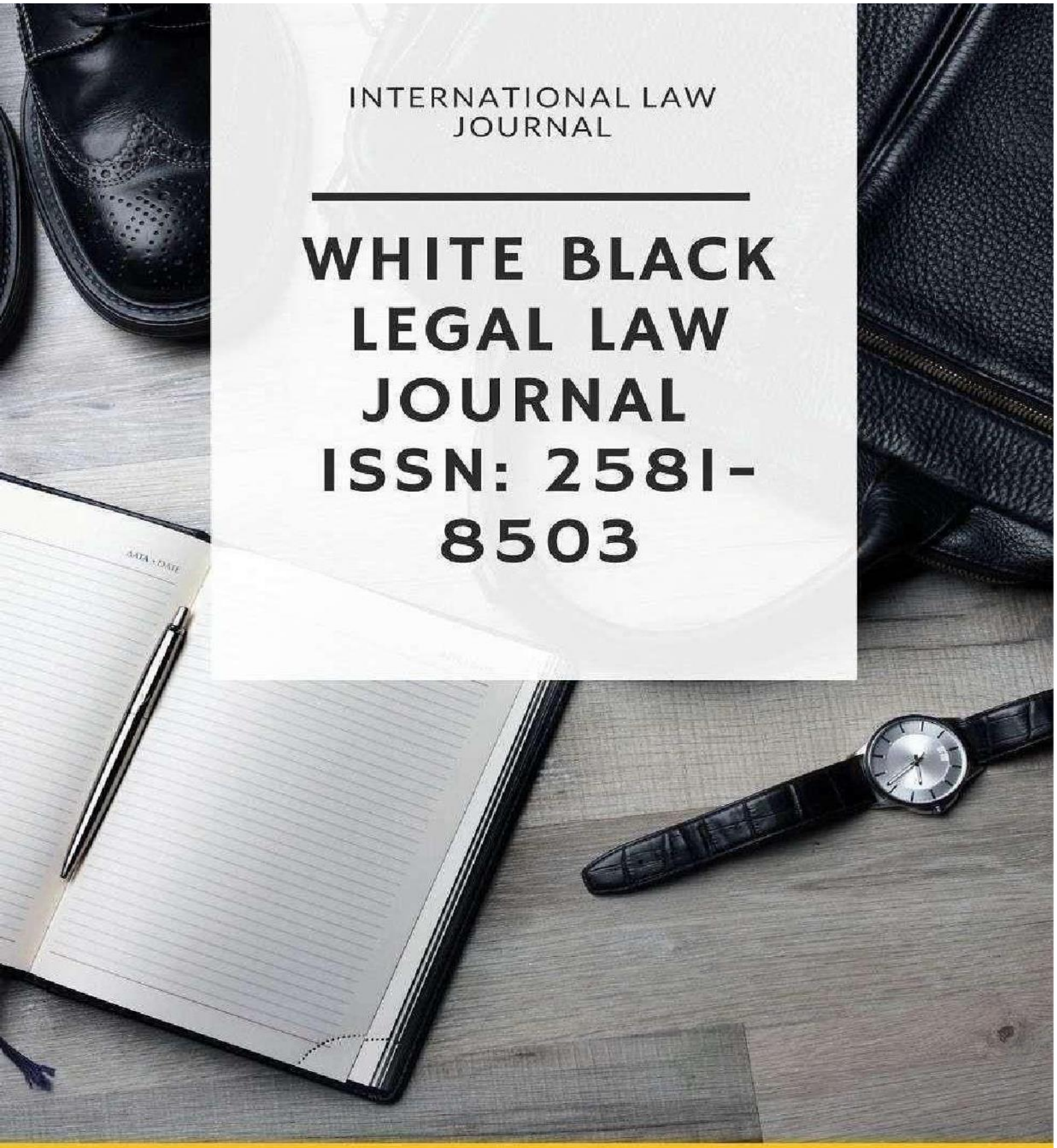

INTERNATIONAL LAW JOURNAL

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.

www.whiteblacklegal.co.in
Volume 3 Issue 7 | June 2026 ISSN: 2581-8503

DIGITAL EVIDENCE AND THE RIGHT TO A FAIR TRIAL IN INDIA: A CRITICAL ANALYSIS OF THE EMERGING LEGAL FRAMEWORK

AUTHORED BY - DR. CHITRA SHARMA

Abstract

The exponential growth of digital technologies has fundamentally transformed the nature of criminal investigations and judicial proceedings across jurisdictions. Electronic communications, cloud-based storage, artificial intelligence, Internet of Things (IoT) devices, digital surveillance systems, social media platforms, blockchain records, and encrypted messaging applications have increasingly become the primary repositories of evidentiary material in criminal litigation. Recognising this technological evolution, the Indian legislature enacted the **Bharatiya Sakshya Adhiniyam, 2023 (BSA)**, replacing the century-old **Indian Evidence Act, 1872 (IEA)** with an objective of modernising evidentiary rules and adapting them to a digital-first legal ecosystem. The enactment represents one of the most significant reforms in Indian evidentiary jurisprudence since Independence, particularly by according statutory recognition to electronic and digital records as primary forms of evidence.

Despite these progressive legislative developments, substantial constitutional and procedural concerns continue to surround the treatment of digital evidence in criminal trials. Unlike conventional documentary evidence, electronic records are inherently volatile, easily replicable, susceptible to manipulation, and dependent upon sophisticated technological processes for their acquisition, preservation, authentication and interpretation. Consequently, questions regarding authenticity, integrity, admissibility and forensic reliability assume unprecedented importance. These concerns become particularly acute when viewed through the constitutional lens of **Article 21 of the Constitution of India**, which guarantees not merely procedural fairness but a substantive right to a fair, transparent and meaningful criminal trial.

This paper critically examines whether the Bharatiya Sakshya Adhiniyam, 2023 adequately reconciles technological innovation with constitutional safeguards. It analyses the transition from the Indian Evidence Act to the BSA, evaluates the evolving jurisprudence of the Supreme Court of India on electronic evidence, and explores the continuing deficiencies in forensic protocols, disclosure obligations, judicial capacity and procedural transparency. The paper argues that while the BSA simplifies the admissibility framework for electronic evidence, it

simultaneously expands prosecutorial reliance on technologically complex evidence without creating corresponding safeguards to protect the accused.

The study further contends that the absence of a nationally standardised digital chain of custody, mandatory disclosure of forensic metadata, accreditation of forensic laboratories and independent judicial scrutiny of digital forensic methodologies undermines the constitutional guarantee of equality of arms. Drawing upon comparative jurisprudence from the United Kingdom, United States, Singapore and the European Union, the paper proposes a comprehensive framework for strengthening digital due process within India's criminal justice system. It concludes that meaningful procedural transparency, rather than mere statutory recognition of electronic evidence, constitutes the true foundation of fairness in the digital age.

Keywords: Digital Evidence, Bharatiya Sakshya Adhiniyam 2023, Electronic Records, Article 21, Fair Trial, Criminal Justice, Digital Forensics, Chain of Custody, Constitutional Due Process.

I. Introduction

The twenty-first century has witnessed an unprecedented digital transformation affecting every sphere of human interaction. Communication, commerce, banking, governance, healthcare and education increasingly operate through interconnected digital infrastructures that continuously generate enormous volumes of electronic information. Criminal activity has evolved alongside this technological revolution. Contemporary offences frequently involve smartphones, encrypted messaging platforms, cloud storage, surveillance cameras, biometric systems, GPS devices, cryptocurrency transactions and artificial intelligence-assisted technologies. Consequently, the traditional conception of evidence—centred upon oral testimony, physical documents and tangible objects—has undergone a profound transformation.

Digital evidence has emerged not merely as supplementary material but often as the principal basis upon which criminal liability is established. Mobile phone records reconstruct an individual's movements; WhatsApp conversations reveal conspiracies; CCTV footage determines the sequence of events; metadata authenticates documents; cloud storage preserves incriminating communications; and digital payment trails establish financial transactions. The evidentiary value of these technological artefacts has consequently become indispensable to modern criminal adjudication.

Indian evidence law, however, was originally conceived during the colonial period when

neither computers nor electronic communications existed. The **Indian Evidence Act, 1872**, drafted principally by Sir James Fitzjames Stephen, represented a remarkable codification for its time. Nevertheless, its provisions were fundamentally designed for an era in which documentary evidence existed exclusively in physical form. The advent of computers exposed significant conceptual limitations within the statute, particularly regarding the admissibility and authentication of electronic records.

The Information Technology Act, 2000 attempted to address this legislative vacuum by introducing Sections 65A and 65B into the Indian Evidence Act. These provisions established a specialised framework governing electronic records, requiring a certificate certifying the manner of production and authenticity of electronic evidence. Although intended to ensure reliability, these procedural requirements generated extensive judicial controversy. Divergent interpretations by the Supreme Court created uncertainty regarding whether electronic evidence could be admitted without statutory certification, thereby complicating criminal prosecutions and civil litigation alike.

The enactment of the **Bharatiya Sakshya Adhiniyam, 2023** constitutes Parliament's attempt to overcome these doctrinal ambiguities. The BSA recognises electronic and digital records more comprehensively and seeks to harmonise evidentiary rules with contemporary technological realities. It symbolises a paradigm shift from treating electronic evidence as an exceptional category requiring elaborate procedural justification towards recognising digital information as an ordinary component of modern litigation.

However, legislative modernisation alone cannot guarantee constitutional justice. Digital evidence differs fundamentally from traditional evidence in ways that directly implicate the constitutional right to a fair trial. Unlike physical evidence, digital information can be duplicated without perceptible alteration, modified remotely, encrypted, selectively extracted or interpreted through proprietary forensic software whose functioning remains inaccessible to the defence. The apparent precision of digital evidence frequently conceals significant methodological assumptions and technological limitations.

These concerns assume constitutional significance because Article 21 of the Constitution protects not merely formal legality but substantive fairness. Judicial interpretation has consistently recognised that the right to life and personal liberty encompasses procedural due process, equality before criminal courts and meaningful opportunities to challenge prosecutorial evidence. If digital evidence is accepted without adequate scrutiny of its technological reliability, the constitutional balance between effective prosecution and individual liberty risks being fundamentally disturbed.

The problem is particularly acute in the Indian criminal justice system, where disparities in technological resources between the prosecution and the defence remain substantial. State investigative agencies increasingly rely upon specialised cyber forensic laboratories equipped with sophisticated analytical software, while many accused persons lack both the financial resources and technical expertise necessary to independently verify digital evidence. Consequently, the adversarial system may gradually transform into one characterised by technological asymmetry rather than procedural equality.

Furthermore, judicial institutions themselves confront significant challenges in evaluating technologically sophisticated evidence. Questions concerning hash algorithms, metadata integrity, blockchain verification, encryption protocols, digital imaging, volatile memory acquisition and forensic software validation frequently arise in contemporary criminal trials. These matters require specialised technical understanding that conventional legal education seldom provides. Excessive judicial deference to forensic reports therefore risks converting expert opinion into virtually conclusive evidence, thereby undermining the judicial function of independent evaluation.

The significance of these issues extends beyond evidentiary doctrine. Digital evidence increasingly intersects with broader constitutional concerns relating to privacy, informational self-determination, surveillance, algorithmic governance and state accountability. Following the Supreme Court's recognition of privacy as a fundamental right, the acquisition and utilisation of digital evidence must satisfy constitutional standards of legality, necessity, proportionality and procedural safeguards. The legitimacy of criminal adjudication consequently depends not only upon whether evidence is legally admissible but also upon whether its collection and interpretation respect constitutional guarantees.

Against this backdrop, the present research critically examines the emerging legal framework governing digital evidence in India. It seeks to determine whether the Bharatiya Sakshya Adhiniyam sufficiently protects the constitutional right to a fair trial while simultaneously facilitating effective criminal investigation in an increasingly digitised society.

II. Research Methodology

This study adopts a **doctrinal and analytical research methodology**. It primarily relies upon constitutional provisions, statutory interpretation, judicial precedents, Law Commission reports, parliamentary materials and scholarly legal literature. The research further incorporates comparative legal analysis by examining selected jurisdictions that have developed advanced

evidentiary frameworks for digital evidence.

The study is descriptive insofar as it traces the historical development of electronic evidence within Indian law. Simultaneously, it adopts a critical normative approach by evaluating whether existing legal frameworks adequately protect constitutional guarantees under Article 21. Comparative references to foreign jurisdictions serve not as models for direct transplantation but as analytical tools for identifying institutional best practices capable of informing future reforms within India.

III. Review of Literature

Academic scholarship on electronic evidence has expanded considerably during the last decade, reflecting the increasing centrality of digital technologies within criminal justice systems worldwide. Early scholarship primarily focused upon questions of admissibility under Section 65B of the Indian Evidence Act. Following the Supreme Court's decisions in *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, scholarly attention shifted towards the practical implications of mandatory certification requirements.

Constitutional scholars have increasingly examined digital evidence through the broader framework of due process and procedural fairness. Their central concern is that technological sophistication often creates asymmetries between prosecutorial agencies and accused persons, thereby undermining the principle of equality of arms. Contemporary scholarship also highlights the growing influence of proprietary forensic software, algorithmic decision-making and automated evidence analysis, raising important questions concerning transparency, accountability and judicial oversight.

International literature similarly emphasises that digital evidence presents challenges fundamentally distinct from conventional documentary evidence. Unlike physical documents, electronic records depend upon technological environments for their creation, preservation and interpretation. Consequently, reliability cannot be evaluated merely by examining the document itself but requires scrutiny of the entire technological ecosystem within which the evidence was generated and processed.

Despite these valuable contributions, relatively limited scholarship has examined the Bharatiya Sakshya Adhiniyam from the combined perspectives of constitutional due process, forensic science and comparative criminal procedure. This paper seeks to bridge that gap by integrating doctrinal analysis with constitutional theory and contemporary developments in digital forensic practice.

IV. Evolution of Electronic Evidence in India: From the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023

The law governing documentary evidence in India has historically reflected the technological realities of its respective era. When enacted in 1872, the Indian Evidence Act contemplated documents as physical manifestations of human communication—paper manuscripts, printed materials, official records and signed instruments. Authenticity depended primarily upon handwriting, signatures, seals and oral testimony regarding execution.

The emergence of computers during the late twentieth century fundamentally disrupted these assumptions. Unlike paper documents, digital files possess no fixed physical existence. They are created, stored, transmitted and reproduced through binary code that remains invisible to ordinary human perception. Multiple identical copies may exist simultaneously without any discernible distinction between the "original" and its replicas. Traditional evidentiary concepts consequently proved increasingly inadequate.

The Information Technology Act, 2000 represented the first comprehensive legislative attempt to integrate electronic records into Indian evidence law. By introducing Sections 65A and 65B into the Indian Evidence Act, Parliament recognised electronic records as legally admissible while imposing procedural safeguards intended to ensure reliability. Section 65B established a specialised evidentiary regime requiring certification of the conditions under which electronic evidence was produced. The provision sought to balance technological flexibility with evidentiary authenticity, yet its practical implementation generated persistent litigation and interpretative uncertainty.

The evolution of judicial doctrine under these provisions ultimately revealed a deeper conceptual dilemma. Should digital evidence be treated merely as another category of documentary evidence, or does its unique technological character require an entirely distinct jurisprudential framework? The Bharatiya Sakshya Adhiniyam, 2023 represents Parliament's latest attempt to answer this question, signalling a decisive movement towards recognising digital evidence as an integral component of contemporary adjudication rather than an exceptional evidentiary category.

V. The Structural Transformation under the Bharatiya Sakshya Adhiniyam, 2023

The enactment of the **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** represents a watershed moment in the evolution of Indian evidentiary law. Unlike the Indian Evidence Act, 1872,

which was enacted during an era when documentary evidence existed exclusively in tangible form, the BSA acknowledges that the contemporary justice system operates within a technologically integrated society where digital records frequently constitute the most reliable and probative evidence.

One of the most significant conceptual changes introduced by the BSA is the statutory recognition of electronic and digital records as primary forms of documentary evidence. This shift is not merely semantic but reflects a broader legislative acknowledgement that the distinction between physical and digital documents has largely disappeared in modern governance, commerce and criminal investigation. Government records are now digitally maintained, financial transactions are electronically documented, contracts are executed through electronic signatures, and communications increasingly occur through encrypted digital platforms. Consequently, treating electronic records as exceptional forms of evidence would be inconsistent with contemporary technological realities.

The transition from the Indian Evidence Act to the BSA also attempts to reduce procedural uncertainty that characterised the operation of Section 65B of the former legislation. Under the previous regime, admissibility frequently depended more upon technical compliance with certification requirements than upon the substantive reliability of the evidence itself. Minor procedural defects often resulted in the exclusion of otherwise reliable electronic evidence, thereby frustrating both criminal prosecution and civil adjudication.

Nevertheless, the BSA retains the requirement of certification for certain categories of electronic records. This retention demonstrates that Parliament itself recognises an inherent distinction between digital information and conventional documentary evidence. Unlike paper documents, electronic records may be altered invisibly, duplicated infinitely and transmitted without perceptible changes. Their evidentiary value therefore depends not merely upon their content but upon the integrity of the technological processes through which they were collected, preserved and analysed.

The BSA therefore embodies what may appropriately be described as a **"certification paradox."** On one hand, the legislation elevates electronic records to the status of primary evidence, signalling legislative confidence in digital technologies. On the other hand, it simultaneously retains procedural safeguards that implicitly acknowledge continuing concerns regarding authenticity and manipulation.

This paradox has profound implications for criminal trials. Certification alone cannot establish authenticity if the underlying forensic methodology remains opaque. A certificate merely confirms that certain procedural requirements have been fulfilled; it does not independently

verify whether the device was seized correctly, whether forensic imaging preserved all relevant metadata, whether hash values remained unchanged throughout the investigation, or whether analytical software produced reliable conclusions. Consequently, the BSA simplifies admissibility without necessarily strengthening evidentiary reliability.

VI. Constitutional Dimensions: Article 21 and the Right to a Fair Trial

The constitutional legitimacy of evidentiary rules must ultimately be assessed against the guarantees contained in **Article 21 of the Constitution of India**, which provides that no person shall be deprived of life or personal liberty except according to procedure established by law. Judicial interpretation has transformed this apparently procedural guarantee into a substantive doctrine encompassing fairness, reasonableness, proportionality and due process.

Beginning with *Maneka Gandhi v. Union of India*, the Supreme Court fundamentally altered the constitutional understanding of Article 21 by holding that "procedure established by law" must itself be fair, just and reasonable rather than arbitrary or oppressive. Subsequent decisions expanded this doctrine to include numerous procedural protections, including legal representation, speedy trial, protection against custodial abuse, disclosure obligations and equality before criminal courts.

Within criminal adjudication, the right to a fair trial constitutes one of the most important manifestations of Article 21. Fairness extends beyond the formal conduct of judicial proceedings and encompasses the entire evidentiary process—from investigation and evidence collection to disclosure, cross-examination and judicial evaluation. Every procedural stage must preserve the accused's meaningful opportunity to challenge the prosecution's case.

Digital evidence fundamentally alters this constitutional landscape. Traditional evidence is generally observable through ordinary human senses. Physical documents can be examined visually, signatures compared manually and material objects inspected directly by the court. Electronic evidence, by contrast, exists only through technological mediation. Its authenticity depends upon software, hardware, forensic imaging techniques, metadata analysis and specialised technical expertise that remain inaccessible to most participants within the criminal justice process.

The constitutional challenge therefore lies not merely in admitting digital evidence but in ensuring that the accused possesses a genuine opportunity to contest its reliability. Procedural fairness requires far more than the physical production of electronic records before the court; it requires transparency regarding the methods through which those records were acquired, processed and interpreted.

A. Presumption of Innocence in the Digital Age

The presumption of innocence remains one of the oldest principles of criminal jurisprudence. Although not expressly mentioned within the Constitution, Indian courts have consistently recognised it as an indispensable component of Article 21 and the broader guarantee of a fair trial.

Digital evidence, however, possesses an aura of scientific certainty that may unconsciously influence judicial decision-making. Unlike eyewitness testimony, which courts traditionally approach with caution, electronic evidence frequently enjoys a presumption of technological objectivity. CCTV recordings, GPS coordinates, call detail records and forensic reports often appear mathematically precise and therefore inherently trustworthy.

This perception is problematic for several reasons.

First, digital evidence is produced through technological systems designed and operated by human beings. Software algorithms may contain programming errors, forensic tools may possess methodological limitations and investigators may inadvertently alter electronic data during acquisition. Consequently, technological evidence is neither infallible nor self-authenticating.

Secondly, electronic records rarely speak for themselves. Their interpretation frequently depends upon expert opinion regarding metadata, timestamps, geolocation information, deleted files or encrypted communications. Such interpretations necessarily involve assumptions capable of reasonable disagreement.

Thirdly, contemporary forensic software often operates as a "black box," producing analytical conclusions without revealing the underlying computational methodology. Defence counsel therefore faces significant obstacles in independently verifying the correctness of forensic conclusions presented by prosecution experts.

These realities demonstrate that the constitutional presumption of innocence requires greater procedural safeguards in cases involving digital evidence rather than fewer. The more technologically complex the evidence becomes, the greater should be the obligation upon the prosecution to establish its authenticity through transparent and verifiable procedures.

B. Equality of Arms and Procedural Fairness

The doctrine of **equality of arms**, recognised in comparative constitutional jurisprudence and reflected within Article 21, requires that neither party should enjoy an unfair procedural advantage capable of affecting the outcome of criminal proceedings.

In traditional criminal trials, this principle generally concerns access to witnesses, documentary

evidence and legal representation. Within the context of digital evidence, however, equality of arms acquires an additional technological dimension.

State investigative agencies possess specialised cyber laboratories, forensic imaging equipment, proprietary analytical software and trained digital forensic experts. They often enjoy institutional access to technological resources unavailable to private litigants. Conversely, many accused persons lack the financial means to engage independent digital forensic experts capable of examining the prosecution's evidence.

This asymmetry produces structural inequality.

Where the prosecution alone controls forensic imaging, metadata extraction, hash verification and digital analysis, the defence becomes dependent upon prosecutorial disclosure. Without complete access to forensic images, metadata logs, software versions and validation reports, effective cross-examination becomes virtually impossible.

Consequently, equality of arms in digital litigation demands more comprehensive disclosure obligations than those traditionally applicable to physical evidence. Constitutional fairness requires disclosure not merely of the final forensic report but also of the technological processes through which that report was produced.

C. Procedural Transparency as a Constitutional Requirement

Transparency constitutes the foundation of adversarial criminal procedure. The legitimacy of judicial findings depends upon the opportunity afforded to each party to examine, challenge and rebut the evidence presented by the opposing side.

Digital evidence presents unique challenges because much of its reliability depends upon invisible technical processes. The defence cannot independently observe forensic imaging, metadata extraction or algorithmic analysis merely by inspecting the final report.

Accordingly, constitutional fairness increasingly requires procedural transparency extending beyond conventional disclosure obligations. Such transparency should include disclosure of:

- Original forensic images.
- Cryptographic hash values.
- Device acquisition logs.
- Chain of custody documentation.
- Software versions utilised during forensic analysis.
- Validation reports demonstrating forensic reliability.
- Metadata generated throughout evidence collection.

Without these materials, the accused effectively confronts technological conclusions rather

than verifiable evidence. Such opacity risks transforming criminal adjudication into an exercise of institutional trust rather than judicial scrutiny.

VII. Judicial Development of Electronic Evidence Jurisprudence

Indian jurisprudence concerning electronic evidence has evolved through several landmark decisions that collectively illustrate the judiciary's struggle to reconcile technological innovation with traditional evidentiary principles.

A. State (NCT of Delhi) v. Navjot Sandhu (2005)

The decision in *Navjot Sandhu*, popularly known as the Parliament Attack Case, represented the Supreme Court's earliest substantial engagement with electronic evidence. The Court adopted a relatively liberal approach by permitting electronic evidence through general evidentiary provisions even in circumstances where statutory certification requirements were absent.

Although this approach facilitated criminal prosecution, it simultaneously weakened the specialised safeguards introduced by Parliament for electronic records. The judgment therefore generated uncertainty regarding the relationship between general documentary evidence provisions and the specialised framework governing electronic records.

B. Anvar P.V. v. P.K. Basheer (2014)

The constitutional and doctrinal landscape changed dramatically with the landmark decision in *Anvar P.V. v. P.K. Basheer*. Rejecting the approach adopted in *Navjot Sandhu*, the Supreme Court held that electronic records must satisfy the statutory requirements governing admissibility and that compliance with the certification provisions was generally mandatory.

The judgment significantly strengthened procedural certainty by clarifying that electronic evidence constituted a distinct evidentiary category requiring specialised treatment. However, critics argued that rigid insistence upon certification occasionally excluded reliable evidence where obtaining the requisite certificate proved practically impossible.

C. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

Recognising continuing doctrinal confusion, a three-judge Bench revisited the issue in *Arjun Panditrao Khotkar*. The Court reaffirmed the mandatory character of certification while clarifying certain procedural exceptions where obtaining certification remained genuinely impossible despite reasonable efforts.

This judgment restored doctrinal coherence and remains one of the most authoritative pronouncements on electronic evidence under Indian law. Importantly, the Court acknowledged that procedural safeguards governing digital evidence exist not merely to satisfy technical formalities but to preserve evidentiary integrity.

D. Tomaso Bruno v. State of Uttar Pradesh (2015)

In *Tomaso Bruno*, the Supreme Court emphasised the growing importance of scientific and electronic evidence within criminal adjudication. The Court criticised investigative agencies for failing to collect available CCTV footage and observed that modern criminal investigation must increasingly rely upon objective technological evidence rather than solely upon oral testimony.

This decision reflected an important judicial recognition that electronic evidence enhances rather than diminishes the search for truth—provided its authenticity can be reliably established.

Collectively, these decisions reveal an evolving judicial philosophy that increasingly recognises electronic evidence as indispensable to modern criminal justice while simultaneously emphasising the necessity of procedural safeguards. Yet significant doctrinal questions remain unresolved regarding forensic transparency, defence access to digital evidence and judicial evaluation of technologically complex expert testimony.

VIII. Technical Integrity of Digital Evidence: The Persistent Forensic Lacuna

While the Bharatiya Sakshya Adhiniyam, 2023 significantly modernises the statutory framework governing electronic evidence, it remains largely silent regarding the technical procedures necessary to preserve the integrity of digital evidence. This omission is particularly significant because, unlike conventional documentary evidence, digital evidence derives its evidentiary value not only from its contents but also from the integrity of the forensic process through which it is acquired, preserved and analysed.

A. The Volatile Nature of Electronic Evidence

Digital evidence is fundamentally different from physical evidence. A physical object generally remains unchanged unless deliberately altered. Electronic data, however, is dynamic. Merely switching on a seized mobile phone or computer may modify system files, alter timestamps, overwrite volatile memory, generate new log entries and change metadata. Consequently, improper handling during the earliest stages of investigation may irreversibly compromise

evidentiary integrity.

For this reason, internationally accepted forensic practice requires investigators to create a **bit-by-bit forensic image** of the original storage medium rather than directly analysing the original device. The forensic image serves as an exact digital replica from which all subsequent examinations are conducted, thereby preserving the integrity of the original evidence.

The Bharatiya Sakshya Adhiniyam does not expressly mandate such forensic practices. Consequently, the quality of digital evidence frequently depends upon the technical competence of individual investigating officers rather than uniform statutory standards. This inconsistency threatens both the reliability of criminal investigations and the constitutional guarantee of equal protection before the law.

B. Chain of Custody in the Digital Environment

The doctrine of chain of custody has long been recognised as essential to criminal adjudication. Traditionally, it documents every stage through which physical evidence passes—from seizure and sealing to storage, transportation, laboratory examination and production before the court. Digital evidence requires a substantially more sophisticated chain of custody.

Every interaction with an electronic device—including powering it on, connecting it to forensic software, creating forensic images, calculating cryptographic hash values, copying files, decrypting data or analysing metadata—must be recorded meticulously. Failure to document these activities creates uncertainty regarding whether electronic evidence remained unaltered throughout the investigative process.

A modern digital chain of custody should therefore include:

- Exact time and place of seizure.
- Identity of every officer handling the device.
- Photographic documentation of the seized device.
- Device specifications and serial numbers.
- Forensic acquisition methodology.
- Hash values generated before and after imaging.
- Storage environment and access logs.
- Details of every forensic examination conducted.
- Identity of all experts who accessed the evidence.

The absence of statutory requirements governing these procedures creates significant evidentiary uncertainty under the current legal framework.

C. The Significance of Cryptographic Hash Values

One of the most important safeguards in digital forensic science is the use of **cryptographic hash functions**. Algorithms such as SHA-256 generate unique digital fingerprints for electronic files. Even the alteration of a single binary digit produces an entirely different hash value.

Hash verification therefore enables investigators and courts to establish that electronic evidence remains unchanged throughout the investigative process.

Despite their importance, Indian criminal procedure presently contains no mandatory statutory obligation requiring original hash values to be disclosed to the defence immediately after seizure. Consequently, the accused frequently receives electronic evidence without the necessary technical information required to verify its authenticity independently.

From the perspective of constitutional due process, this omission significantly undermines the defence's ability to challenge prosecutorial evidence effectively.

D. Forensic Laboratories and Accreditation

Digital forensic conclusions possess evidentiary value only to the extent that the laboratories generating them maintain internationally recognised standards of scientific reliability.

Globally, forensic laboratories are increasingly accredited under **ISO/IEC 17025**, which prescribes standards relating to laboratory competence, equipment calibration, documentation, quality assurance and methodological validation.

Although several Indian forensic laboratories have obtained accreditation, the country still lacks a uniform statutory framework requiring that all digital forensic examinations relevant to criminal prosecutions be conducted exclusively by accredited laboratories operating under nationally standardised protocols.

Such inconsistency risks producing uneven standards of forensic quality across different States and investigative agencies.

IX. Comparative Perspectives

Comparative legal analysis demonstrates that several jurisdictions have recognised that technological innovation must be accompanied by corresponding procedural safeguards.

A. United Kingdom

The United Kingdom has developed comprehensive digital forensic guidance through the **Forensic Science Regulator** and the **Criminal Procedure Rules**. Investigative agencies are

required to document forensic methodology comprehensively while maintaining detailed audit trails throughout evidence acquisition and analysis.

British courts increasingly emphasise disclosure obligations extending beyond the final forensic report to include underlying data and methodological documentation wherever necessary for ensuring procedural fairness.

B. United States

American jurisprudence evaluates scientific evidence primarily through the **Daubert standard**, which requires judges to assess the reliability, testability, peer review, known error rates and general scientific acceptance of expert methodologies before admitting technical evidence.

This gatekeeping function requires judges to evaluate not merely expert conclusions but the scientific reliability of the methodology itself. Such an approach provides a useful comparative model for strengthening judicial scrutiny of digital forensic evidence in India.

C. Singapore

Singapore has emerged as a regional leader in digital evidence governance through specialised cybercrime investigation units, judicial education programmes and technologically advanced forensic infrastructure.

The Singaporean legal framework places considerable emphasis upon maintaining forensic integrity from seizure to trial, thereby minimising opportunities for evidentiary contamination.

D. European Union

The European Union increasingly approaches digital evidence through the combined perspectives of criminal procedure and fundamental rights. Judicial scrutiny extends beyond evidentiary reliability to include proportionality, privacy, data protection and transparency.

The European emphasis upon procedural accountability reinforces the proposition that technological efficiency cannot justify erosion of constitutional safeguards.

X. Critical Evaluation of the Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam undoubtedly represents substantial legislative progress. It modernises evidentiary terminology, recognises digital realities and attempts to simplify procedural complexities that characterised earlier jurisprudence.

Nevertheless, three structural concerns remain.

First, the statute focuses predominantly upon admissibility rather than forensic reliability. Admissibility determines whether evidence may be considered by the court; reliability determines whether it deserves belief. Modern criminal justice requires equal attention to both.

Secondly, the legislation inadequately addresses institutional disparities between prosecution and defence. Digital evidence often remains effectively controlled by investigating agencies possessing exclusive technological expertise. Without comprehensive disclosure obligations, adversarial equality becomes largely illusory.

Thirdly, the statute provides insufficient guidance regarding judicial evaluation of technologically sophisticated evidence. Judges continue to rely heavily upon expert testimony despite increasing recognition that forensic software itself requires independent scrutiny.

The consequence is a legal framework that successfully accommodates digital evidence but does not yet fully accommodate digital justice.

XI. Recommendations for Reform

The foregoing analysis suggests that meaningful reform must extend beyond statutory admissibility.

1. Mandatory Digital Forensic Protocols

Parliament should enact legally binding Standard Operating Procedures governing every stage of digital evidence collection, forensic imaging, preservation, transportation and courtroom presentation. Uniform procedures would substantially reduce inconsistencies across investigative agencies.

2. Statutory Disclosure of Forensic Metadata

The prosecution should be legally required to disclose:

- Original forensic images.
- Complete metadata.
- Hash values.
- Device acquisition reports.
- Audit logs.
- Software versions.
- Validation reports.

- Chain of custody documentation.

Such disclosure would significantly strengthen equality of arms.

3. National Digital Forensic Authority

India should establish an independent statutory authority responsible for:

- Accrediting forensic laboratories.
- Certifying forensic software.
- Publishing national technical standards.
- Conducting quality assurance inspections.
- Training investigators and judges.

Independent oversight would enhance both scientific reliability and public confidence.

4. Judicial Capacity Building

Continuous judicial education should include specialised training concerning:

- Digital forensic science.
- Metadata interpretation.
- Cryptographic verification.
- Artificial intelligence evidence.
- Blockchain technologies.
- Cyber investigations.

Improved judicial literacy would strengthen courts' gatekeeping function.

5. Independent Court-Appointed Technical Assessors

Complex digital evidence cases should permit appointment of neutral technical assessors assisting the court independently of either party. Such experts would enhance judicial understanding while preserving adversarial fairness.

6. Blockchain-Based Digital Chain of Custody

Emerging technologies such as blockchain may provide immutable audit trails documenting every interaction with digital evidence throughout criminal proceedings. Although implementation challenges remain, pilot programmes should be considered for serious cybercrime investigations.

7. Legislative Recognition of Digital Due Process

Finally, Parliament should explicitly recognise **digital due process** as a foundational principle governing electronic evidence. Such recognition would require courts to evaluate not merely statutory admissibility but also procedural transparency, technological reliability and constitutional fairness.

XII. Conclusion

The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 marks a defining moment in the evolution of Indian evidentiary law. The BSA acknowledges the undeniable reality that digital information has become the principal currency of contemporary criminal litigation. Electronic records, metadata, surveillance systems and digital communications now occupy a central position within criminal investigations, making legislative modernisation both necessary and inevitable.

Yet, technological progress cannot be equated with constitutional progress. The mere recognition of electronic records as primary evidence does not resolve the deeper challenges posed by digital technologies. Questions concerning authenticity, forensic integrity, metadata preservation, algorithmic transparency and equality of arms remain largely unresolved. Without rigorous procedural safeguards, digital evidence may inadvertently strengthen prosecutorial power while diminishing the accused's constitutional capacity to challenge the evidence effectively.

Article 21 of the Constitution demands more than formal legality. It requires procedures that are fair, transparent, reasonable and capable of preventing wrongful conviction. In the digital age, these constitutional guarantees necessarily extend beyond traditional evidentiary doctrines to encompass technological accountability.

The future of Indian criminal justice therefore depends not simply upon embracing digital evidence but upon constructing institutions capable of scrutinising it critically. Mandatory forensic standards, comprehensive disclosure obligations, judicial technological competence, accredited forensic laboratories and transparent chain of custody mechanisms are no longer optional administrative improvements; they constitute constitutional necessities.

Ultimately, justice in the digital era cannot rest upon technological sophistication alone. It must rest upon **forensic transparency, institutional accountability and unwavering commitment to constitutional due process**. Only by integrating these principles into the evolving legal framework can India ensure that the pursuit of technological efficiency never comes at the

expense of the fundamental right to a fair trial.

Selected Bibliography

Statutes

- Bharatiya Sakshya Adhiniyam, 2023.
- Constitution of India, 1950.
- Indian Evidence Act, 1872.
- Information Technology Act, 2000.
- Bharatiya Nagarik Suraksha Sanhita, 2023.
- Bharatiya Nyaya Sanhita, 2023.

Cases

- *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
- *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
- *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
- *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
- *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
- *Zahira Habibullah Sheikh v. State of Gujarat*, (2004) 4 SCC 158.
- *Selvi v. State of Karnataka*, (2010) 7 SCC 263.

Books

- Avtar Singh, *Law of Evidence*.
- Batuk Lal, *Law of Evidence*.
- Vepa P. Sarathi, *Law of Evidence*.
- Stephen Mason, *Electronic Evidence*.
- Paul Roberts and Adrian Zuckerman, *Criminal Evidence*.
- Ian Dennis, *The Law of Evidence*.

Reports and Articles

- Law Commission of India Reports on the Indian Evidence Act.
- PRS Legislative Research, *Analysis of the Bharatiya Sakshya Bill, 2023*.

- ISO/IEC 17025:2017, *General Requirements for the Competence of Testing and Calibration Laboratories*.
- National Institute of Standards and Technology (NIST), *Guidelines on Mobile Device Forensics*.
- Indian Journal of Constitutional Law, recent articles on digital due process and fair trial.
- Journal of Digital Forensics, Security and Law.
- International Journal of Evidence and Proof.
- Computer Law & Security Review.