



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

TECHNOLOGY AS THE NEW PROCEDURAL SAFEGUARD? A CRITICAL STUDY OF DIGITAL CRIMINAL JUSTICE UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

AUTHORED BY - KOMAL KAILASHNATH SHARMA

Institution - Shree L.R. Tiwari College of Law

Academic year or designation- 5th Year BA.LL.B. (2026–2027)

ABSTRACT

The Bharatiya Nagarik Suraksha Sanhita, 2023 shows a shift, towards using technology in criminal procedures in India. Electronic communication, digital investigation, electronic evidence, electronic service and virtual proceedings have become part of the procedural framework. While these developments may improve accessibility, efficiency and traceability, they also raise a deeper question that when does technology merely facilitate criminal procedure, and when can it function as a procedural safeguard?

This paper critically examines this question through a five-dimensional framework of traceability, authenticity, transparency, proportionality and accountability. It analyses the role of technology across the criminal procedure lifecycle, including digital initiation of proceedings, electronic service, investigation and device custody, electronic evidence, virtual proceedings and the consequences of technological failure. The study further deals with the technological imbalance between State agencies and accused persons and considers the continuing digital presence of criminal allegations even after proceedings have concluded.

The paper develops five interconnected concepts which are Chain of Digital Accountability, Functional Equivalence, Digital Equality of Arms, Digital Failure Safeguard and Digital Closure Protocol to assess whether technological processes preserve meaningful procedural rights. It argues that digitisation by itself does not guarantee fairness- electronic transmission may not amount to meaningful notice, digital evidence may require greater verification, virtual presence may not ensure meaningful participation, and technological capacity may increase both investigative power and privacy risks.

The study concludes that technology can operate as a procedural safeguard only when its use remains traceable, verifiable, transparent, proportionate and institutionally accountable. Digital

criminal justice should therefore move beyond technological adoption towards accountable digitisation, ensuring that increased State capacity does not diminish individual procedural protection.

Keywords: Bharatiya Nagarik Suraksha Sanhita, 2023; Digital Criminal Justice; Procedural Safeguards; Electronic Evidence; Digital Accountability; Due Process.

INTRODUCTION

Criminal process determines the manner in which the coercive power of the State is exerted against an individual. It governs the initiation of criminal proceedings, investigation, collection and preservation of evidence, appearance before courts, adjudication and the communication of judicial decisions. Its purpose, therefore, cannot be reduced to ensuring that a case moves efficiently from one procedural stage to another. Criminal procedure must also ensure that the exercise of State power remains subject to fairness, legality and meaningful judicial scrutiny. The Supreme Court has repeatedly treated Articles 14 and 21 as requiring substantive and procedural fairness, recognising that “procedure established by law” must be just, fair and reasonable.¹

A major technology component has been added to this procedural framework by the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS"). Its provisions recognise electronic communication in the initiation of criminal proceedings, electronic service of processes, technological documentation during investigation and electronic modes of conducting trials, inquiries and proceedings. Section 173, for instance, permits information relating to a cognizable offence to be given by electronic communication, while Section 530 provides for trials, inquiries and proceedings to be held in electronic mode.² As a result, technology is now integrated into criminal procedure rather than just being an administrative tool used in conjunction with it.

This transformation presents an important constitutional and procedural question. Does converting a procedural act into a digital form necessarily make that process more protective of rights? An electronic complaint may reduce barriers to approaching the police, but questions remain regarding authentication, registration and subsequent accountability. Digital investigation may enable investigators to preserve and analyse substantial quantities of

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 173, 530, India Code (2023), <https://www.indiacode.nic.in/bitstream/123456789/20099/1/eng.pdf>

information, but the same capability may expose personal and third-party data far beyond what is necessary for the investigation. Virtual proceedings may improve access to courts, but physical absence may also affect communication with counsel, effective participation and the ability to follow or challenge evidence.

The constitutional significance of these concerns becomes particularly clear in relation to privacy. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a constitutionally protected right connected with liberty, dignity and individual autonomy. The Court further developed proportionality as a means of examining restrictions upon fundamental rights.³ Digital criminal investigation consequently raises a question not merely of whether the State possesses technological access, but whether the particular access is legally justified, directed towards a legitimate purpose and proportionate to that purpose.

The problem is not technology itself. Digital systems can create advantages that conventional paper-based processes may not provide. Properly designed systems can create verifiable records, preserve procedural histories, facilitate communication, assist in the preservation of evidence and enable participation without physical presence. The difficulty arises when technological capacity is mistaken for procedural protection. A system may record everything without making the record reliable; transmit information without ensuring meaningful notice; preserve evidence without making it effectively challengeable; or collect extensive personal information without adequately limiting its use.

This paper approaches that problem by distinguishing between a digital procedural mechanism and a digital procedural safeguard. A mechanism determines how a procedural act is performed. A safeguard performs a further function that it constrains the exercise of State power, protects an individual's procedural position, or facilitates meaningful scrutiny and challenge. On this basis, the paper proposes five criteria for determining when technology performs a safeguarding function: traceability, authenticity, transparency, proportionality and accountability.

These criteria provide the analytical framework for examining technology across the criminal-procedure lifecycle. Traceability asks whether the procedural history can be reconstructed. Authenticity asks whether a digital record or process can be reliably verified. Transparency asks whether the affected person can understand and challenge what has occurred. Proportionality asks whether technological powers are exercised only to the extent necessary for a legitimate procedural purpose. Accountability asks who bears responsibility when a

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

technological process produces an error, loses information, compromises participation or otherwise fails.

The inquiry also extends beyond the immediate stages of investigation and trial. Digital criminal justice can have consequences after proceedings have legally concluded because electronically stored allegations, case records and searchable information may continue to shape an individual's informational identity.

The paper does not contend that the BNSS's technological provisions are inherently either rights-enhancing or rights-restrictive. Instead, it argues that their constitutional value depends upon the conditions governing their operation. The central proposition is that technology can become a procedural safeguard only where its use is accompanied by mechanisms capable of making the process traceable, authentic, transparent, proportionate and accountable.

RESEARCH GAP

The rapid incorporation of technology into Indian criminal procedure has already generated substantial legal scholarship. Recent research has analyzed the statutory and evidential repercussions of the BNSS and the Bharatiya Sakshya Adhiniyam, 2023 (“BSA”), notably in relation to electronic evidence, digital investigation, virtual proceedings and forensic processes. The emerging scholarship therefore makes it difficult to sustain a claim that the technological provisions of the BNSS remain completely unexplored. The research gap lies elsewhere: in how these individual technological mechanisms are conceptually connected to procedural safeguards and constitutional accountability.

Existing scholarship has examined the importance of electronic evidence and digital procedures under the BNSS, including e-FIRs, electronic trials, chain of custody and the interaction between the BNSS and BSA.⁴ Other recent work has focused more specifically on the evidentiary and forensic dimensions of digital criminal justice, including authentication, certification, and chain of custody and the institutional limitations of forensic infrastructure.⁵ Scholarship has also considered electronic records and video conferencing in relation to efficiency, summary trials, access to justice and due process.⁶ Further literature has examined digitalisation from the perspective of prosecution, witness protection, search and

Mohan Kumar G, The Importance of Electronic Evidence and Digital Procedures Under BNSS, J. Emerging Trends & Novel Res. (2026), <https://rjpn.org/jetnr/viewpaperforall.php?paper=JETNR2608071>
Shobhita Singh & Shaiwalini Singh, The Epistemological Crisis of Digital Evidence: Navigating India's Transition to the BSA and BNSS, 6 Indian J. Legal Rev. 184 (2026), <https://ijlr.iled.edu.in/v6i421/>
A. Barsad Begam, K.J. Rajan & Akash J., Digital Forensics and Electronic Evidence Under the Bharatiya Sakshya Adhiniyam, 2023: Judicial Trends and Challenges in Cybercrime Trials, 41 Int'l J. Special Educ. 277 (2026), <https://www.internationalsped.com/index.php/ijse/article/view/5485>

seizure, and investigative powers.⁷

These studies provide an important foundation, but they predominantly examine particular technological mechanisms, evidentiary questions, institutional challenges or efficiency implications. Even where procedural safeguards are discussed, they are generally considered in relation to the specific mechanism under examination. This paper approaches the problem differently. It asks whether these apparently separate mechanisms can be evaluated through a single procedural-safeguard framework. It proposes that technology should be treated as a procedural safeguard only where its operation satisfies five interconnected requirements: traceability, authenticity, transparency, proportionality and accountability.

The paper's contribution is consequently not another catalogue of BNSS technology provisions. It examines the relationship between technological capacity and procedural protection across the criminal-procedure lifecycle. It further addresses questions that arise when technology fails, when the State possesses substantially greater technological resources than the accused, and when digital criminal records continue to affect an individual after the proceedings have legally concluded.

The research thus shifts the inquiry from “What has BNSS digitised?” to “Under what conditions does digitisation protect procedural rights?” This distinction forms the basis of the paper's proposed Digital Procedural Safeguard Framework.

RESEARCH QUESTIONS

The following research questions serve as the basis for this study:

1. In what ways has technology been integrated into the various stages of criminal procedure in the Bharatiya Nagarik Suraksha Sanhita, 2023?
2. To what extent can electronic processes under the BNSS strengthen traceability, authenticity, transparency and accountability within criminal proceedings?
3. What procedural and constitutional concerns arise from increased reliance on digital investigation, electronic evidence and virtual proceedings?
4. Does electronic communication necessarily ensure meaningful notice, participation and access to justice?
5. How should privacy and proportionality operate when digital investigation enables access to large volumes of personal and third-party information?

Ankita Kumari Dhaker & Priyanka Joshi, Role of Electronic Records and Video Conferencing in Accelerating Summary Trials Under BNSS, 2023, J. Advances & Scholarly Res. Allied Educ. (2026), <https://www.ignited.in/index.php/jasrae/article/view/16430>

6. What procedural consequences should follow where a technological system fails, electronic evidence is compromised, or digital communication does not achieve its intended procedural purpose?
7. Does the technological advantage available to State agencies create a meaningful imbalance between the prosecution and the accused, and if so, what safeguards can address that imbalance?
8. How should criminal justice systems respond to the continued digital existence of allegations and criminal records after proceedings have legally concluded?
9. Under what conditions can technology move beyond administrative efficiency and operate as a genuine procedural safeguard?

OBJECTIVES

The objectives of this research are:

1. Examine the principal technological mechanisms incorporated into the BNSS and their relationship with criminal procedural rights.
2. Analyze whether electronic processes improve the traceability, authenticity, transparency, proportionality and accountability of criminal procedure.
3. Examine the constitutional implications of digital criminal justice with particular reference to fairness, privacy, due process and meaningful participation.
4. Evaluate the procedural implications of electronic evidence, digital investigation and virtual proceedings.
5. Develop standards for addressing technological failure without unfairly transferring institutional failures onto the individual.
6. Examine the problem of digital equality of arms between State agencies and accused persons.
7. Analyse the continuing digital consequences of criminal proceedings after acquittal, discharge, quashing or other final outcomes.
8. Develop a Digital Procedural Safeguard Framework capable of evaluating technology across the criminal-procedure lifecycle.
9. Propose practical safeguards that can enable technological efficiency while preserving procedural fairness and constitutional accountability.

HYPOTHESIS

The present study proceeds on the hypothesis that:

According to the Bharatiya Nagarik Suraksha Sanhita, 2023, "technological incorporation into criminal procedure can increase procedural safeguards only provided it is complemented by suitable measures of traceability, authenticity, transparency, proportionality, and accountability."

The hypothesis is premised on the distinction between technological efficiency and procedural fairness. The mere conversion of a physical process into an electronic one does not necessarily make the process more accessible, reliable or constitutionally compliant. Electronic communication may fail to provide meaningful notice, digital evidence may require independent verification, virtual proceedings may not always ensure effective participation, and expanded investigative access to personal data may create proportionality concerns.

The study therefore proceeds on the assumption that technology becomes a genuine procedural safeguard only when the legal system simultaneously provides the individual with an effective ability to know, participate, verify, challenge and obtain a remedy in relation to technologically mediated criminal processes.

RESEARCH METHODOLOGY

In order to investigate the role of technology in criminal procedure under the Bharatiya Nagarik Suraksha Sanhita, 2023, this study adopts a doctrinal, analytical, and critical research technique.

The Constitution of India, the BNSS, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and pertinent Supreme Court and High Court rulings are among the primary legal materials used in this doctrinal study. Statutory rules, procedural directions and relevant institutional materials concerning technology-enabled criminal proceedings are also considered where they directly inform the operation of the statutory framework.

The research is analytical because it examines the relationship between technological mechanisms and established principles of criminal procedure, fairness, due process, privacy, proportionality, meaningful participation and the ability to challenge State action. Judicial decisions are analysed not merely for their outcomes but for the procedural principles that can be applied to digital criminal processes.

The study is further critical in examining whether technological mechanisms under the BNSS

actually perform a safeguarding function or merely improve procedural administration. For this purpose, the paper develops five analytical criteria which is traceability, authenticity, transparency, proportionality and accountability. Secondary materials, including books, scholarly articles, legal commentaries, research papers and institutional publications, are used to identify existing academic approaches and locate the present study within the developing literature on digital criminal justice.

The scope of the research is confined primarily to the procedural implications of technology under the BNSS. The paper neither conducts an empirical evaluation of technology infrastructure nor makes unsubstantiated assertions about the actual performance of certain organizations.

CONCEPTUALISING DIGITAL PROCEDURAL SAFEGUARDS

The incorporation of technology into criminal procedure requires a distinction between a digital procedural mechanism and a digital procedural safeguard. A mechanism determines how a procedural act is performed; a safeguard performs the additional function of controlling the exercise of State power and protecting the procedural position of the person affected by that power. When assessing the technological architecture presented by the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS"), this distinction is crucial.

The BNSS contains several provisions through which technology becomes part of ordinary criminal procedure. Information about a cognizable offense may be communicated electronically under Section 173, subject to the legal necessity for authentication. Electronic summons service and associated procedures are recognized in Sections 63 to 71. Section 193 incorporates requirements concerning the custody of electronic devices and electronic communication of specified investigative information. Section 530 further provides for trials, inquiries and proceedings to be held in electronic mode.⁸ These provisions demonstrate that digital technology is intended to operate across multiple stages rather than as an isolated procedural convenience.

The constitutional significance of this transformation must nevertheless be assessed against established principles of procedural fairness. In *Maneka Gandhi v. Union of India*, the Supreme Court rejected a narrow understanding of procedure under Article 21 and held that the procedure affecting personal liberty must satisfy requirements of fairness and

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 63–71, 173, 193, 530, India Code (2023), <https://www.indiacode.nic.in/bitstream/123456789/20099/1/eng.pdf>

reasonableness.⁹The principle is particularly relevant where technology changes the manner in which a person receives notice, participates in proceedings, encounters State investigative power or challenges material relied upon against them.

Similarly, the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India becomes significant where digital criminal investigation permits access to extensive quantities of personal information.¹⁰The technological ability to collect or process information cannot, by itself, determine the constitutional legitimacy of such access. Questions of purpose, necessity, proportionality and safeguards remain relevant.

A. Traceability

Traceability concerns whether a procedural event can subsequently be reconstructed. A traceable system should permit identification of relevant procedural actions, their sequence and, where appropriate, the authority responsible for them. Electronic records can potentially strengthen traceability by creating time-stamped and reproducible procedural histories.

However, traceability is meaningful only where the underlying record is reliable. A detailed digital trail of an unreliable or improperly generated record cannot itself establish procedural legitimacy.

B. Authenticity

Authenticity concerns whether the digital record or process can be reliably verified. Electronic evidence raises particular concerns because digital information may be copied, modified, transferred or reproduced without obvious physical indicators of alteration. In order to demonstrate the integrity and evidentiary validity of electronic records, the statutory framework governing them becomes crucial.

Authenticity must also be distinguished from truth. Establishing that a digital record is genuine does not automatically establish that every factual proposition contained within it is true. The former is a question of reliability and provenance; the latter remains a matter for evidentiary evaluation.

C. Transparency

Transparency requires that the affected person be able to understand the procedural action sufficiently to exercise the corresponding legal right. Consequently, electronic transmission cannot always be equated with meaningful notice, just as virtual presence cannot automatically be equated with meaningful participation.

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

Transparency therefore includes accessibility, comprehensibility, disclosure and a realistic opportunity to respond or challenge.

D. Proportionality

Proportionality operates as a limiting principle on the expanded informational capacity of digital criminal justice. A digital device may contain substantially more information than is relevant to a particular investigation. Therefore, the question is not just whether information is technically accessible, but also whether the legitimate purpose for which it is sought justifies the level of access.

This dimension connects digital criminal procedure with constitutional privacy principles and prevents technological convenience from becoming a substitute for legal necessity.

E. Accountability

Accountability asks who bears responsibility for a digital procedural action and what remedy exists when the process fails. A technological system cannot become an independent bearer of legal responsibility. Decisions concerning its adoption, operation, preservation and correction remain attributable to institutions and authorized persons. This becomes particularly important where technological failure results in missed notice, loss of evidence, interruption of proceedings or inaccurate digital records.

The five dimensions are interdependent. Traceability without authenticity may produce a detailed but unreliable record; authenticity without transparency may leave the affected person unable to challenge it; transparency without proportionality may expose excessive personal information; and all four without accountability may leave procedural failure without an effective remedy.

DIGITAL INITIATION AND ELECTRONIC PROCESSES UNDER THE BNSS

The first point at which technology encounters an individual's rights within the criminal process is often the initiation and communication of proceedings. The BNSS significantly expands the role of electronic communication at this stage. Section 173 permits information relating to a cognizable offence to be given by electronic communication, while Sections 63 to 71 provide for electronic modes concerning summons and their service.¹¹ These provisions show why digital transmission cannot be automatically equated with procedural compliance, but they also have the ability to lower administrative and geographical barriers.

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 63–71, 173.

A. Electronic Information and the Digital Initiation of Criminal Process

Section 173 permits information relating to a cognizable offence to be communicated electronically, with the informant required to authenticate it within the statutory period.¹² The provision can make the first point of contact with the criminal justice system more accessible, particularly where physical presence at a police station presents practical difficulties.

Its significance, however, extends beyond convenience. Registration of criminal information can itself have serious consequences for individuals. The constitutional importance of timely registration is reflected in *Lalita Kumari v. Government of Uttar Pradesh*, where the Supreme Court held that registration of an FIR is mandatory where information discloses a cognizable offence, subject to the limited circumstances in which a preliminary inquiry is permissible.¹³ The BNSS retains this basic procedural architecture while introducing an electronic route for communication.

The digital format therefore creates a new accountability question that what happens between electronic submission and formal registration? A technically successful transmission should not permit an electronically submitted complaint to disappear into an administrative system without a traceable outcome. A meaningful digital process should permit the procedural history of the information to be reconstructed from receipt and authentication to registration, allocation, investigation and communication of subsequent developments. This paper describes this as the Chain of Digital Accountability.

B. Electronic Summons and Meaningful Notice

The BNSS also permits electronic service of summons and related processes. Sections 63 to 71 establish the statutory framework for summons, including electronic modes of service and the preservation of proof of service.¹⁴ The principal advantage is obvious that electronic communication can substantially reduce delay and make service less dependent upon physical delivery.

Nevertheless, transmission and notice are not identical concepts. A summons' legal aim is to give the individual in question enough information to fulfill the legal responsibility placed upon them, not just to get a message out of a court-controlled system.

This distinction becomes particularly important when different statutory notices carry different legal consequences. In proceedings concerning Section 35 of the BNSS, the Supreme Court has specifically cautioned against treating electronic communication under the general

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 173(1).
Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1.
Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 63–71.

electronic-proceedings provision as automatically authorising service of a Section 35 notice through WhatsApp or other electronic modes. The Court emphasised that the statutory requirements governing such notice cannot be circumvented merely by relying upon electronic modes.¹⁵

The principle emerging from this distinction may be termed Meaningful Notice that the reliability required for electronic service should correspond to the legal consequence attached to the communication.

C. The Graduated Reliability Principle

This leads to a further proposition of this paper, the Graduated Reliability Principle. Not every electronic communication should require an identical level of authentication, proof of receipt and verification. The greater the procedural consequence of non-compliance, the stronger the justification for requiring reliable proof that the communication reached the intended recipient in a legally sufficient manner.

For example, an informational communication may require less rigorous verification than a notice where failure to respond may affect liberty or result in significant procedural consequences. This approach prevents the language of technological efficiency from obscuring differences in legal consequence.

D. Applying the Five-Part Framework

The digital initiation and service mechanisms under the BNSS can consequently be assessed through the proposed framework:

1. Traceability- electronic submissions and service should leave a verifiable procedural trail.
2. Authenticity- the system should establish that the communication originates from the authorised source and reaches the intended recipient through a legally recognized channel.
3. Transparency- the person should be able to understand what has been communicated and what action is required.
4. Proportionality- the system should not demand unnecessary personal information merely to facilitate digital communication.
5. Accountability- responsibility should remain identifiable where information is not registered, service fails or an electronic record is incorrectly maintained.

The significance of these requirements is that they transform electronic communication from a

Satender Kumar Antil v. Central Bureau of Investigation, 2025 SCC OnLine SC (order dated Jan. 21, 2025).

question of speed into a question of procedural reliability. The objective is not to reject digital processes because they introduce new risks, but to ensure that those risks do not undermine the procedural rights that the underlying physical process was intended to protect.

DIGITAL INVESTIGATION AND THE CHAIN OF DIGITAL ACCOUNTABILITY

The evidential relationship between the State and the individual is fundamentally altered when technology is used into criminal investigations. A standard investigation may involve physical documents, objects and witnesses whose collection and handling can often be observed or reconstructed through comparatively tangible records. Digital investigation is different. A single device may contain vast quantities of communications, photographs, location information, financial records, browsing history and information belonging to persons other than the accused. The investigative value of such material is substantial, but so is the possibility of over-collection, alteration, loss or misuse.

The BNSS recognises this changed investigative environment. Section 193 requires the police report to contain, among other matters, information concerning the sequence of custody of an electronic device where such device is relevant to the investigation.¹⁶ This requirement is important because it shifts the emphasis from the manufacture of a digital device to the device's procedural history and the data it contains.

A. From Chain of Custody to Chain of Digital Accountability

Traditional chain-of-custody principles primarily ask whether an item produced before the court is the same item that was collected during investigation and whether its integrity has been maintained. In digital investigations, that inquiry remains essential, but it is insufficient by itself.

The more appropriate question is not merely that who possessed the device? It is also that who accessed the information, for what purpose, through what process, what was extracted, what was retained, and what was ultimately disclosed?

This paper therefore proposes the concept of a Chain of Digital Accountability. It consists of five interconnected stages:

1. Seizure - identification and lawful acquisition of the device or digital material;
2. Preservation - protection against alteration, deletion or contamination;

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 193(3)(i).

3. Acquisition - extraction or copying of relevant information through an identifiable process;
4. Analysis - examination of the information, including the tools and methodology used where legally relevant; and
5. Disclosure - making relevant material available in a manner that permits meaningful scrutiny and challenge.

The intention is not to impose an artificial requirement that all technical operations be included in the trial record. Rather, the objective is to ensure that where digital evidence materially affects an individual's liberty, its procedural history remains sufficiently reconstructable to permit judicial scrutiny.

B. Authenticity Is Not the Same as Truth

The distinction between authenticity and truth becomes particularly important in digital investigations. The Supreme Court's jurisprudence on electronic records has consistently treated the proof of electronic material as a matter requiring compliance with the applicable evidentiary framework. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, while interpreting Section 65B of the Indian Evidence Act, distinguished the original electronic record from computer outputs and emphasised the statutory requirements governing proof of electronic records.¹⁷ The BSA has the statutory framework for electronic and digital records was later reorganized, but the fundamental issue is still that a court must be able to ascertain the nature of the digital material and how its evidentiary status is formed before assessing what it establishes.

Accordingly, a hash value, metadata, forensic image or certificate may assist in establishing integrity or provenance, but none should be treated as independently establishing the truth of the factual proposition for which the material is relied upon. Authenticity protects the reliability of the record; substantive evidentiary evaluation determines its significance.

C. Digital Investigation and Proportionality

The capacity of digital forensic tools also creates a privacy problem that is qualitatively different from many conventional searches. A mobile phone may contain information that is entirely unrelated to the suspected offence and may include communications and personal information concerning family members, colleagues or other third parties.

The constitutional right to privacy therefore imposes an important constraint upon digital investigation. In *K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

privacy as a constitutionally protected right and applied proportionality to restrictions upon that right.¹⁸ Subsequent Supreme Court decisions have articulated proportionality through considerations including legitimate purpose, suitability, necessity and balancing of competing interests.¹⁹

The implication for digital investigation is that the ability to access information cannot itself constitute the justification for accessing it. Investigative relevance should remain connected to the purpose for which access is authorised. Where a device contains information substantially beyond that purpose, appropriate safeguards concerning search, review, retention and disclosure become necessary.

D. Disclosure and the Accused's Ability to Challenge

Digital investigation also changes the meaning of disclosure. Providing the accused with a large volume of electronic material does not necessarily constitute meaningful disclosure if the material is technically inaccessible, poorly organised or impossible to understand without specialised tools.

The procedural value of disclosure lies in enabling the accused to know the material relied upon and to challenge it effectively. Consequently, the Digital Equality of Arms principle developed in this paper requires attention not merely to whether electronic material has technically been supplied, but whether the accused has a reasonable opportunity to inspect, understand and contest material capable of affecting the outcome.

This is particularly important where the prosecution possesses specialised forensic tools, trained personnel or proprietary software that the accused cannot reasonably access. The State's technological advantage should not become an evidentiary advantage insulated from meaningful scrutiny.

E. The Five-Part Application

Digital investigation can therefore be evaluated through the proposed framework:

1. Traceability- the history of seizure, preservation, acquisition, analysis and disclosure should be reconstruct able.
2. Authenticity- the integrity and provenance of electronic material should be capable of verification.
3. Transparency- the accused should have sufficient information to understand and challenge material relied upon.

K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 SCC 1.

4. Proportionality- In order to prevent needless information intrusion, investigative access must stay linked to a valid aim.
5. Accountability- responsibility for investigative decisions and failures should remain attributable to identifiable authorities.

The significance of the Chain of Digital Accountability is ultimately that it places a procedural obligation alongside technological capability. The more powerful the State's capacity to discover digital information becomes, the greater the need for a corresponding capacity to explain, verify, limit and account for its use.

Digital investigation can consequently operate as a procedural safeguard when its technological power is accompanied by institutional discipline. Without that discipline, the same technology that preserves evidence and improves investigative accuracy may also enable indiscriminate data collection, obscure the investigative process and make meaningful challenge more difficult.

ELECTRONIC EVIDENCE AND DATA MINIMISATION

The increasing dependence upon digital investigation necessarily places electronic evidence at the centre of contemporary criminal procedure. The Bharatiya Sakshya Adhiniyam, 2023 ("BSA") expressly recognises electronic and digital records within the evidentiary framework. Section 61 provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital, subject to the requirements of Section 63. Section 63 establishes the statutory conditions governing the admissibility of electronic records produced from computers and communication devices.²⁰

This statutory recognition is important, but admissibility should not be confused with reliability or relevance. A digital record may satisfy the conditions necessary for admission while still requiring careful judicial evaluation of what it establishes. The distinction between authenticity, admissibility and probative value is therefore central to a rights-sensitive digital criminal process.

A. Authenticity, Integrity and Evidentiary Value

Electronic evidence differs from many conventional forms of evidence because its reproduction does not necessarily result in a visibly distinguishable physical copy. Emails, messages, server records, location information, photographs, audio files and other digital material can exist

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, India Code (2023), <https://www.indiacode.nic.in/bitstream/123456789/20063/1/aa202347.pdf>

across multiple systems and devices. The BSA's definition of “document” expressly includes electronic and digital records such as emails, server logs, computer records, smartphone data, messages and locational evidence.²¹

The legal question is therefore not simply whether a digital record exists, but whether the court can sufficiently determine its provenance and integrity. This reinforces the Chain of Digital Accountability developed in the preceding section. Preservation, extraction and production must remain capable of explanation where the reliability of the material is disputed. At the same time, authenticity should not be allowed to become a substitute for substantive evaluation. Digital evidence should therefore be assessed through ordinary principles of relevance, reliability and proof in addition to the requirements specifically applicable to electronic records.

B. Data Minimisation as a Procedural Requirement

The greater concern arises before the digital material reaches the courtroom. The same device that contains potentially relevant evidence may also contain enormous quantities of intensely personal and irrelevant information.

A smartphone can simultaneously contain evidence relating to an alleged offence and information concerning health, finances, family relationships, professional communications, photographs, location history and communications with persons who have no connection with the investigation. The constitutional privacy framework provides an important limitation. Justice K.S. Puttaswamy (Retd.) v. Union of India recognised privacy as a fundamental right and connected it with dignity, autonomy and liberty.²² Where digital investigation interferes with privacy, the existence of investigative utility must therefore be considered alongside the legality and necessity of the interference.

This paper accordingly proposes Data Minimisation as a procedural principle of digital investigation. It does not require investigators to ignore potentially relevant information. Rather, it requires the scope of collection, examination, retention and disclosure to remain connected to the legitimate purpose for which the investigative power is exercised.

C. Disclosure Must Be Usable

Digital evidence also changes the nature of disclosure. A prosecution may technically provide thousands of electronic files to the accused while still making effective scrutiny difficult. File volume, unfamiliar formats, inaccessible software, poor organisation or the absence of relevant

Id. § 2(1)(d).
Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

metadata may transform formal disclosure into an ineffective procedural exercise.

The objective of disclosure is not merely to transfer data. Its purpose is to give the accused a significant chance to comprehend and contest evidence used by the prosecution. This connects electronic evidence directly with Digital Equality of Arms. The same concern applies to exculpatory material.

D. Retention and the Lifecycle of Digital Evidence

The evidentiary lifecycle does not necessarily end when material is admitted or rejected at trial. Digital material may continue to exist across investigative databases, court systems and institutional archives. This creates a distinction between retention for a legitimate legal purpose and indefinite exposure or unrestricted accessibility.

The distinction becomes particularly significant when a proceeding concludes without conviction. A criminal justice system may have legitimate reasons to preserve an underlying judicial record while having substantially weaker reasons to permit unrestricted dissemination of every associated personal detail. This issue is developed further in the paper's discussion of the digital afterlife of an accused person.

The central proposition emerging from this analysis is therefore-

“Authenticity protects the reliability of what the State uses; proportionality protects the individual from what the State does not need to use.”

Electronic evidence can consequently strengthen criminal justice only when the legal system regulates not merely whether digital information can be used, but also how much information is collected, how its integrity is established, how it is disclosed, and what happens to it after its procedural purpose has ended.

VIRTUAL PROCEEDINGS AND MEANINGFUL PARTICIPATION

The use of audio-video technology in criminal proceedings represents one of the most visible forms of digital transformation under the BNSS. Section 530 expressly provides that trials, inquiries and proceedings may be held in electronic mode.²³ The provision has the potential to reduce geographical barriers, facilitate the appearance of persons who cannot conveniently attend court physically and reduce delays associated with transporting accused persons, witnesses or experts. The High Court of Uttarakhand's 2025 rules, for example, recognise electronic hearings, video-conferencing appearances, recording of witness testimony and

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 530.

several other procedural stages through audio-video means.²⁴

Yet the legal significance of virtual proceedings cannot be assessed solely by asking whether a person was technically present on screen. The more important question is whether the electronic mode preserves the procedural function of physical participation.

A. From Physical Presence to Functional Equivalence

The Supreme Court addressed the validity of video-conferencing for recording evidence in *State of Maharashtra v. Dr. Praful B. Desai*, holding that recording evidence through video-conferencing could satisfy the requirement of the witness being present before the court where the essential features of examination and cross-examination were preserved.²⁵ The decision demonstrates that physical presence is not necessarily the only means through which a procedural function can be achieved.

The principle can be extended into what this paper terms Functional Equivalence-

“Where criminal procedure is conducted through electronic means, the electronic process should preserve the substantive procedural function of its physical counterpart.”

Functional equivalence does not require technological and physical proceedings to look identical. It requires them to provide materially comparable procedural opportunities.

B. Virtual Presence Is Not Necessarily Meaningful Participation

A person may technically appear through video conference while experiencing interruptions, inadequate audio, limited visibility or an inability to communicate privately with counsel. These circumstances demonstrate why virtual presence and meaningful participation must remain conceptually distinct.

The distinction is particularly important for an accused person. Criminal proceedings may involve questions of liberty, evidence, identification, examination of witnesses and legal submissions. If technological conditions prevent the accused from following proceedings or communicating effectively with counsel, the formal availability of a video link cannot by itself establish meaningful participation.

The same concern applies to witnesses. A video link may make testimony geographically possible, but the integrity of testimony may depend upon the witness being able to hear questions clearly, understand objections and respond without technological distortion.

C. Digital Evidence and the Right to Challenge

High Court of Uttarakhand, Electronic Communication and Audio-Video Electronic Means (Nyay Shruti) Rules, 2025, rr.4.14.9(2025), https://upload.indiacode.nic.in/showfile?actid=AC_UK_89_393_00007_00007_17576751_21346&filename=the_high_court_of_uttarakhand_electronic_communication_and_audiovideo_electronic_means_%28nyay_shruti%29_rules%2C_2025.pdf&type=hindirule
State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.

Virtual proceedings also affect the presentation and examination of electronic evidence. The Supreme Court's proceedings in *CBI v. Mohd. Yasin Malik* illustrate that technological methods may be used to facilitate participation and transmission of material in proceedings conducted through video conference. The Court dealt with the appearance of the respondent through video conference and procedural arrangements surrounding the proceedings.²⁶

The broader principle is that technology should facilitate, rather than diminish, the opportunity to confront and challenge material relied upon in a criminal proceeding. A digital document displayed on a screen, for example, should remain capable of being identified, examined and questioned in accordance with the applicable evidentiary rules.

Thus, the question should not be whether the court can display evidence electronically. It should be whether the parties have a realistic opportunity to examine and contest it.

D. Technological Failure During Material Proceedings

The possibility of technological failure introduces another procedural concern. Connectivity may be interrupted during the examination of a witness, an accused's response, the presentation of evidence or a material submission. Not every interruption will affect the fairness of the proceeding. However, where the interruption occurs at a procedurally significant moment, simply continuing the hearing may create an incomplete or unreliable record.

The court should therefore distinguish between technical inconvenience and material procedural prejudice. Where the latter occurs, appropriate remedies may include repetition of the affected portion, adjournment, restoration of an opportunity to cross-examine or another effective procedural cure.

E. Applying the Five-Part Framework

Virtual proceedings illustrate the operation of the five dimensions particularly clearly:

1. Traceability- the electronic proceeding should generate a reliable record of what occurred.
2. Authenticity- recordings and electronic documents should remain capable of verification.
3. Transparency- participants should be able to understand the proceeding and its procedural consequences.
4. Proportionality- technology should be used to facilitate participation without creating unnecessary restrictions or surveillance.

Central Bureau of Investigation v. Mohd. Yasin Malik & Ors., Crim. App. Nos. 1786–1787 of 2025 (Sup. Ct. Apr. 4, 2025).

5. Accountability- responsibility should be identifiable where technological conditions materially compromise participation.

Technology can expand access to criminal courts, but access is meaningful only when accompanied by effective participation. A video link that technically connects an accused to a courtroom but prevents meaningful communication with counsel or effective engagement with evidence may satisfy connectivity while failing the deeper requirement of procedural fairness. The appropriate constitutional approach is consequently one of functional equivalence rather than technological substitution.

WHEN TECHNOLOGY FAILS - PROCEDURAL CONSEQUENCES OF DIGITAL FAILURE

The effectiveness of a digital criminal justice system cannot be assessed only by examining situations in which technology operates successfully. A procedural system that increasingly depends upon electronic communication, digital evidence and virtual proceedings must also determine who bears the consequences when the technology fails. Connectivity failures, corrupted files, inaccessible platforms, lost electronic records, defective transmission and technical incompatibility can affect the ability of an accused, witness, victim or court to perform a procedural act. The legal system must therefore distinguish between an ordinary technical inconvenience and a technological failure capable of producing procedural prejudice. This issue assumes greater significance because digital systems are increasingly becoming institutional infrastructure rather than optional conveniences. The Supreme Court's 2026 National Conference on Judicial Process Re-engineering and Digital Transformation specifically emphasised robust digital preservation, disaster-recovery mechanisms, standardised electronic-evidence management and institutional control over technological transformation.²⁷

A. Technology Failure as a Procedural Event

A failure in a digital criminal process may occur at several stages. An electronic summons may not reach its intended recipient; a virtual hearing may be interrupted; a digital file may become inaccessible; electronic evidence may be overwritten before preservation; or a system-generated record may contain an error.

The important question is whether the failure has merely inconvenienced the proceeding or has

Supreme Court of India, National Conference on Judicial Process Re-engineering and Digital Transformation, Press Release (Apr. 11, 2026), <https://www.sci.gov.in/press-release-dated-april-11-2026/>

altered a person's ability to exercise a procedural right.

The Madhya Pradesh High Court's judicial training material concerning electronic evidence specifically identifies preservation during trial, CCTV, call-detail records, mobile data and compliance with Sections 193, 230 and 503 BNSS as connected issues requiring judicial attention.²⁸ This reflects the broader point that preservation is itself a procedural responsibility.

B. Institutional Technological Responsibility

This paper proposes the principle of Institutional Technological Responsibility-

“Where a criminal procedure is conducted through a technological system selected, controlled or mandated by the State or court, a person should not ordinarily suffer an adverse procedural consequence merely because that system failed, unless the failure is attributable to that person or the governing law expressly provides otherwise.”

The principle does not create immunity from procedural requirements. A person who deliberately refuses to use an available system, provides false information or causes the technical failure cannot automatically rely upon technological failure as a defence.

The Supreme Court has also recently emphasised, in interpreting electronic communication under the BNSS, that statutory restrictions on electronic modes cannot simply be bypassed in the name of technological convenience. The Court linked those restrictions to the protection of Article 21.²⁹

C. The Technological Attribution Test

To determine whether a technological failure should affect procedural rights, this paper proposes a five-stage Technological Attribution Test-

1. Identify the failure - What exactly failed?
2. Identify control - Which institution or participant controlled the relevant technological system?
3. Assess reasonable accessibility - Could the affected person reasonably have avoided or corrected the failure?
4. Determine material prejudice - Did the failure affect a substantive procedural opportunity?
5. Identify the cure - Can the prejudice be effectively remedied?

This approach prevents every technical problem from becoming a ground for reopening proceedings while ensuring that material technological failures receive appropriate procedural

Madhya Pradesh State Judicial Academy, Electronic Evidence Training Material (2025), https://mpsja.mphc.gov.in/Joti/pdf/EV/Time%20Table%20ECT_14%20%2806.12.2025%29.pdf
Satender Kumar Antil v. Central Bureau of Investigation, 2025 SCC OnLine SC.

attention.

D. Irreversible Digital Failure

Some technological failures cannot be completely cured. Electronic material may be automatically overwritten; a corrupted recording may not be recoverable; metadata may be lost; or a relevant communication may never have been successfully transmitted.

In such circumstances, the legal response cannot be based upon the assumption that every digital loss is equivalent to the loss of a physical document. The court may need to consider whether the unavailable material was potentially material, whether its absence prejudices a party and whether alternative evidence can adequately address the loss.

DIGITAL EQUALITY OF ARMS AND CONSTITUTIONAL CONCERNS

The digitalisation of criminal procedure does not distribute technological capacity equally among the participants in a criminal proceeding. Investigating agencies and prosecution authorities may have access to forensic laboratories, specialised software, centralised databases, trained technical personnel and interconnected criminal-justice platforms. An accused person, particularly one without substantial financial or technical resources, may not possess comparable capacity to understand, verify or challenge technologically generated material. The resulting concern is not whether the State and accused must possess identical technology, but whether the accused retains a meaningful ability to contest the exercise of State power.

This paper therefore uses the expression Digital Equality of Arms to describe the procedural condition in which technological advantages available to the State do not become an unreviewable evidentiary or investigative advantage.

A. Technological Asymmetry and the Accused

The problem begins with the nature of digital evidence itself. A prosecution may rely upon forensic extraction, location records, device data, server information or other technically generated material that an accused may be unable independently to reproduce or interpret. Formal disclosure of such material may therefore be insufficient if the accused cannot reasonably understand its origin, methodology or significance.

The requirement of equality of arms does not mean that every accused must be provided with the same technological infrastructure available to the State. Rather, it requires procedural arrangements capable of ensuring that technological complexity does not prevent meaningful challenge. This is particularly important where the State's investigative power extends to

personal digital devices. Section 94 of the BNSS permits a court or police officer, subject to the statutory requirements, to require production of documents, electronic communications and communication devices likely to contain digital evidence.³⁰ The breadth of such material makes judicial supervision particularly important.

In October 2025, the Supreme Court clarified the procedural handling of digital devices produced under Section 94. Where an investigating officer directs production of a digital device, the direction is to produce the device before the jurisdictional court; the court is then to hear the concerned party and advocate regarding objections to the information sought from the device.³¹ This approach is significant because it places an element of judicial scrutiny between investigative access and unrestricted examination of potentially extensive personal information.

B. Articles 14 and 21 in the Digital Context

The constitutional framework reinforces this requirement. Article 14's guarantee against arbitrary State action and Article 21's protection of personal liberty operate together to require fairness in criminal procedure. *Maneka Gandhi v. Union of India* established that procedure affecting personal liberty cannot be arbitrary and must satisfy standards of fairness and reasonableness.³²

Digital criminal procedure does not create an alternative constitutional standard. If anything, the increased informational and investigative capacity of the State makes the existing standards more significant. The concern can be expressed through a simple proposition- "Digitisation should expand the State's capacity to discover evidence without diminishing the accused's capacity to challenge it."

This requires courts to examine not merely whether digital material has been collected lawfully, but whether the accused has received a meaningful opportunity to understand and contest material upon which the prosecution relies.

C. Technology as a Constraint on State Power

Technology should not be viewed exclusively as an instrument that strengthens the prosecution. Properly designed systems may also constrain State action.

Section 105 of the BNSS, for example, requires the process of search and seizure to be recorded through audio-video electronic means and transmitted to the Magistrate.³³ Such recording can

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 94(1).
Suo Motu Writ Petition (Crim.) No. 2 of 2025 & Ors., Supreme Court of India, Order dated Oct. 31, 2025, https://api.sci.gov.in/supremecourt/2025/35619/35619_2025_1_1503_65372_Judgement_31-Oct-2025.pdf
Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 105.

create an objective procedural record against which disputed accounts of the search may subsequently be examined.

Similarly, the requirement in Section 193 concerning the sequence of custody of an electronic device can create an evidentiary trail capable of subjecting investigative handling to judicial scrutiny.³⁴

D. Digital Equality of Arms Framework

The analysis supports six practical requirements-

1. Meaningful disclosure - relevant digital material must be provided in a usable form.
2. Technical understandability- The accused should be given a fair chance to comprehend the creation or interpretation of important digital content.
3. Opportunity for verification - where authenticity or methodology is disputed, meaningful verification should be possible.
4. Preservation of potentially exculpatory material - digital evidence should not be preserved solely according to its apparent usefulness to the prosecution.
5. Reasonable technical assistance - appropriate cases may require access to technical expertise necessary to challenge complex evidence.
6. Protection against excessive data access - investigative technology should not expose information beyond what is reasonably necessary for the legitimate purpose.

These requirements do not seek to obstruct legitimate investigation. They seek to ensure that investigative sophistication does not make judicial scrutiny merely theoretical.

THE DIGITAL AFTERLIFE OF AN ACCUSED PERSON

The conclusion of proceedings is typically seen in criminal procedure as the end of the immediate procedural interaction between the State and the accused. An FIR, charge-sheet, judgment, order, news report or database entry may remain searchable long after the legal proceedings have concluded. The result is a distinction between legal finality and digital permanence: a proceeding may be legally over while its digital representation continues to affect the person concerned.

This problem is particularly significant where the final outcome is an acquittal, discharge or quashing. A person may therefore experience what this paper describes as a digital afterlife of accusation the continued association of an individual's name with criminal allegations even after the legal process has moved beyond those allegations.

Id. § 193(3)(i).

A. Legal Finality and Digital Persistence

Whether or not criminal records should be erased is not the only issue. Criminal justice institutions may have legitimate reasons to preserve judicial and investigative records. The more specific question is whether permanent name-based searchability and unrestricted public accessibility are necessary for retention.

The distinction between retention and accessibility is increasingly recognised in Indian judicial discourse. In *Laksh Vir Singh Yadav v. Union of India*, decided by the Delhi High Court in May 2026, the Court considered petitions concerning de-indexing and masking of judicial records and digital content, including cases involving acquittal, discharge and quashing. The Court treated informational privacy, dignity and the practical effect of digital searchability as relevant considerations, while also recognising the competing importance of open justice and public interest.³⁵

This distinction permits four different responses to digital criminal information:

1. Erasure - removal of the underlying information;
2. Masking - removal or concealment of identifying particulars;
3. De-indexing - preventing name-based search results from directly locating the material while retaining the source;
4. Restricted accessibility - limiting access according to legitimate legal or institutional purposes.

These remedies should not be treated as interchangeable.

B. The Digital Closure Protocol

The analysis supports the Digital Closure Protocol proposed in this paper. When criminal proceedings legally conclude, digital systems should be capable of recognising and accurately reflecting that conclusion.

The protocol should involve:

1. identifying the final legal outcome;
 2. updating interconnected records;
 3. assessing the continuing legal purpose of retention;
 4. assessing the appropriate level of public accessibility;
 5. providing mechanisms for correction, masking or de-indexing where legally justified;
- and

Laksh Vir Singh Yadav v. Union of India, 2026 SCC OnLine Del. (May 29, 2026), <https://indiankanoon.org/doc/4658201/>

6. preserving the integrity of the underlying judicial record.

THE DIGITAL PROCEDURAL SAFEGUARD FRAMEWORK

The preceding analysis demonstrates that the technological provisions of the BNSS cannot be evaluated adequately by asking whether a particular process has become electronic. Electronic initiation, digital investigation, electronic evidence, virtual proceedings and digital record management each alter the manner in which criminal procedure operates, but their constitutional and procedural value depends upon the safeguards accompanying their use. Therefore, the main contribution of this article is to assess these mechanisms using a single Digital Procedural Safeguard Framework that consists of five interrelated dimensions: accountability, traceability, authenticity, transparency, and proportionality.

A. Traceability

Traceability concerns whether the history of a procedural action can be reconstructed. In digital criminal procedure, this includes identifying when information was received, when an electronic process was issued or served, how a device was handled, how evidence was extracted and what subsequent procedural actions occurred.

Traceability is particularly significant because digitisation can either strengthen or weaken institutional visibility. A properly designed electronic system can create a reliable audit trail; an inadequately designed system may instead create an opaque administrative layer in which actions are difficult to reconstruct.

B. Authenticity

Authenticity concerns whether the digital record or process can be verified. It requires attention to provenance, integrity, preservation and the applicable evidentiary requirements.

The importance of authenticity is particularly evident in electronic evidence. A digital record cannot acquire evidentiary reliability merely because it has been generated electronically. Its origin, integrity and manner of production may remain relevant to judicial assessment. The principle also applies to electronic communication and virtual proceedings. The system should be able to verify that an electronic record is authentic and hasn't been inappropriately altered when a procedural consequence depends on it.

C. Transparency

Transparency requires more than electronic availability. A procedural action must be capable of being understood and challenged by the person affected by it.

This principle underlies the distinction developed earlier between electronic transmission and

meaningful notice. Similarly, the concept of Functional Equivalence requires virtual proceedings to preserve the substantive opportunities associated with physical participation. Transparency therefore requires the system to answer practical questions: What has happened? What information has been relied upon? What action is required from the individual? What opportunity exists to challenge the action?

D. Proportionality

Proportionality limits the use of technological capacity. Digital systems permit the State to collect, connect and analyse substantially more information than may have been practically accessible through conventional investigative methods.

This is particularly significant in relation to digital devices. The presence of potentially relevant information on a device does not mean that all information contained on that device is equally relevant or necessary. The privacy implications of digital investigation therefore require the State's technological capacity to remain connected to a legitimate procedural purpose. Data minimisation, limited retention and appropriate restrictions on access are consequently not merely data-management principles. Within digital criminal procedure, they become components of procedural proportionality.

E. Accountability

Accountability is the connecting element of the framework. A technological system cannot itself bear constitutional responsibility. Responsibility remains with the institutions and persons who authorise, operate, maintain and rely upon the system.

This becomes particularly important when technology fails. The Digital Failure Safeguard developed in this paper proceeds from the principle that a person should not ordinarily suffer an adverse procedural consequence merely because a State-controlled or court-controlled technological system failed. The appropriate response requires consideration of control, material prejudice and available remedies.

Accountability also extends beyond individual procedural events. Where a digital criminal record fails to reflect an acquittal, discharge or other final outcome, the system should provide a mechanism for correction or appropriate restriction. This is the basis of the Digital Closure Protocol.

FINDINGS

The preceding analysis establishes that the technological transformation introduced by the BNSS presents both procedural opportunities and new forms of procedural risk. The principal

finding of this study is that digitisation does not independently produce fairness. Its contribution to criminal justice depends upon the legal and institutional safeguards surrounding its operation.

1. Digitalisation can strengthen procedural traceability. Electronic communication, digital records and electronic custody information can create a more reconstructable procedural history. However, this advantage depends upon reliable audit trails and proper institutional maintenance.
2. Electronic transmission cannot automatically be equated with meaningful procedural notice. The legal significance of a communication depends upon the consequence attached to it. This supports the Graduated Reliability Principle, under which greater procedural consequences require correspondingly stronger standards of authentication and proof of service.
3. Digital investigation expands both evidentiary capability and privacy risk. A single device can contain extensive information unrelated to the offence under investigation. Consequently, technological capacity must remain subject to purpose limitation and proportionality.
4. Authenticity and truth remain distinct. Establishing the integrity or provenance of an electronic record does not by itself establish the truth of the proposition contained within it. Digital evidence therefore requires both technical verification and ordinary judicial evaluation of relevance and probative value.
5. Virtual presence does not necessarily amount to meaningful participation. The procedural function of physical participation must be preserved when proceedings are conducted electronically. This is the basis of the paper's principle of Functional Equivalence.
6. Technological inequality can affect the fairness of criminal proceedings. State agencies may possess greater forensic and technological resources than an accused. The appropriate response is not identical technological capacity, but a meaningful opportunity for the accused to understand, verify and challenge technologically generated evidence.
7. Technological failure must be treated as a procedural issue. Where a State-controlled technological system prevents a person from exercising a procedural right, the resulting prejudice should not automatically become that person's procedural default. This supports the proposed Digital Failure Safeguard.

8. Criminal procedure can have consequences beyond legal finality. Digital records may continue to associate an individual with criminal allegations even after acquittal, discharge or quashing. The legal status of a proceeding should therefore be capable of being accurately reflected within relevant digital systems.

RECOMMENDATIONS

Based on these findings, the study recommends the following:

1. Adopt uniform digital procedural standards. Rules and institutional protocols should incorporate the five requirements of traceability, authenticity, transparency, proportionality and accountability into technology-enabled criminal processes.
2. Establish standardised digital audit trails. Significant electronic procedural actions should generate verifiable records identifying the relevant action, time, authorised user or institution and subsequent modification where applicable.
3. Introduce graduated standards for electronic service. The reliability and proof required for electronic communication should correspond to the legal consequence attached to the communication.
4. Strengthen preservation and disclosure of electronic evidence. Electronic material should be preserved through reliable procedures, and disclosure should be sufficiently organised and accessible to permit meaningful scrutiny by the accused.
5. Incorporate a Digital Failure Safeguard. Where a court or State-controlled technological system fails, courts should consider attribution, material prejudice and available remedies before imposing an adverse procedural consequence.
6. Strengthen Digital Equality of Arms. The accused should have a fair chance to comprehend and contest the source, technique, and interpretation of any technologically difficult evidence that significantly impacts the case.
7. Apply data minimization to digital investigation. With the proper restrictions about irrelevant and third-party information, investigative access should stay related to the lawful reason for which it is authorized.
8. Establish a Digital Closure Protocol. Legally significant outcomes such as acquittal, discharge and quashing should be capable of being accurately reflected in interconnected digital records, while distinguishing legitimate retention from unrestricted public accessibility.

9. Maintain identifiable human responsibility. Technological systems should assist criminal justice institutions without displacing institutional responsibility for consequential procedural decisions or system failures.

The recommendations collectively support a broader proposition: the objective of digital criminal justice should not be maximum digitisation, but accountable digitisation. Technology should increase the State's ability to administer criminal justice without correspondingly reducing the individual's ability to understand, participate in and challenge that process.

CONCLUSION

The Bharatiya Nagarik Suraksha Sanhita, 2023 signifies a substantial change in the way criminal proceedings can be started, looked into, recorded, and carried out. By recognising electronic communication, digital records, electronic service and proceedings through electronic means, the BNSS places technology within the ordinary architecture of criminal justice rather than treating it merely as an administrative convenience. The significance of this transformation, however, cannot be measured by the extent to which physical processes are replaced by digital ones.

This study has demonstrated that digitisation and procedural fairness are not synonymous. Electronic communication may improve accessibility without guaranteeing meaningful notice; digital investigation may improve evidentiary capacity while increasing privacy risks; electronic evidence may be technically authentic without conclusively establishing the truth of its contents; and virtual proceedings may provide physical-distance solutions without necessarily ensuring meaningful participation. Technological failure may also create procedural prejudice if institutional failures are automatically attributed to the individual. The hypothesis advanced by this paper is therefore supported: technology can strengthen procedural safeguards under the BNSS only when technological capacity is accompanied by appropriate legal and institutional controls. The five dimensions developed through this study are traceability, authenticity, transparency, proportionality and accountability which provides a framework for determining whether a digital mechanism actually performs a safeguarding function.

The paper's additional concepts are the Chain of Digital Accountability, Functional Equivalence, Digital Equality of Arms, Digital Failure Safeguard and Digital Closure Protocol which demonstrate how these principles can operate at different stages of the criminal-procedure lifecycle. Together, they shift the focus from technological adoption to technological

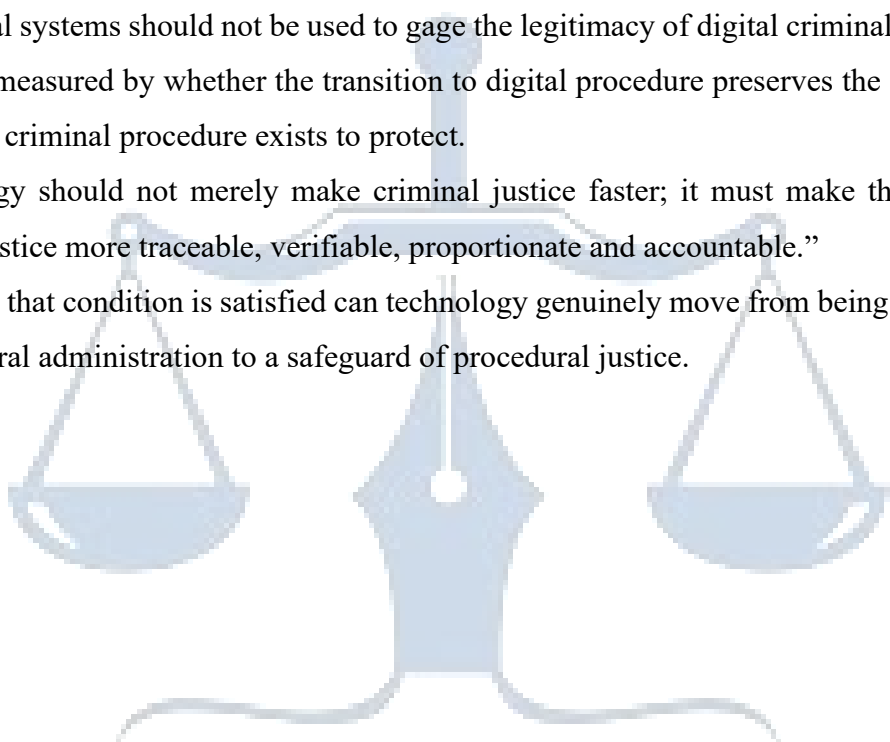
responsibility.

The central concern is therefore not whether technology should have a place in criminal procedure. Its place is already established. The more important question is how that technological power should be governed. A rights-sensitive digital criminal justice system must ensure that the State's increased capacity to collect, process and communicate information is accompanied by an equally meaningful capacity of the individual to understand, verify, challenge and obtain a remedy.

In the end, the number of electronic processes or the speed at which information flows through institutional systems should not be used to gage the legitimacy of digital criminal procedure. It should be measured by whether the transition to digital procedure preserves the constitutional values that criminal procedure exists to protect.

“Technology should not merely make criminal justice faster; it must make the exercise of criminal justice more traceable, verifiable, proportionate and accountable.”

Only when that condition is satisfied can technology genuinely move from being a mechanism of procedural administration to a safeguard of procedural justice.



WHITE BLACK
LEGAL