# Technology, forensics and criminal procedure: A critical study of recent reforms in India

**Rashtra Bandu[1]*, Prof. (Dr.) Aradhana Parmar[2]**

[1] Research Scholar, Faculty of Law, Maharishi Arvind University, Jaipur, Rajasthan, India

rashtrabandhu123@gmail.com

[2] Supervisor, Faculty of Law, Maharishi Arvind University, Jaipur, Rajasthan, India

**Abstract:** The transformation of crime through digital technology has compelled criminal justice systems to reconsider conventional methods of investigation, evidence collection, prosecution and adjudication. India has recently undertaken one of the most significant restructurings of its criminal justice framework through the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Bharatiya Sakshya Adhiniyam, 2023 (BSA), and the Bharatiya Nyaya Sanhita, 2023 (BNS), which came into force on 1 July 2024. These reforms seek to incorporate forensic science, electronic communication, digital evidence, audio-video recording and technology-assisted judicial processes into mainstream criminal procedure. The BNSS introduces, inter alia, forensic examination of crime scenes in serious offences, audio-video recording of searches and seizures, electronic communication of information relating to cognizable offences, electronic service of summons, audio-video recording of statements and the possibility of conducting trials and other proceedings through electronic means. Section 176(3) of the BNSS requires, from a date to be notified by each State within the statutory implementation period, the attendance of a forensic expert at crime scenes involving offences punishable with imprisonment of seven years or more and videography of the evidence-collection process. Sections 61–63 of the BSA strengthen the legal recognition of electronic and digital records, while its statutory certificate mechanism incorporates device particulars and hash values for authenticating electronic evidence.

The reforms represent a significant shift from confession- and testimony-dependent investigation toward evidence-based criminal justice. They may increase transparency, reduce manipulation, improve documentation and strengthen prosecution where forensic evidence is collected scientifically. Nevertheless, technological modernisation also produces constitutional, institutional and evidentiary challenges. The reliability of forensic techniques, shortages of laboratories and trained experts, digital chain-of-custody requirements, algorithmic integrity, cybersecurity, privacy, biometric-data retention, uneven technological infrastructure and risks of exclusion of digitally disadvantaged participants require careful attention. The Criminal Procedure (Identification) Act, 2022 adds another dimension by authorising extensive collection and long-term retention of biometric and other measurements, thereby requiring reconciliation between scientific investigation and the constitutional right to privacy.

This article critically analyses the historical evolution of technology and forensic science in Indian criminal procedure, examines the principal reforms introduced by the new criminal laws, evaluates their practical and constitutional implications and compares Indian developments with selected international approaches. It argues that technology should supplement rather than replace judicial scrutiny, procedural fairness and professional investigation. The success of India's new forensic-oriented criminal justice model will ultimately depend less on statutory declarations than on scientific standards, laboratory capacity, independent quality assurance, judicial competence, data protection and consistent implementation across States.

**Keywords:** Technology; Forensic Science; Criminal Procedure; Bharatiya Nagarik Suraksha Sanhita; Bharatiya Sakshya Adhiniyam; Electronic Evidence; Digital Forensics; Crime-Scene Investigation; Chain of Custody; Biometric Evidence; Cyber Forensics; Criminal Justice Reforms; Privacy; Fair Trial.

## INTRODUCTION

Technology has transformed the nature of both crime and criminal investigation. Contemporary criminal conduct frequently produces evidence in forms that did not exist when the basic architecture of India's traditional criminal justice system was developed. Mobile phones preserve communications, locations, photographs and behavioural patterns; surveillance cameras record events continuously; cloud platforms retain remotely stored information; financial transactions generate digital trails; biometric databases enable identification; and social-media platforms may contain communications relevant to motive, conspiracy, harassment, fraud or organised crime. At the same time, artificial intelligence, deepfakes, encryption, anonymous digital communications and sophisticated cybercrime techniques have made the authentication and interpretation of evidence increasingly complex.

For much of India's legal history, criminal procedure and evidence law were designed primarily for a physical world. The Code of Criminal Procedure, 1973 (CrPC), although repeatedly amended, retained a predominantly paper-based procedural structure, while the Indian Evidence Act, 1872 had been enacted long before electronic communication and digital storage. Amendments made through the Information Technology Act, 2000 introduced provisions dealing with electronic records, but courts subsequently encountered persistent questions regarding admissibility, authenticity and certification.

Indian criminal jurisprudence gradually developed standards for electronic evidence. In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court emphasised statutory certification requirements governing electronic records. The subsequent decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) reaffirmed the importance of the certificate contemplated under the then Section 65B of the Indian Evidence Act where secondary electronic evidence was relied upon. These decisions demonstrated that digital evidence could not simply be treated as an ordinary physical document: its reliability depended on questions of origin, integrity, device operation and authentication.

Against this background, the enactment of the BNS, BNSS and BSA in 2023 represents an attempt to reconstruct the procedural framework around contemporary technological realities. The three statutes received presidential assent in December 2023 and came into force from 1

July 2024. The Ministry of Home Affairs characterises the new framework as technology-enabled and oriented toward accessible and timely justice.

Among these laws, the BNSS and BSA are particularly relevant to technology and forensic science. The BNSS expressly recognises audio-video electronic means and electronic communication at multiple procedural stages. Information about cognizable offences may be communicated electronically under Section 173, subject to statutory formalities. Section 105 requires the process of search and seizure to be recorded through audio-video electronic means, preferably through a mobile phone, with the recording forwarded without delay to the appropriate Magistrate. Section 176(3) introduces forensic crime-scene investigation for offences punishable with imprisonment of seven years or more, linked to State notification within the prescribed implementation window, and requires videography of the forensic collection process. Sections 180 and 183 permit specified statements and confessions to be recorded through audio-video methods, while Section 530 allows trials, inquiries, evidentiary recording, summons-related processes and appellate proceedings to be conducted electronically.

The BSA,2023 simultaneously modernises the evidentiary framework. Section 61 makes clear that an electronic or digital record cannot be denied admissibility merely because of its electronic character, subject to Section 63. Section 57 significantly expands the concept of primary evidence in digital settings: multiple files in which an electronic record is simultaneously or sequentially stored may constitute primary evidence; electronic records produced from proper custody may be treated as primary evidence unless disputed; and multiple simultaneously stored or transmitted video recordings may themselves constitute primary evidence.

These developments have the potential to improve criminal investigation significantly. Crime-scene videography may reduce disputes concerning recovery and seizure. Scientific analysis may reduce dependence on custodial interrogation and unreliable testimony. Electronic summons and virtual participation can reduce procedural delays. Digital case management may improve institutional coordination. Yet every technological reform raises new questions of reliability, accountability and constitutional rights.

The principal objective of this article is therefore not merely to describe India's recent reforms but to critically assess whether they are capable of producing a more scientific and fair criminal justice system. It examines their historical foundations, forensic implications, evidentiary innovations, privacy concerns, implementation challenges and comparative international relevance. The central proposition is that technology can improve criminal justice only when accompanied by scientifically validated methods, transparent procedural safeguards and meaningful judicial oversight.

**Historical Background**

The relationship between forensic science and criminal justice in India developed gradually. Colonial criminal procedure primarily depended upon witness testimony, confessions, documentary material, medical evidence and physical objects. The Indian Evidence Act, 1872 established general rules concerning relevance, expert opinion, documentary evidence and proof. Although the statute was advanced for its time, it was naturally designed for an era in which written documents existed mainly in tangible form and communication occurred through physical correspondence or telegraphic systems. Expert testimony was admissible, but modern disciplines such as DNA profiling, digital forensics, cyber forensics and automated biometric identification did not exist.

The development of fingerprint science was an important early technological contribution to criminal investigation in India. Fingerprint classification and identification became institutionalised during the colonial period and eventually formed part of police practice. The Identification of Prisoners Act, 1920 authorised the collection of specified identifying measurements from certain classes of persons. This legislation remained the principal statutory foundation for criminal-identification measurements for more than a century until its replacement by the Criminal Procedure (Identification) Act, 2022.

Following independence, forensic medicine, ballistics, handwriting examination, toxicology, fingerprints and chemical analysis became progressively integrated into criminal investigation. Central and State forensic science laboratories were established, although availability and quality varied considerably across jurisdictions. The Code of Criminal Procedure, 1973 modernised several aspects of investigation, medical examination and

judicial procedure but continued to reflect an essentially physical conception of investigative material.

Technological change accelerated dramatically from the late twentieth century. Computers entered commercial and governmental activity, telecommunication expanded and digital records increasingly acquired legal and economic significance. The Information Technology Act, 2000 gave statutory recognition to electronic records and digital signatures and amended existing laws, including the Indian Evidence Act, to accommodate electronic evidence. Sections 65-A and 65-B of the Evidence Act subsequently became central to questions of digital admissibility.

The emergence of mobile phones, email, CCTV systems and internet communication transformed criminal investigations during the 2000s. Call-detail records, mobile-location information, electronic banking trails and computer files increasingly appeared in terrorism, corruption, economic offences and conventional criminal cases. Yet police investigators, prosecutors and courts often faced difficulties in determining how electronic records should be collected, preserved and proved.

Judicial interpretation became especially important. The Supreme Court initially adopted a comparatively flexible approach toward some forms of electronic evidence, but *Anvar P.V. v. P.K. Basheer* (2014) clarified that statutory requirements applicable to computer outputs were mandatory where secondary electronic evidence was tendered. The decision recognised the distinctive vulnerability of digital evidence to alteration and copying. In *Tomaso Bruno v. State of Uttar Pradesh* (2015), the Court emphasised the importance of scientific and electronic evidence and observed the increasing relevance of CCTV and related technologies in criminal investigation.

Constitutional jurisprudence was evolving at the same time. In *Selvi v. State of Karnataka* (2010), the Supreme Court examined involuntary narco-analysis, polygraph examination and brain-electrical activation profile testing. It held that compelled administration of such techniques implicated protections against testimonial compulsion and personal liberty. The case was significant because it established that scientific investigation cannot escape constitutional limitations merely because a technique is described as technological or forensic.

A further constitutional turning point occurred in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), in which a nine-judge Bench recognised privacy as a fundamental right. The judgment has profound implications for biometric databases, surveillance, device searches, communications data and forensic technologies. Investigative powers interfering with privacy require lawful authority and must satisfy constitutional standards concerning legitimate purpose, necessity and proportionality.

In *Arjun Panditrao Khotkar* (2020), the Supreme Court revisited electronic-evidence certification and reaffirmed the central role of procedural authenticity. By this period, however, digital evidence had become ubiquitous. Messaging applications, social media, cloud services, GPS systems and networked devices meant that almost any serious criminal investigation could potentially involve electronic material.

Institutional developments accompanied these changes. The National Forensic Sciences University Act, 2020 created a specialised national institution to strengthen education, research and professional capacity in forensic science. The Criminal Procedure (Identification) Act, 2022 then replaced the Identification of Prisoners Act, 1920 and substantially widened the concept of *"measurements."* It includes fingerprints, palm prints, footprints, photographs, iris and retina scans, physical and biological samples and their analysis, and certain behavioural attributes. The legislation also assigns the National Crime Records Bureau a central role in collection, storage and sharing of records and provides for digital or electronic retention for seventy-five years, subject to specified exceptions.

The 2023 criminal-law reforms must therefore be understood as the culmination of a longer transition rather than a sudden technological revolution. The BNSS,2023 incorporated electronic communication and audio-video processes throughout criminal procedure, while the BSA reorganised evidentiary rules applicable to electronic and digital records. The reforms also elevated forensic science from an optional investigative aid to a statutory component of serious-crime investigation.

The transition, however, revealed an infrastructure problem. Scientific investigation requires trained crime-scene personnel, laboratories, equipment, quality-control systems and specialists capable of explaining forensic results in court. Recognising the anticipated increase in forensic workload, the Union Government approved the National Forensic Infrastructure Enhancement

Scheme (NFIES) in June 2024 with an outlay of ₹2,254.43 crore for 2024-25 to 2028-29, including nine additional NFSU campuses, seven Central Forensic Science Laboratories and enhancement of the NFSU Delhi campus.

Implementation continues to evolve. An official July 2026 update stated that ₹119.09 crore had been released and utilised under NFIES and that transit NFSU campuses were operating in Nagpur, Raipur, Khordha, Chengalpattu and Jaipur, while the approved forensic infrastructure continued to be developed. The historical development consequently demonstrates that India's contemporary challenge is no longer whether science and technology should enter criminal procedure. They are already central to it. The critical questions now concern reliability, accessibility, capacity, standardisation and protection of constitutional rights.

**Forensic Investigation under the Bharatiya Nagarik Suraksha Sanhita, 2023**

One of the most important reforms is contained in Section 176(3) of the BNSS. It provides that, for offences punishable with imprisonment of seven years or more, the officer in charge of a police station must, from the date notified by the State Government within the statutory period, cause a forensic expert to visit the crime scene, collect forensic evidence and ensure videography of the process through a mobile phone or another electronic device. Where a forensic facility is unavailable, the State may notify use of a facility in another State.

The provision represents an important conceptual shift. Traditional investigation could depend excessively upon statements, confessions, recoveries and eyewitness testimony. Scientific investigation can provide objective corroboration through DNA, fingerprints, toxicology, ballistics, digital devices, trace evidence and other disciplines. Mandatory forensic involvement in serious offences may therefore reduce investigative arbitrariness and increase the evidentiary quality of prosecutions.

However, the expression *"forensic evidence"* encompasses many disciplines with very different levels of reliability. DNA profiling conducted under validated laboratory procedures is fundamentally different from techniques whose error rates or scientific foundations may be less secure. Courts should therefore avoid the assumption that every conclusion contained in a forensic report is inherently accurate.

Crime-scene integrity is equally important. A sophisticated laboratory cannot correct evidence contaminated at the scene. Investigating officers must therefore secure the location, document the initial condition, use appropriate protective equipment, prevent unnecessary handling, package evidence correctly and record every transfer.

Section 105 of the BNSS contributes significantly to transparency by requiring audio-video recording of the search and seizure process, including preparation and signing of the seizure list, with the recording forwarded to the relevant Magistrate. Videography can provide contemporaneous evidence about where an object was recovered, who was present and how the seizure occurred. It may protect accused persons against fabricated recovery while simultaneously protecting investigators against false allegations.

The value of such recording nevertheless depends upon technical integrity. Questions may arise regarding whether recording began after the search had already commenced, whether footage was selectively captured, whether metadata was preserved and whether files were later edited. Standard operating procedures should therefore prescribe continuous recording where practicable, automatic timestamps, device identification, secure uploading and cryptographic hashing.

**Electronic and Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023**

The BSA represents an important modernisation of India's evidence law. Section 61 states that electronic or digital records are not to be denied admissibility simply because of their electronic form and, subject to Section 63, possess the same legal effect, validity and enforceability as other documents.

Section 57 is particularly important because it adapts the concept of primary evidence to digital architecture. Where electronic information is stored in multiple files simultaneously or sequentially, each file may constitute primary evidence. A digital record produced from proper custody may constitute primary evidence unless disputed, while simultaneous stored copies of video recordings and automated storage, including temporary files, may also qualify.

This approach recognises that the traditional distinction between an *"original"* and a *"copy"* becomes difficult in digital environments. A digital file can be replicated without visible

degradation, stored across several systems and synchronised automatically. The law therefore appropriately moves toward authenticity and integrity rather than physical originality alone.

Section 63 retains a structured mechanism governing computer output. Significantly, the Schedule requires detailed information concerning the source device and provides for recording hash values. The statutory form refers to SHA-1, SHA-256, MD5 or another legally acceptable standard and requires the hash report to accompany the certificate.

Hashing is an important forensic technique because it produces a digital fingerprint of data. If a file changes, its hash ordinarily changes, thereby enabling investigators and courts to test whether the material presented later corresponds to the data originally acquired.

The statutory recognition of hashing is therefore a positive development. Nevertheless, the inclusion of legacy algorithms such as SHA-1 and MD5 in the prescribed format deserves reconsideration. International cybersecurity standards have progressively moved away from weaker collision-resistant algorithms. The United States National Institute of Standards and Technology has encouraged transition away from SHA-1 in favour of stronger SHA-2 or SHA-3 families. India's evidentiary practice should therefore adopt dynamically updated technical standards rather than allow statutory forms to freeze outdated cryptographic practices.

**Chain of Custody and Digital Integrity**

Electronic evidence can be copied, altered, compressed, converted or deleted with relative ease. Maintaining an auditable chain of custody is consequently indispensable.

The BNSS recognises this issue by requiring the police report to include the "sequence of custody" in the case of an electronic device. This is a valuable safeguard because it directs attention to the persons and institutions through whose hands the device passed.

Nevertheless, a meaningful digital chain of custody requires more than listing custodians. It should document the time and place of seizure, device condition, identity of seizing officers, packaging, storage, forensic imaging, hash values before and after examination, software and hardware tools used, access logs and every transfer. The Parliamentary Standing Committee examining the evidence reforms specifically recognised that electronic and digital records are

susceptible to tampering and recommended secure handling and processing through a proper chain of custody. This concern remains highly relevant.

National forensic protocols should therefore provide uniform chain-of-custody requirements enforceable across States. Without such standards, the mere expansion of admissibility may increase rather than reduce disputes concerning authenticity.

**Technology-Enabled Criminal Procedure**

The BNSS introduces digital processes at several stages beyond forensic collection. Section 173 permits information relating to a cognizable offence to be communicated electronically irrespective of the area where the offence was committed, subject to the statutory requirement that electronically supplied information be signed within three days. This facilitates easier reporting and reinforces the practical concept underlying jurisdiction-neutral reporting.

Electronic summons are another important reform. The BNSS recognises service through electronic communication and treats electronically served summons as valid subject to prescribed requirements. This can reduce delays caused by conventional physical service.

Statements during investigation may also be recorded using audio-video electronic means. Confessions and statements before Magistrates may, in specified circumstances, be recorded electronically, while Section 530 broadly permits trials, inquiries, examination of witnesses, recording of evidence, summons processes, appellate proceedings and other proceedings to be conducted electronically.

Government digital platforms seek to operationalise these reforms. Applications including e-Sakshya, e-Summon, Nyaya Setu and Nyaya Shruti have been introduced to support electronic evidence, summons, institutional integration and video-conferencing. The Government has described e-Sakshya as a mechanism for storing videography, photography and testimonies on an electronic evidence server and Nyaya Shruti as facilitating witness hearings through video conferencing.

Such systems can improve efficiency, but their legitimacy depends upon cybersecurity, authentication and resilience. Technical failure must not prejudice the accused or victim.

Digital platforms require backup systems, secure access controls, audit trails, encryption and independent cybersecurity review.

**Criminal Identification, Biometrics and Privacy**

The Criminal Procedure (Identification) Act, 2022 complements the broader forensic orientation of recent criminal justice reforms. Its definition of measurements includes fingerprints, palm prints, footprints, photographs, iris and retina scans, physical and biological samples and their analysis, signatures, handwriting and specified examinations.

The Act empowers the NCRB to collect, store, process and share measurements and provides for retention in digital or electronic form for seventy-five years, subject to provisions governing destruction where qualifying individuals are released without trial, discharged or acquitted after exhaustion of legal remedies.

The investigative advantages are substantial. Biometric databases can help identify repeat offenders, connect suspects to crime scenes and solve cases where conventional investigative leads are unavailable. DNA and fingerprint comparison may also exonerate innocent persons.

However, biometric information is uniquely sensitive because, unlike passwords, it ordinarily cannot be changed when compromised. Centralised storage creates risks of unauthorised access, misuse, function creep and data breaches. The breadth of persons from whom measurements may be taken and the long retention period therefore raise significant questions under the privacy doctrine established in *Puttaswamy*.

Privacy should not be treated as an obstacle to investigation. The constitutional requirement is that investigative intrusion should be lawful, necessary and proportionate. Effective criminal investigation and privacy protection can coexist through purpose limitation, access controls, independent oversight, logging, deletion rules, judicial authorisation where appropriate and remedies for misuse.

**Forensic Capacity and Institutional Challenges**

The statutory aspiration for scientific investigation will succeed only if forensic infrastructure is capable of handling the additional workload. Mandatory or expanded forensic collection

may significantly increase submissions to laboratories. Existing delays can undermine justice because an investigation may remain incomplete while scientific reports are pending.

The Government has recognised this challenge. NFIES provides ₹2,254.43 crore for infrastructure expansion between 2024-25 and 2028-29, including nine NFSU campuses and seven CFSLs. Earlier modernisation programmes have also supported equipment, mobile forensic vans and State laboratories.

The expansion of buildings, however, is only one component. Laboratories require qualified scientists, validated instrumentation, regular calibration, proficiency testing, secure evidence storage and recognised quality-management systems. Forensic science is particularly vulnerable to cognitive bias when analysts know investigative theories or suspect identities before examining evidence. Blind or sequential testing protocols may therefore be appropriate for particular disciplines.

The Ministry of Home Affairs has reported quality manuals aligned with laboratory-accreditation standards and working procedure manuals in forensic disciplines. Such standardisation is essential, but accreditation must operate as a continuing quality process rather than a one-time administrative certificate.

Another difficulty is geographical inequality. Metropolitan police may have rapid access to specialised teams, while rural and remote districts may face shortages of forensic experts, secure storage and digital connectivity. The statutory possibility of using facilities in other States addresses laboratory availability to some extent, but transportation can produce delays and chain-of-custody complications.

**Reliability of Forensic Science and the Risk of Overconfidence**

A scientific-looking report can carry substantial persuasive influence before courts and juries. Yet forensic conclusions should never be treated as infallible merely because they are expressed by an expert.

Different forensic disciplines possess different empirical foundations. DNA profiling has strong statistical methodologies when properly conducted, but contamination, mixed samples and interpretation errors remain possible. Fingerprints can be highly useful but require

competent comparison. Digital forensics depends upon appropriate imaging and preservation. Other pattern-comparison disciplines may involve greater subjective judgment.

Judicial officers and advocates must therefore be trained to distinguish admissibility from scientific weight. Relevant questions include whether the methodology has been validated, whether error rates are known, whether the laboratory followed standard procedures, whether the analyst was qualified and whether another expert could reproduce the conclusion.

India may benefit from an independent forensic science regulator or equivalent statutory quality body with authority to prescribe standards, audit laboratories and investigate serious quality failures. Institutional independence is important because forensic laboratories frequently work closely with investigating agencies. Science used in criminal proceedings must assist the court rather than become an extension of the prosecution.

**Constitutional and Fair-Trial Concerns**

Technology-driven criminal justice must operate within Articles 14, 20, 21 and 22 of the Constitution. Efficiency cannot become a justification for procedural dilution. The privilege against testimonial compulsion is especially relevant to technologically extracted information. *Selvi v. State of Karnataka* remains important in distinguishing between legitimate physical evidence and compelled testimonial responses extracted through invasive techniques.

Privacy concerns arise from device searches, communications data, biometric databases and large-scale data integration. The proportionality principles developed in *Puttaswamy* should guide statutory interpretation and administrative rules.

Electronic proceedings also raise questions of effective participation. Video-conferencing may reduce costs and delay, but an accused person must still be able to communicate confidentially with counsel, understand the proceedings and challenge witnesses effectively. Virtual appearance should not become a mechanical substitute for meaningful judicial presence where physical production is required for fairness.

The principle of equality is equally significant. Digital systems can improve access for some while excluding persons with limited technological literacy, disabilities, poor connectivity or linguistic barriers. Criminal justice cannot assume universal digital competence.

## International Perspectives

### United Kingdom

The United Kingdom provides a useful comparative model because scientific investigation operates within a detailed framework governing police powers, disclosure and forensic quality. The Police and Criminal Evidence Act 1984 and accompanying Codes of Practice regulate important investigative procedures, including search, seizure, detention and identification.

A particularly relevant institutional development is the Forensic Science Regulator Act 2021, which strengthened the statutory basis for forensic quality standards. The British approach demonstrates that increasing dependence upon forensic evidence should be accompanied by an independent regulatory mechanism capable of establishing and enforcing scientific standards.

India's expansion of forensic laboratories and mandatory crime-scene examination can benefit from a similar emphasis on institutional quality. The central issue is not simply whether forensic evidence is obtained but whether it is produced according to validated and auditable standards.

### United States

The United States provides an important model of judicial scrutiny of scientific evidence. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993), the United States Supreme Court articulated factors relevant to evaluating scientific reliability, including testing, peer review, known or potential error rates and general acceptance. Federal Rule of Evidence 702 has subsequently developed around the requirement that expert testimony rest upon reliable principles and methods appropriately applied.

Although the institutional and procedural contexts differ from India, the underlying lesson is valuable. Courts should examine methodology rather than accepting an expert's status as sufficient proof of reliability.

The United States also demonstrates the central role of digital-forensics standards. Agencies and institutions use detailed procedures for forensic imaging, preservation, hashing and

validation. India's BSA recognition of hash values represents movement in this direction, but the relevant technical standards should remain capable of regular updating.

International cryptographic guidance is particularly instructive. NIST has urged movement away from SHA-1 toward stronger SHA-2 and SHA-3 algorithms. India's evidentiary forms should therefore be technologically dynamic and avoid dependence upon outdated hash algorithms.

**European Union**

European criminal justice systems operate within a strong data-protection and human-rights framework. European approaches emphasise purpose limitation, proportionality, security and accountability in processing personal information, including law-enforcement data.

For India, the European experience demonstrates that modern investigation and privacy need not be seen as mutually exclusive. Large forensic and biometric databases can operate under strict access rules, security obligations and independent supervision.

**Australia and Canada**

Australia and Canada similarly provide examples of increasing reliance on DNA databases, digital forensic evidence and remote judicial processes accompanied by procedural safeguards and professional accreditation.

Comparative experience demonstrates three recurring principles. First, scientific evidence requires quality assurance independent of investigative enthusiasm. Second, digital evidence requires demonstrable integrity and chain of custody. Third, technological efficiency must remain subordinate to fair-trial rights.

India's reforms are therefore directionally consistent with global developments, but the long-term effectiveness of the model will depend upon whether implementation incorporates these institutional safeguards.

**Critical Assessment of the Recent Reforms**

The strongest feature of India's recent reforms is their recognition that scientific evidence must become part of routine criminal investigation rather than an exceptional resource. Mandatory forensic involvement in serious offences can improve the objective quality of investigations.

A second important advantage is transparency through audio-video documentation. Search, seizure and evidence collection have historically generated disputes concerning manipulation or fabrication. Contemporaneous recording can reduce such disputes.

Third, electronic procedure has the potential to reduce delay. Digital summons, remote witness examination and electronic records can save substantial administrative time.

Fourth, the BSA acknowledges the distinctive architecture of electronic records. Its treatment of multiple digital files and automated storage as primary evidence reflects technological reality more accurately than a purely physical conception of originals and copies.

Nevertheless, several concerns remain. The first is implementation capacity. A legal mandate cannot create trained experts overnight. If laboratories become overwhelmed, scientific investigation may produce longer rather than shorter delays.

The second is the danger of formalism. Investigators may come to regard crime-scene videography or forensic referral as administrative checkboxes rather than substantive scientific practices. Quality must be measured, not merely completion.

Third, digital integrity requires stronger uniform standards. Reporting the sequence of custody is useful, but digital evidence should be governed through detailed protocols covering forensic imaging, access, hashing, storage, transfer and audit.

Fourth, privacy and data protection must remain central. Expanded biometric collection and integration of police, forensic, prison, prosecution and court systems generate substantial amounts of sensitive information. Cybersecurity failures could compromise individuals and investigations simultaneously.

Fifth, forensic independence deserves greater attention. Experts should not feel institutional pressure to produce prosecution-oriented conclusions. Their obligation is scientific objectivity.

Finally, judicial education is crucial. Judges must be able to distinguish between the apparent authority of technology and genuine scientific reliability.

**Suggestions for Strengthening the Reformed Framework**

India should develop a comprehensive national digital-evidence protocol applicable across police forces and forensic laboratories. It should prescribe imaging, hashing, metadata preservation, storage, access and audit requirements.

A statutory or functionally independent forensic quality regulator should be considered. Such a body could establish scientific standards, oversee accreditation, prescribe competency requirements and investigate laboratory failures.

The BSA certificate mechanism should be periodically updated through technologically neutral rules. Strong contemporary hash algorithms should be preferred, and outdated algorithms should be phased out when international scientific standards no longer regard them as appropriate.

States should establish adequate mobile forensic units so that the Section 176(3) model is practically accessible beyond metropolitan areas. Crime-scene officers should receive specialised training distinct from conventional policing.

Defence access to forensic evidence should also be strengthened. Fair trial requires meaningful opportunity to challenge expert conclusions, obtain underlying data where legally permissible and seek independent examination.

Digital and biometric databases should operate under strict role-based access, encryption, audit logging and defined deletion rules. Unauthorised access should attract effective legal consequences.

Judicial academies and law universities should expand training in digital evidence, forensic methodology, artificial intelligence, cybersecurity and scientific reasoning. Modern criminal litigation increasingly requires technological literacy from judges, prosecutors and defence counsel alike.

## FUTURE SCOPE

The future of criminal procedure will be shaped by technologies far more complex than those presently addressed by legislation. Artificial intelligence may assist facial recognition, video analysis, document examination and pattern detection. Generative AI will simultaneously make fabrication of audiovisual evidence more sophisticated. Deepfake detection will therefore become an increasingly important forensic discipline.

Digital evidence will also shift toward cloud-based and decentralised environments. Investigators may need to obtain data stored across multiple jurisdictions and controlled by multinational platforms. Indian criminal procedure will consequently require stronger mechanisms for lawful cross-border access to electronic evidence and international cooperation.

Internet-of-Things devices, smart vehicles, wearable technology and connected household systems will generate new categories of evidentiary data. Courts will need standards governing authenticity, interpretation and privacy in relation to such devices.

Forensic genomics may expand beyond conventional DNA matching toward more advanced analytical techniques. These developments could improve identification but will intensify concerns regarding genetic privacy and familial inference.

Future research should empirically assess the effect of Section 176(3) BNSS after wider State implementation. Important variables include time taken for forensic attendance, quality of crime-scene preservation, laboratory pendency, acquittal and conviction patterns and geographical disparities.

Research should also examine whether audio-video recording of search and seizure actually reduces procedural disputes and whether digital platforms improve the experience of victims and witnesses.

The NFIES programme offers a significant opportunity to build capacity, but its outcomes should be independently evaluated. Infrastructure expenditure should be linked to measurable improvements in laboratory turnaround times, accreditation, staff competency and evidentiary quality.

Artificial intelligence used within the criminal justice system should remain explainable and auditable. Algorithmic outputs must never be treated as substitutes for evidence merely because they are generated computationally.

The long-term direction should therefore be toward **rights-respecting scientific criminal justice** - a system in which technology improves truth-finding while constitutional protections become stronger rather than weaker.

## CONCLUSION

Recent reforms in India's criminal procedure represent an important transition from a predominantly paper-based and testimony-oriented system toward technologically enabled and scientifically informed criminal justice. The Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 explicitly recognise electronic communication, audio-video documentation, forensic crime-scene investigation and digital evidence.

Section 176(3) BNSS has the potential to transform investigation of serious offences by embedding forensic expertise at the crime scene. Section 105 can strengthen transparency through recorded searches and seizures. Electronic summons, digital information reporting and virtual proceedings can reduce procedural delay. Sections 57 and 61–63 BSA adapt traditional evidentiary principles to the realities of digital storage and authentication.

These reforms should nevertheless be evaluated by their actual implementation rather than their technological appearance. Forensic evidence is valuable only when scientifically reliable. Digital evidence is persuasive only when authenticity and integrity can be demonstrated. Video recording increases transparency only when recordings are complete, securely stored and protected against manipulation.

India must therefore invest simultaneously in infrastructure, personnel, laboratory accreditation, chain-of-custody protocols, judicial education and cybersecurity. The continuing NFIES investment is an important institutional response, but infrastructure expansion must translate into scientifically competent and timely forensic services.

The constitutional dimension is equally important. Biometric identification, device examination, data sharing and technologically mediated proceedings interfere with important

dimensions of privacy and personal liberty. The principles developed in *Selvi* and *Puttaswamy* must therefore remain central to implementation.

International experience demonstrates that successful forensic systems require more than sophisticated laboratories. They require quality regulation, methodological transparency, professional independence and meaningful defence access. India should consider institutionalising these safeguards as the new framework matures.

The recent reforms should ultimately be understood not as the replacement of law by technology but as an opportunity to integrate law and science more effectively. Neither a machine-generated output nor a forensic report can determine guilt by itself. Criminal liability must continue to be established according to law, through admissible and reliable evidence tested in a fair judicial process.

Technology can assist the pursuit of truth; it cannot define truth. Forensic science can strengthen justice; it cannot substitute for judicial reasoning. India's reforms will achieve their transformative potential only when scientific efficiency, human rights, procedural fairness and institutional accountability develop together.

**References**

1. Government of India. (1872). *The Indian Evidence Act, 1872*. Legislative Department.
2. Government of India. (1920). *The Identification of Prisoners Act, 1920*. Legislative Department.
3. United Kingdom Parliament. (1984). *Police and Criminal Evidence Act 1984*. The Stationery Office.
4. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
5. Government of India. (2000). *The Information Technology Act, 2000*. Ministry of Law and Justice.
6. National Institute of Standards and Technology. (2006). Cryptographic hash standards: Where do we go from here? *IEEE Security & Privacy, 4*(2).
7. *Selvi & Others v. State of Karnataka*, (2010) 7 SCC 263.
8. *Anvar P.V. v. P.K. Basheer & Others*, (2014) 10 SCC 473.
9. *Tomaso Bruno & Another v. State of Uttar Pradesh*, (2015) 7 SCC 178.

10. *Justice K.S. Puttaswamy (Retd.) & Another v. Union of India & Others*, (2017) 10 SCC 1.
11. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Others*, (2020) 7 SCC 1.
12. Government of India. (2020). *The National Forensic Sciences University Act, 2020*. Ministry of Law and Justice.
13. United Kingdom Parliament. (2021). *Forensic Science Regulator Act 2021*. The Stationery Office.
14. Government of India. (2022). *The Criminal Procedure (Identification) Act, 2022*. Ministry of Home Affairs.
15. Government of India. (2022). *The Criminal Procedure (Identification) Rules, 2022*. Ministry of Home Affairs.
16. National Institute of Standards and Technology. (2022). *NIST policy on hash functions*. U.S. Department of Commerce.
17. Government of India. (2023). *The Bharatiya Nagarik Suraksha Sanhita, 2023*. Ministry of Law and Justice.
18. Government of India. (2023). *The Bharatiya Sakshya Adhiniyam, 2023*. Ministry of Law and Justice.
19. Department-related Parliamentary Standing Committee on Home Affairs. (2023). *Report on the Bharatiya Sakshya Bill, 2023*. Parliament of India.
20. Government of India, Ministry of Home Affairs. (2024). *National Forensic Infrastructure Enhancement Scheme*. Government of India.