

Technology-Driven Criminal Justice in India: Opportunities, Challenges, And Constitutional Safeguards Under the New Criminal Laws

Veerasha¹, Dr. Rajvendra Kumar Chaudhari²

¹Research Scholar, Mansarovar Global University, Sehore

²Associate Professor, Faculty of law, Mansarovar Global University, Sehore

Abstract—The enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has formalised an expanded role for electronic communication, audio-video processes, and electronic or digital records in India's criminal justice framework. Technology can facilitate reporting, investigation, evidence management, and court proceedings, but it also raises questions concerning privacy, authenticity, chain of custody, unequal access, and procedural fairness. This paper examines technology-driven criminal justice through five themes: digital access to justice, technology-enabled investigation, electronic evidence, constitutional safeguards, and institutional readiness. It adopts a qualitative doctrinal and conceptual methodology based on statutory texts, selected judicial decisions, and official government materials.

The paper argues that technology should be treated as an instrument of justice rather than an independent measure of modernisation. Its benefits depend on lawful collection, reliable preservation, transparent procedures, competent personnel, judicial scrutiny, and meaningful access for all participants. A conceptual framework the Accountable Digital Criminal Justice Framework is proposed to connect technological capability with legality, evidentiary integrity, inclusion, and accountability.

The paper concludes that digital transformation can support timely and accessible justice only when accompanied by rights-based safeguards, adequate infrastructure, and systematic evaluation. The framework is offered as a conceptual proposition for future empirical testing, not as an established or validated model.

Index Terms—digital criminal justice, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, electronic evidence, forensic science, privacy, fair trial.

I. INTRODUCTION

Technology has become an increasingly important component of criminal justice administration. Electronic communications, mobile devices, digital transactions, surveillance systems, online platforms, and computer-stored records may be relevant to the reporting, investigation, prosecution, and adjudication of offences. Criminal justice institutions must therefore develop methods for obtaining, preserving, evaluating, and presenting digital information while protecting legal rights.

India's new criminal law framework includes three enactments: the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA). The principal provisions came into force on 1 July 2024, subject to specified exceptions. The BNSS provides for electronic communication and audio-video processes in specified criminal procedures, while the BSA expressly addresses electronic and digital records (Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023).

The BNSS includes provisions concerning electronic communication, production of documents and digital evidence, audio-video recording in specified contexts, and electronic-mode proceedings. For example, Section 94 addresses production of documents and things, including electronic communication and communication devices that may contain digital evidence; Section 530 permits trials, inquiries, and proceedings to be held in electronic mode in accordance with the provision. Government materials also describe technology-enabled appearances through

video-conferencing applications (Ministry of Home Affairs, 2026).

However, the availability of technology does not itself establish that justice has become more accessible, accurate, or fair. Digital systems can reduce some barriers while creating others. Electronic evidence may be easy to copy but difficult to authenticate; remote hearings may reduce travel but depend on connectivity and private access to legal counsel. Technology-driven reform must therefore be assessed through a legal and institutional framework that places constitutional rights at its centre.

II. STATEMENT OF THE PROBLEM

The central problem addressed in this paper is the tension between the potential benefits of technology-enabled criminal justice and the risks that arise when digital tools are deployed without sufficient safeguards. The new laws create a statutory basis for wider use of electronic processes and digital records, but effective implementation requires reliable infrastructure, trained personnel, evidence-handling standards, privacy protection, and fair access to proceedings.

A technology-centred approach that measures success only through digitisation or speed may overlook evidentiary reliability, exclusion of digitally disadvantaged participants, and the risk of disproportionate intrusion into privacy. The problem is therefore to conceptualise a model of digital criminal justice that combines operational effectiveness with legality, accountability, inclusion, and due process.

III. OBJECTIVES OF THE STUDY

1. To examine the major provisions and conceptual dimensions of technology-enabled investigation, procedure, and electronic evidence under the new criminal laws in India.
2. To analyse the opportunities and challenges of digital criminal justice in relation to evidentiary reliability, privacy, access to justice, and constitutional safeguards.
3. To propose an accountable, rights-centred conceptual framework and recommendations for the effective implementation of technology in India's criminal justice system.

IV. RESEARCH METHODOLOGY

This paper adopts a qualitative, doctrinal, and conceptual research design. It does not involve primary data collection, interviews, surveys, or statistical analysis. The primary sources are the BNSS and BSA, read alongside relevant constitutional principles. Secondary materials include selected Supreme Court decisions and official publications of the Ministry of Home Affairs, the Bureau of Police Research and Development, and India Code.

A thematic method is used to organise the analysis under five themes: digital access to justice; technology-enabled investigation; electronic evidence and forensic integrity; constitutional safeguards and privacy; and institutional readiness. The paper is analytical rather than empirical. It does not claim to demonstrate that the new laws have reduced delays, increased conviction rates, or improved public confidence. Those propositions require independent empirical assessment.

V. LEGAL AND CONCEPTUAL BACKGROUND

5.1 Technology in the BNSS

The BNSS recognises audio-video electronic means and electronic communication within its procedural framework. Section 94 permits a court or police station officer, subject to the statutory conditions, to require production of a document, electronic communication, communication device, or other thing considered necessary or desirable for an investigation, inquiry, trial, or proceeding. Section 530 provides for trials, inquiries, and proceedings under the Sanhita to be held in electronic mode, using electronic communication or audio-video electronic means. These provisions create procedural possibilities, but their use remains governed by statutory requirements and applicable safeguards.

5.2 Electronic and Digital Records under the BSA

Sections 61 and 62 of the BSA address the legal effect and proof of electronic or digital records. Section 63 sets out conditions relevant to the admissibility of specified electronic records and computer outputs. The statutory recognition of electronic records is important, but admissibility does not make every digital item automatically authentic, complete, or

reliable. The origin, integrity, context, and manner of production remain material to evidentiary evaluation.

5.3 Judicial Background on Electronic Evidence

In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court considered the proof of electronic records under the former Indian Evidence Act. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), the Court further examined the certification requirements under the earlier framework. These decisions form part of the doctrinal background to electronic evidence law. Since they interpreted predecessor legislation, the BSA must be applied according to its own text, while relevant principles are considered in accordance with law.

5.4 Constitutional Context

Technology-enabled criminal justice must operate consistently with constitutional protections, including personal liberty and fair procedure under Article 21, safeguards relating to arrest and detention under Article 22, and applicable protections against compelled self-incrimination under Article 20(3). The Supreme Court's decisions in *Maneka Gandhi v. Union of India* (1978) and *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) provide important constitutional context concerning fair procedure and privacy. The precise application of these principles depends on the facts, legal authority, and nature of the state action.

VI. THEMATIC ANALYSIS

6.1 Theme I: Digital Access to Justice and Procedural Convenience

Electronic communication and remote participation may reduce the need for physical travel, support communication across jurisdictions, and facilitate the participation of witnesses, experts, accused persons, and legal professionals where legally appropriate. Government materials describe the use of video-conferencing systems for virtual appearances in criminal proceedings (Ministry of Home Affairs, 2026). Such tools may be particularly useful where distance, security, custody, or scheduling creates logistical barriers.

Nevertheless, procedural convenience is not equivalent to meaningful access. A participant may lack a stable internet connection, suitable device,

digital literacy, accessible interface, or private space in which to communicate confidentially with counsel. Technical failures may interrupt testimony or prevent effective participation. Remote proceedings should therefore include contingency arrangements, accessibility support, identity verification, and safeguards for confidential lawyer-client communication.

The central conceptual point is that digital access should supplement, rather than automatically displace, appropriate physical and assisted procedures. Institutions should evaluate whether technology expands effective participation across different social and geographical groups.

6.2 Theme II: Technology-Enabled Investigation and Digital Policing

Digital information can assist investigations by helping establish timelines, identify communication patterns, locate relevant records, and corroborate or challenge witness accounts. The BNSS provisions on production of electronic communications and devices provide a procedural route for obtaining material that may be relevant to an investigation. The use of digital tools may also improve documentation and coordination.

However, the collection of digital material can involve extensive personal information unrelated to the alleged offence. Investigators must distinguish relevant material from unrelated private data, maintain records of access and extraction, and comply with applicable legal authorisation requirements. Broad or poorly documented collection can undermine privacy and create disputes over scope, reliability, and fairness.

Digital policing also depends on technical competence. Officers need training in lawful acquisition, preservation, documentation, and recognition of potential manipulation. Standard procedures should identify who collected the material, when and how it was obtained, what tools were used, and how the original data was protected. Technology can strengthen investigation only when supported by professional standards and accountability.

6.3 Theme III: Electronic Evidence, Authenticity, and Forensic Integrity

Digital records are potentially fragile and readily replicable. A screenshot, audio clip, video, chat

export, or device image may be incomplete, altered, misattributed, or separated from relevant context. The BSA's provisions on electronic records create a legal framework for their use, but evidentiary evaluation must still consider the requirements applicable to the particular record.

Four dimensions are especially important. First, authenticity asks whether the record is what it is represented to be. Second, integrity concerns whether the information has remained complete and unaltered. Third, provenance and chain of custody concern the history of acquisition, transfer, storage, and examination. Fourth, contextual reliability concerns whether the record is interpreted with sufficient information about its source, timing, and surrounding circumstances.

Forensic tools, including cryptographic hash values, write-protection methods, forensic imaging, and documented extraction procedures, can support integrity assessment when used appropriately. These tools do not eliminate the need for expert explanation, disclosure of limitations, or judicial evaluation. A hash value can help demonstrate that a file has not changed since a particular point in the process, but it cannot by itself prove that the file was genuine before that point. The BSA's statutory certificate schedule includes fields for identifying the digital source and recording hash values. Such documentation can contribute to traceability, but effective evidence management also requires secure storage, controlled access, preservation of relevant metadata, and the ability of the opposing party to challenge the evidence in accordance with law.

6.4 Theme IV: Privacy, Fair Trial, and the Risk of Digital Overreach

Digital investigations can expose sensitive personal information, including communications, location data, photographs, financial records, and information about third parties. The constitutional right to privacy, recognised by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), provides an important framework for examining state collection and use of personal information. The legality and constitutionality of a particular investigative measure depend on its legal basis, purpose, scope, and safeguards.

A rights-centred approach calls for purpose limitation, proportionality, access controls, secure retention, and

clear rules for handling information unrelated to the investigation. Where information is disclosed to the prosecution or relied upon in court, procedures should protect legitimate privacy interests without preventing a fair opportunity to challenge material evidence.

Fair-trial concerns also arise when one party has substantially greater access to technical expertise or digital material. Disclosure should be sufficiently meaningful to permit the defence to understand and challenge the evidence, subject to lawful protections. Courts should be alert to the risk that technical complexity may give digital evidence an appearance of certainty that its actual provenance or limitations do not justify.

6.5 Theme V: Institutional Readiness, Digital Divide, and Accountability

Technology-enabled justice requires more than software procurement. It depends on reliable connectivity, secure systems, trained staff, forensic capacity, maintenance, technical support, and clear institutional responsibility. Differences in resources between states, districts, and institutions may affect how consistently digital processes can be implemented.

The digital divide can affect victims, witnesses, accused persons, and lawyers. People with limited connectivity, disability-related access needs, language barriers, or low digital literacy may find electronic processes difficult to use. Institutions should provide assisted access, accessible formats, language support, and alternatives when technology would otherwise impair meaningful participation.

Accountability requires audit trails, documented access, incident reporting, independent review, and clear responsibility for errors or data breaches. Procurement and deployment decisions should be accompanied by training and evaluation. The success of a digital system should be measured by its contribution to lawful, reliable, and inclusive justice not merely by the number of processes moved online.

VII. DISCUSSION: TECHNOLOGY AS A MEANS, NOT AN END

The themes indicate that technology creates both capacity and risk. Electronic processes may improve coordination and reduce logistical barriers, while digital evidence can provide important investigative

leads and courtroom material. Yet each benefit depends on legal controls, technical quality, and institutional competence.

A useful distinction is between digitisation, digital capability, and justice outcomes. Digitisation means converting processes or records into electronic form. Digital capability involves the skills, infrastructure, and governance needed to use those systems reliably. Justice outcomes concern whether people experience fair, timely, accurate, accessible, and constitutionally compliant procedures. Progress at the first level does not automatically establish progress at the third.

Accordingly, digital transformation should be assessed against a set of mutually reinforcing criteria: legality, evidentiary integrity, privacy protection, inclusion, procedural fairness, and accountability. A system that is fast but inaccessible, technologically advanced but insecure, or efficient but opaque cannot be considered successful solely on the basis of its technical features.

VIII. PROPOSED CONCEPTUAL FRAMEWORK: ACCOUNTABLE DIGITAL CRIMINAL JUSTICE FRAMEWORK

This paper proposes the Accountable Digital Criminal Justice Framework (AD-CJF). It is an original conceptual proposition developed for this paper and has not been empirically validated.

The framework places technology-enabled criminal procedure and digital evidence at the centre, supported by five conditions: (a) legality and constitutional compliance; (b) authenticity and evidentiary integrity; (c) privacy and data security; (d) inclusion and meaningful access; and (e) institutional competence and accountability. These conditions are expected to support intended outcomes such as reliable evidence, fair participation, procedural timeliness, and public confidence.

The framework assumes that the dimensions interact. For example, secure evidence systems are of limited value if access is so restricted that a fair challenge becomes impossible; remote hearings may be efficient but undermine fairness if the accused cannot communicate privately with counsel. Future research

may operationalise the dimensions through indicators and examine them across jurisdictions and types of proceedings.

IX. MAJOR CONCEPTUAL FINDINGS

- a) Technology is an enabling instrument, not an independent guarantee of justice; outcomes depend on the legal and institutional conditions of use.
- b) The BNSS provides for electronic and audio-video processes in specified contexts, while the BSA recognises electronic and digital records subject to statutory requirements.
- c) Digital evidence requires attention to authenticity, integrity, provenance, context, and meaningful opportunities for challenge.
- d) Privacy and fair-trial protections remain central when state authorities obtain, analyse, retain, or disclose digital information.
- e) Remote and online procedures can improve convenience but may exclude people who lack connectivity, devices, accessibility support, or digital literacy.
- f) Effective implementation requires trained personnel, secure infrastructure, standard protocols, auditability, and continuing evaluation.

These findings are conceptual conclusions from legal and documentary analysis, not empirical measurements of implementation outcomes.

X. RECOMMENDATIONS

10.1 Adopt Standard Digital Evidence Protocols
Investigating agencies should maintain documented procedures for lawful acquisition, forensic imaging, hashing where appropriate, metadata preservation, chain of custody, secure storage, and disclosure. Protocols should be periodically reviewed as technology changes.

10.2 Strengthen Training and Forensic Capacity
Police, prosecutors, defence counsel, judicial officers, and forensic personnel should receive role-specific training in digital evidence, technical limitations, privacy, and evidentiary evaluation. Investment should include laboratories, secure systems, maintenance, and technical support.

10.3 Protect Privacy and Minimise Unnecessary Data
Digital collection and review should be limited to lawful purposes and relevant scope. Institutions should use access controls, retention rules, secure deletion where legally permissible, and procedures for handling unrelated or sensitive third-party information.

10.4 Preserve Fair Participation in Remote Proceedings

Remote participation should include reliable identity checks, accessible platforms, interpretation where required, technical support, contingency procedures, and confidential communication with legal counsel. Physical or assisted alternatives should be available when necessary to preserve meaningful participation.

10.5 Improve Disclosure and Contestability

Parties should receive legally appropriate access to the digital material and information necessary to understand its origin, extraction, processing, and limitations. Courts should be able to evaluate expert methods and consider challenges to authenticity or completeness.

10.6 Establish Accountability and Evaluation

Institutions should maintain audit trails, incident-reporting systems, clear responsibility for data handling, and periodic independent reviews. Evaluation should examine fairness, reliability, access, security, and timeliness rather than counting digital transactions alone.

10.7 Support Empirical Research

Future research should combine legal analysis with field studies of investigators, lawyers, judges, forensic experts, and court users. Comparative and longitudinal studies could examine whether digital systems improve access and timeliness without increasing exclusion, evidentiary disputes, or privacy risks.

XI. LIMITATIONS AND SCOPE FOR FURTHER RESEARCH

The paper is conceptual and doctrinal. It does not assess particular state-level implementations, analyse a dataset of criminal cases, or measure the actual effects of digital procedures. It also does not offer a comprehensive section-by-section commentary on the

BNSS and BSA. Statutory provisions and implementation practices may change, and any applied study should verify the law and rules in force at the relevant time.

Further research could operationalise the AD-CJF through indicators such as connectivity failures, time required for forensic processing, completeness of chain-of-custody records, frequency of evidentiary challenges, access to legal assistance, data-security incidents, and user experiences. Such work should account for differences in case type, institutional resources, geography, and the legal context of each proceeding.

XII. CONCLUSION

The new criminal laws in India provide a significant statutory setting for examining the expanding role of technology in criminal justice. The BNSS enables specified electronic and audio-video processes, while the BSA addresses the legal treatment and proof of electronic and digital records. These provisions can support investigation, procedural coordination, and access to proceedings, but their value depends on how they are implemented.

The central argument of this paper is that technology should be evaluated as a means of achieving justice rather than as an end in itself. Digital systems must operate within constitutional and statutory limits, preserve evidentiary integrity, protect privacy, support meaningful participation, and remain open to scrutiny. Without these conditions, digitisation may reproduce existing inequalities or introduce new risks.

The proposed Accountable Digital Criminal Justice Framework offers a structure for analysing the relationship between technological capability and rights-based justice. It identifies legality, evidentiary integrity, privacy, inclusion, and institutional accountability as mutually reinforcing conditions. As a conceptual framework, it invites empirical testing rather than claiming proven outcomes.

Ultimately, technology-driven criminal justice will be meaningful when it contributes to procedures that are reliable, fair, accessible, secure, and constitutionally compliant. Sustained training, infrastructure, transparent protocols, judicial scrutiny, and independent evaluation are therefore essential to translating technological potential into substantive justice.

REFERENCES

- [1] *Anvar P. V. v. P. K. Basheer*, (2014) 10 SCC 473.
- [2] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
- [3] *Bharatiya Nagarik Suraksha Sanhita*, 2023, No. 46 of 2023, India Code. India Code
- [4] *Bharatiya Sakshya Adhiniyam*, 2023, No. 47 of 2023, India Code. India Code PDF
- [5] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- [6] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
- [7] Ministry of Home Affairs, “New criminal laws: Use of audio-video electronic means under the Bharatiya Nagarik Suraksha Sanhita,” Press Information Bureau, Mar. 10, 2026. Press Information Bureau
- [8] Ministry of Home Affairs, “New criminal laws,” Government of India, n.d. Ministry of Home Affairs
- [9] Ministry of Home Affairs, “Guidelines for investigating officers on using the e-Sakshya app at the scene of crime,” Bureau of Police Research and Development, n.d. Bureau of Police Research and Development