

A study on the 'Role of Artificial Intelligence in Police Investigation under the New Criminal Laws

Samriti

Assistant Professor, Vivekananda School of Law and Legal Studies, Vivekanand Institute of Professional Studies-Technical Campus, Delhi.

ABSTRACT

The enactment of India's new criminal legislations—the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Bharatiya Sakshya Adhiniyam (BSA)—marks a paradigm shift toward a technology-driven, forensics-first criminal justice system. Central to this reform is the imperative for law enforcement to leverage advanced digital tools, elevate electronic records to primary evidence, and mandate forensic involvement in serious offenses. This study examines the evolving role of Artificial Intelligence (AI) in police investigations within this new legal framework. It analyzes key applications, including AI-driven predictive policing, automated facial recognition systems (AFRS), deep learning in digital forensics, and algorithmic pattern recognition in crime analytics. While these tools offer unprecedented efficiency, faster case resolution, and enhanced lead generation, their adoption exposes critical legal and operational challenges. The findings emphasize that while BNSS and BSA implicitly pave the way for AI-assisted investigations, the existing evidentiary regime requires statutory standardization, algorithmic auditing, and human-in-the-loop oversight to ensure reliability. The paper concludes by proposing a risk-based regulatory framework to balance AI innovation in policing with constitutional guarantees of due process and public trust.

Keywords: Artificial Intelligence, Police Investigation, Bharatiya Nagarik Suraksha Sanhita (BNSS), Bharatiya Sakshya Adhiniyam (BSA), Predictive Policing, Digital Forensics.

Received 26.04.2026

Revised 20.05.2026

Accepted 20.06.2026

CITATION OF THIS ARTICLE

Samriti. A study on the 'Role of Artificial Intelligence in Police Investigation under the New Criminal Laws. Inter. J. Edu. Res. Technol. 17[2] June 2026; 01-06.

INTRODUCTION

The landscape of modern criminal justice is undergoing a structural shift. Historically, police investigations relied heavily on human intuition, localized intelligence networks, and the painstaking manual review of physical evidence. However, the digital explosion of the 21st century has drastically changed the nature of crime. Today, a single investigation can generate terabytes of data, from smartphone locations and encrypted messaging logs to hours of high-definition body camera and closed-circuit television (CCTV) footage. Faced with severe staffing shortages and an unprecedented volume of information, law enforcement agencies have integrated Artificial Intelligence (AI) into their core investigative workflows. AI acts as an algorithmic force multiplier, altering how evidence is analyzed, patterns are recognized, and resources are deployed. Yet, this technological revolution is a double-edged sword; as AI accelerates the pursuit of justice, it simultaneously introduces profound legal, ethical, and systemic risks.

Focusing an academic study specifically on police investigation under the new criminal laws requires analyzing how Artificial Intelligence transitions from a theoretical administrative tool to an active field agent and primary investigator's aid. With the operationalization of the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA), Indian policing has formally entered a "Smart Policing" paradigm. State police forces are already deploying specialized AI tools (such as the UP Police's *Trinetra 2.0*, Delhi Police's *CMAPS*, and Gujarat Police's *NARIT-AI*) to bridge the gap between technological capabilities and procedural mandates. In a very recent defamation suit involving obscene, AI-generated social media posts targeting a politician. Justice Subramonium Prasad drew a sharp line between protected political satire and malicious AI deployment. The Court declared that while AI is increasingly used for political expression, courts have a binding duty to ensure that AI-

generated deepfakes, morphed images, or manipulated videos do not violate an individual's fundamental Right to Dignity.¹

A public figure approached the Delhi High Court seeking protection against online actors generating pornographic material, fake endorsements, and unauthorized merchandise using their likeness. Building upon the landmark *Anil Kapoor (2023)* precedent, the Delhi High Court granted broad injunctions specifically barring the unauthorized commercial or personal exploitation of a celebrity's name, image, voice, or likeness via Generative AI, Machine Learning, face-morphing tools, and deepfakes.² Policing technology is evolving rapidly because organized crime is weaponizing AI. Modern syndicates use large language models to rapidly create malware, deploy deepfake audio/video to bypass biometric security, and generate synthetic identities for financial fraud. To maintain operational capability, law enforcement must use advanced AI tools to detect and counter these sophisticated digital threats.

Core application of AI in Indian Policing

In the Indian context, the deployment of Artificial Intelligence (AI) in police investigations and the broader criminal justice system is expanding rapidly. Law enforcement is transitioning from legacy manual or isolated digital archives into a highly interconnected, data-driven ecosystem. However, this shift faces acute scrutiny due to the lack of dedicated AI legislation and the need to align technologies with constitutional rights. National Database Integration: AI is being integrated into foundational databases like the Crime and Criminal Tracking Network Systems (CCTNS) and the Interoperable Criminal Justice System (ICJS) to seamlessly track criminal records across state borders. Surveillance & Video Analytics (Safe City Project): Under projects like Delhi's *Safe City Project*, thousands of CCTV cameras are integrated using real-time AI video analytics. Tools like *AMPED FIVE* are used by agencies to clarify low-quality video footage and cross-reference faces with government databases (voter rolls, driver's licenses). Predictive Policing: Big cities (e.g., Delhi, Mumbai, Bengaluru) leverage machine learning algorithms to map historical crime data, optimize resource allocation, and forecast geographical crime hotspots.

Operational Legal Tools & Chatbots:

- NyaySanhita.in (UP Police): An AI platform helping citizens (particularly women) and police officers map incident descriptions directly to applicable provisions under the new criminal codes.
- Abhay (CBI): An AI chatbot deployed by the Central Bureau of Investigation to help citizens quickly verify the authenticity of digital arrest notices.

The Statutory Mandate for AI in Police Work

The new laws do not explicitly use the term "Artificial Intelligence," but they build the exact digital infrastructure that enables AI policing: by mandating electronic FIRs (e-FIRs) and the audio-video recording of searches, seizures, and witness statements, the BNSS creates massive, standardized digital datasets. AI thrives on this data, automating administrative summaries and transcribing or indexing video files for investigators.³

The BSA establishes primary status for electronic records. However, for AI-generated police evidence (such as a facial recognition match or a predictive crime heatmap), Section 63 establishes a tight procedural loop. The "person in charge" of the computer device or software must certify its integrity, making the software's operational reliability a core component of the police charge sheet (*Challan*).⁴

Real-World Applications in Indian Police Frameworks

An investigative study should evaluate how Indian state police forces currently use algorithmic models in field investigations. Portals like Trinetra 2.0 (used by Uttar Pradesh law enforcement) digitize over 11 lakh criminal records, enabling field officers to run real-time AI-driven facial recognition, voice sample analysis, and text-based semantic searches via mobile applications. Tools like NARIT-AI (deployed by the Gujarat Police in 2026) utilize Retrieval-Augmented Generation. Instead of using the open internet, it searches a secure, closed database of bare acts (BNS, BNSS, BSA) and Supreme Court judgments to analyze FIRs, generate evidence checklists for investigating officers (IOs), and flag potential procedural loopholes before the case goes to court. Systems like CMAPS (Crime Mapping Analytics and Predictive System) used by the Delhi Police analyze spatial-temporal data to anticipate crime clusters, shifting police strategy from a reactive posture to proactive resource optimization.

High-Stakes Legal Challenges for the Prosecution

While AI increases investigative velocity, it introduces deep vulnerabilities that a defense attorney will exploit during a trial: Under Article 21 of the Constitution, due process must be fair, just, and reasonable.

¹ Raghav Chadha v. Ashok Kumar (John Doe) and Ors. (Delhi High Court, 2026).

² Akkineni Naga Chaitanya v. John Doe (June 2026) & Abhishek Sharma v. Social Media Accounts (July 2026).

³ Section 176 & 183 of BNSS, 2023

⁴ Section 63 of BSA, 2023

If a predictive policing algorithm flags a specific neighborhood or individual, it creates a risk of "automated suspicion." The study must analyze how a suspect can legally challenge an AI risk score or algorithmic targeting during the "pre-FIR" or preliminary inquiry stage under the BNSS. Unlike a static CCTV clip, an AI output (like an automated facial reconstruction or an anomaly report in a financial fraud case under Section 318 of the BNS) is *derivative data*. It is processed by a third-party algorithmic model. Proving the chain of custody and software integrity under Section 63 of the BSA requires prosecutors to defend the algorithm's error margins and training datasets. If the police rely on an AI tool to establish a link in the chain of evidence, the defense has a right to cross-examine the logic behind that conclusion. Because proprietary AI software functions as a "black box," masking its source code under commercial trade secrets prevents true transparency, threatening the accused's right to a fair trial.

Structure methodology of police investigation

Under the modernized criminal justice framework of the Bharatiya Nagarik Suraksha Sanhita (BNSS), the structured methodology of a police investigation follows a strict, legally mandated lifecycle. This process transitions an investigation from a raw complaint into an analytically sound, digitally preserved case file ready for judicial scrutiny.

The Core Lifecycle of a Police Investigation

The lifecycle of a police investigation in India is a structured statutory progression governed by the **Bharatiya Nagarik Suraksha Sanhita (BNSS)**, moving systematically from the capture of information to the collection of evidence and judicial filing. It formally initiates under Section 173 with the registration of a First Information Report (FIR), which allows for modern paths like e-FIRs and Zero FIRs, or a time-bound 14-day Preliminary Inquiry for mid-tier offenses. Once initiated, the focus shifts to crime scene management, which legally mandates the mobilization of forensic experts for severe offenses punishable by 7 years or more, alongside mandatory audio-video recording of all searches and seizures to preserve the chain of custody. The Investigating Officer (IO) then transitions to the evidentiary phase, which involves examining witnesses under Sections 179 and 180, executing searches, and navigating custodial interrogations under Section 187, where Police Custody can be authorized in broken blocks across the initial 40 or 60 days of detention. Throughout this lifecycle, the IO must adhere to strict timelines—such as updating the victim on case progress within 90 days—while logging day-to-day developments in the Case Diary. The investigation finally concludes with the submission of a Police Report under Section 193 to the jurisdictional Magistrate, in the form of either a Closure Report when the evidence is insufficient or a formal Chargesheet establishing a *prima facie* case, which officially transitions the matter from an executive inquiry to a judicial trial.

A major Indian news agency sued OpenAI, alleging that the tech giant scraped its copyrighted news material without authorization to train ChatGPT models. This is India's premier test of the "Fair Use" doctrine under the Copyright Act, 1957. The court is currently examining whether using publicly available intellectual property for AI training constitutes an industry-standard transformation or direct copyright infringement.⁵

PHASE-BY-PHASE OPERATIONAL WORKFLOW

a. Initiation and Intake (The Genesis of the Case): The investigation formally begins with the recording of the First Information Report. Under the new laws, this includes registering e-FIRs, which must be signed by the complainant within 3 days to be legally finalized.⁶ For specific offenses punishable by 3 to 7 years, the Investigating Officer (IO) may conduct a time-bound preliminary inquiry within 14 days, with prior permission from a senior officer, to ascertain whether a *prima facie* case exists before registering a FIR.⁷

b. Crime Scene Preservation and "e-Sakshya": A cornerstone of the modernized procedure is the strict requirement for audio-video recording during searches and seizures. The IO must use mobile or digital devices to record the recovery of evidence in real-time.⁸ For offenses carrying a punishment of 7 years or more, the dispatch of a forensic expert to the crime scene is mandatory. The expert is responsible for identifying, packaging, and securing biological or physical evidence.⁹ As materials are seized, a detailed on-site inventory is prepared. For digital artifacts (smartphones, hard drives, DVRs), the IO must immediately generate a cryptographic hash (e.g., SHA-256) to secure the digital chain of custody.

⁵ ANI v. OpenAI (Delhi High Court, ongoing since late 2024)

⁶ Section 173 of BNSS, 2023

⁷ Section 173(3) of BNSS, 2023.

⁸ Section 185 of BNSS, 2023

⁹ Section 176(3) of BNSS, 2023

c. Interrogations, Statements, and Advanced Analytics: Statements of witnesses are recorded by the IO. The law permits these statements to be recorded electronically, streamlining the intake of testimony.¹⁰ Statements or confessions taken before a Magistrate must be recorded via audio-video means, specifically for heinous crimes or offenses involving vulnerable victims.¹¹ In complex financial fraud (such as BNS §318) or cyber-crime investigations, the data-mining phase involves aggregating Call Detail Records (CDRs), IPDRs, and bank ledgers. Modern police units apply analytical algorithms at this stage to map networks, track fund diversions, and flag anomalies.¹²

d. Arrest, Custody, and Procedural Controls: Arrest Memo and Intimation (BNSS §35-49). When an arrest is executed, the police must immediately inform a designated family member or friend and upload the arrest details to a district-level centralized digital portal. The arrested accused must undergo a mandatory medical examination by a registered medical practitioner within 24 hours of detention.¹³ The accused must be produced before the nearest Judicial Magistrate within 24 hours. The police can seek police custody or judicial custody under modified statutory timelines.¹⁴

e. Final Report and Charge Sheet Compilation: Upon completion of the investigation, the IO compiles the Final Report (commonly known as the Charge Sheet or *Challan*).¹⁵ The report details the nature of the information, names of parties, and the evidence collected. Crucially, all secondary electronic records attached to the charge sheet must be accompanied by the statutory Section 63 BSA Certificate (signed by both the custodian and an independent expert) to be legally admissible in court.

Key Performance Indicators (KPIs) of a Modern Investigation

To ensure an investigation survives judicial scrutiny, the IO must treat three parameters as non-negotiable:

Parameter	Method of Verification	Legal Consequence of Failure
Chain of Custody	Unbroken logbook signatures and timestamped videography.	Evidence is deemed compromised or planted.
Data Integrity	Matching hash values from the scene of crime to the forensic lab report.	Inadmissibility under Section 63 of the BSA.
Statutory Timelines	Filing the charge sheet within 60/90 days (or extended parameters under BNSS §187).	The accused becomes eligible for mandatory "Default Bail."

Modern investigation requires a balance of physical policing and digital precision. An investigation is only as strong as its procedural compliance; the finest forensic or analytical evidence will fail at trial if its digital footprint or statutory certificate is flawed.

AI-derived forensic evidence must satisfy the authentication and certification requirements of Section 63 of the Bharatiya Sakshya Adhiniyam (BSA).

The admissibility of Artificial Intelligence (AI)-derived forensic evidence under the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represents a major shift from the old framework of the Indian Evidence Act (IEA). Section 63 of the BSA replaces the old Section 65B of the IEA, introducing stricter statutory conditions designed to safeguard the integrity of electronic records in the era of deepfakes and algorithmic manipulation.

When an investigator or a forensic expert relies on an AI system—such as automated pattern matching, deepfake detection, or algorithmic financial anomaly parsing—the output is considered an electronic record containing a derivative statement. To be admissible, it must strictly clear the hurdles of Section 63 of the BSA.

Before applying Section 63, a court must determine the nature of the digital evidence: Primary Electronic Evidence. If the original server, cloud resource, or computing device running the AI model is brought directly before the court to demonstrate real-time output generation, it can be admitted as primary evidence without a certificate.¹⁶ In almost all practical forensic scenarios, an investigator exports a PDF report, a processed video, or a data sheet to a flash drive or a printout.¹⁷ This secondary output strictly requires a Section 63(4) certificate for every submission.

The old Section 65B allowed a single signature from the device's manager. To prevent unauthenticated or manipulated digital submissions, the BSA introduced a highly formalized Schedule appended to the Act.

¹⁰ Section 180 of BNSS, 2023

¹¹ Section 183 of BNSS, 2023

¹² Section 318 of BNSS, 2023

¹³ Section 53 of BNSS, 2023

¹⁴ Section 187 of BNSS, 2023

¹⁵ Section 193 of BNSS, 2023

¹⁶ Section 57 of Bhartiya Suraksha Sanhita, 2023

¹⁷ Section 63 of Bhartiya Suraksha Sanhita, 2023

This certificate is divided into two distinct operational parts. This section must be completed and signed by the individual who has lawful control and operational charge of the computer resource or communication device running the AI application. They must certify the four operational criteria under Section 63(2):

1. The AI tool/computer was regularly used to process data during the relevant period.
2. Information of this kind was regularly fed into the system in the ordinary course of activities.
3. The system was operating properly throughout the material time (or any malfunction did not corrupt the data's accuracy).
4. The output accurately reproduces or is derived from the original information.

The Expert Certification: This is the most critical addition for AI-derived forensics. Part B must be signed by an independent expert. The Supreme Court upheld the validity of Section 63(4) and clarified that while an Examiner of Electronic Evidence notified under Section 79A of the IT Act is the standard, a person possessing special skills and documented expertise in computer science and cyber forensics can also sign Part B, provided the court is satisfied with their qualifications.

The Cryptographic Hash Value Mandate: Section 63(4) legally prioritizes data integrity by requiring the cryptographic hash value to be disclosed directly in the statutory certificate. For any AI forensic output (e.g., a face-recognition match report), the expert must compute and state the exact hash value (typically using a robust algorithm such as SHA-256). Any slight modification, text alteration, or algorithmic re-rendering will break the hash match. A certified electronic record submitted without its corresponding cryptographic hash is legally incomplete and highly susceptible to rejection.

Specific Scrutiny Challenges for AI Forensics and Constitutional Challenges:

Satisfying the literal text of Section 63 is only the first step. When the electronic record is generated by an AI algorithm, the prosecution faces deep evidentiary hurdles during cross-examination:

Statutory Condition	The AI Legal Friction
Section 63(2)(c) (System operating properly)	The "Black Box" Problem: How does an expert certify that an advanced deep learning model "operated properly" if its internal neural network parameters (weights and biases) are non-transparent and proprietary?
Section 63(4)(b) (Particulars of the device/software)	Software Version Control: AI outputs vary drastically based on model updates, training datasets, and temperature settings. The certificate must explicitly state the exact software version and model parameters used during data extraction.

- The Evidentiary Framework: The transition to the Bharatiya Sakshya Adhiniyam, 2023 (BSA)—which replaced the Indian Evidence Act—alongside the IT Act forms the bedrock of digital forensics, though direct legal standards for auditing the "explainability" of AI algorithms remain fragmented.
- Privacy & Proportionality: Post the landmark *Justice K.S. Puttaswamy v. Union of India (2017)* ruling on the Right to Privacy, any state-backed AI surveillance or data mining must satisfy strict criteria of legality, necessity, and proportionality.¹⁸
- Algorithmic Bias: Academic circles heavily critique automated facial recognition technology (FRT) in India for its potential to amplify systemic biases against marginalized communities due to disproportionate underlying data sets.
- Judicial Skepticism towards AI: While courts utilize AI for translations (e.g., *SUVAS*), the Supreme Court of India has severely reprimanded the use of AI-fabricated citations and deepfakes in filings (e.g., *Gummadi Usha Rani v. Sure Mallikarjuna Rao, 2026*), setting a strict precedent against unverified AI tools in the legal stream.¹⁹

The Supreme Court's Draft Rules (2026): In line with many judgments, the Supreme Court released the Draft Policy on the Use of Artificial Intelligence in Courts 2026. It establishes a federal structure (an Apex Body at the SC level and committees at each High Court) to govern permissible AI use in administration, legal research, and automated translation, while punishing the systemic filing of fabricated AI-generated material.

CONCLUSION

Artificial Intelligence has fundamentally redefined the mechanics of police investigations. By automating administrative burdens, untangling vast webs of digital evidence, and parsing hours of video analytics, it

¹⁸ *K.S. Puttaswamy v. Union of India (2017)*

¹⁹ *Gummadi Usha Rani v. Sure Mallikarjuna Rao, 2026*.

rescues modern detective work from data paralysis. However, tech-driven speed cannot substitute for constitutional justice. To ensure that AI-derived forensic evidence survives a motion to suppress under the BSA, the investigative and reporting workflow must adapt: The expert must prove that the baseline data fed into the AI system was collected via bit-for-bit forensic cloning, preserving a verifiable chain of custody *before* the AI performed any transformations. Compute the hash values at the moment of data acquisition, the moment of AI processing, and the final generation of the secondary electronic document. Do not treat Part B of the Schedule as a rubber-stamp exercise. The expert should attach an addendum detailing the AI tool's error rates, verification algorithms, and testing methodologies to satisfy the court of the AI tool's technical reliability.

Ultimately, AI must remain a tool that amplifies human judgment rather than replacing it. The maturity and success of AI in 21st-century policing will not be measured by how advanced an agency's algorithms are, but by the transparency, ethical governance, and public trust that guide their deployment. AI rescues modern detective work from data paralysis, but speed cannot replace justice. The success of AI in law enforcement relies entirely on the transparency and ethical governance that guide its deployment.

Strategic Framework for the Future

To responsibly leverage AI without compromising civil liberties, agencies must adopt four core principles:

1. Co-Design Partnerships: Collaborate with legal experts, academics, and community stakeholders to ensure software aligns with democratic values.
2. Independent Governance: Establish continuous technical oversight, regular bias testing, and adversarial "red-teaming" to maintain algorithmic accuracy.
3. Strict Data Sovereignty: Mandate vendor transparency and ensure sensitive case files are processed on secure, sovereign infrastructure rather than public clouds.
4. Proper Training and Expert: The Police Department needs to train the concerned police officers on technology-based equipment and appoint an expert to handle the AI-based equipment.

REFERENCES

1. Faqir, R. S. A. (n.d.). Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. *International Journal of Cyber Criminology*. Cited by: 85
2. Rigano, C. (n.d.). Using artificial intelligence to address criminal justice needs. Cited by: 273
3. Shevchuk, V. (n.d.). Artificial intelligence in criminal proceedings: Criminalistics, criminal procedure and psychology issues. *International Annals of Criminology*. Cited by: 10
4. Stoykova, R., Porter, K., & Beka, T. (2024). The Ai Act in a law enforcement context: The case of automatic speech recognition for transcribing investigative interviews. <https://doi.org/10.2139/ssrn.4913090> Cited by: 11
5. Cruz, J. I., & Layasri, B. (2025). Artificial intelligence in Indian cyber forensics. *International Journal of Legal Leaders & Research*.
6. Jain, A., & Gupta, S. (2023). AI-powered criminal identification in India: Evaluating human rights concerns in automated identification systems. SPAST Reports.
7. Mahalle, Y. G. (2025). Cybercrime, artificial intelligence, and forensic evidence law in India: Reassessing legal standards in the digital age. *Lawful Legal*.
8. Ranjan, R., et al. (2022). The role of artificial intelligence in criminal investigations in India. *Journal of Artificial Intelligence and Autonomous Intelligence*.

Copyright: © 2026 Author. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.