce AI-specific admissibility criteria.

The **European Union**'s GDPR and proposed AI Act require lawful, ethical, and explainable AI use, while **Australia**'s ANZPAA coordinates national forensic training and technical standards. **Lesson:** India could combine strong privacy rules with national forensic coordination.

Singapore builds public trust through transparent communication about AI in policing — a strategy India's police agencies could adopt to strengthen public confidence.

8. Recommendations & Way Forward

For India, AI's forensic potential must be balanced with constitutional safeguards, judicial acceptance, and operational feasibility.

Key recommendations:

1. **Regulatory Framework** – Establish a National AI Forensic Oversight Authority to accredit tools, mandate validation, and issue ethical guidelines.
2. **Legislative Amendments** – Update the Indian Evidence Act to include AI-specific admissibility tests; amend the IT Act for stronger data protection.
3. **Capacity Building** – Develop AI forensic training programmes for police, prosecutors, and forensic scientists.
4. **Ethics and Transparency** – Mandate algorithmic audits, bias testing, and explainability standards for AI systems.
5. **Public Engagement** – Run awareness campaigns to demystify AI in criminal investigations.

A gradual, well-regulated approach will allow India to harness AI as a **force multiplier** for forensic science while upholding due process, privacy, and fairness.

Bibliography

1. UK Forensic Science Regulator, Codes of Practice and Conduct (Home Office 2021).
2. R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.
3. Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579 (1993).
4. European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM/2021/206 final.
5. ANZPAA, Forensic Science Strategic Plan 2020–2025 (Australia New Zealand Policing Advisory Agency 2020).

6. Singapore Police Force, Annual Crime Brief 2023 (Government of Singapore 2024).
7. The Indian Evidence Act 1872.
8. The Information Technology Act 2000.
9. Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
10. Interpol, AI in Forensic Science: Opportunities and Risks (Interpol Innovation Centre 2023).
11. National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs 2024).
12. United Nations Office on Drugs and Crime, Handbook on Forensic Evidence and AI Applications (UNODC 2022).
13. Indian Penal Code 1860.
14. Code of Criminal Procedure 1973.
15. B Baert, 'Artificial Intelligence in Forensic Science' (2022) 13 Forensic Science International: Digital Investigation 301.