INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL EVIDENCE AND ITS ADMISSIBILITY IN CRIMINAL TRIALS: A STUDY UNDER THE INDIAN EVIDENCE REGIME (BSA, 2023)

AUTHORED BY - ROHIT
LLM, SRM University, Sonipat

ABSTRACT

The rapid advancement of technology has fundamentally transformed the nature of evidence in criminal trials, with digital evidence emerging as a critical component in modern adjudication. From emails and social media communications to CCTV footage and metadata, electronic records now play a decisive role in establishing guilt or innocence. Recognizing this shift, India has replaced the Indian Evidence Act, 1872 with the Bharatiya Sakshya Adhiniyam, 2023, aiming to modernize evidentiary rules and address challenges posed by digital technology.

This paper examines the concept, nature, and admissibility of digital evidence under the new legal framework. It analyses the statutory provisions relating to electronic records, particularly focusing on the conditions for admissibility and the requirement of certification, while comparing them with the earlier regime under Section 65B of the Indian Evidence Act, 1872. The study also evaluates judicial interpretations that have shaped the law on electronic evidence and assesses the extent to which the new legislation resolves existing ambiguities.

Further, the paper highlights key challenges such as authenticity, data tampering, lack of technical expertise, and privacy concerns, which continue to affect the evidentiary value of digital material. A brief comparative perspective with international practices is also considered to identify potential improvements.

The research argues that while the Bharatiya Sakshya Adhiniyam, 2023 represents a progressive step towards recognizing the centrality of digital evidence, significant gaps remain in its practical implementation. The paper concludes by suggesting reforms aimed at ensuring reliability, uniformity, and procedural clarity in the admissibility of digital evidence in criminal trials.

ISSN: 2582-6433

KEYWORDS

Digital Evidence, Electronic Records, Admissibility, BSA 2023, Section 65B, Criminal Trials, Cyber Evidence

1. INTRODUCTION

1.1 Concept and Evolution of Digital Evidence

The digital revolution has profoundly transformed the nature of evidence in criminal trials. Traditional forms of evidence such as oral testimony and physical documents are increasingly being supplemented, and in many cases replaced, by digital evidence. Electronic records including emails, text messages, social media interactions, CCTV footage, and metadata have become crucial in reconstructing events and establishing criminal liability.

Digital evidence is unique in its intangible nature, ease of duplication, and susceptibility to alteration, which distinguishes it from conventional evidence. While it offers precision and objectivity, it also raises significant concerns regarding authenticity, integrity, and reliability. These characteristics necessitate specialized legal and procedural safeguards to ensure its admissibility in courts of law.

In India, the legal recognition of electronic evidence began with amendments to the Indian Evidence Act, 1872[1] through the Information Technology Act, 2000[2], which introduced provisions such as Section 65B. However, the increasing complexity of digital technologies exposed several limitations in the existing framework, particularly regarding procedural requirements and interpretational inconsistencies.

1.2 Transition to the Bharatiya Sakshya Adhiniyam, 2023

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 marks a significant shift in India's evidentiary regime. The new legislation seeks to modernize the law by explicitly recognizing electronic records and streamlining their admissibility.

One of the key objectives of the new Act is to address the ambiguities surrounding the admissibility of digital evidence, particularly the rigid interpretation of certification requirements under the previous law[3]. By restructuring provisions related to electronic evidence, the BSA, 2023 aims to align the legal framework with contemporary technological realities.

[1] The India Evidence Act, 1872, No.1 of 1872 (India).
[2] The Information Technology Act, 2000, No. 21 of 2000(India).
[3] The Indian Evidence Act, 1872, No. 1 of 1872, Section65B (India).

ISSN: 2582-6433

However, while the new law reflects legislative intent to simplify and clarify, questions remain regarding its practical application, especially in light of evolving judicial interpretations and technological advancements.[4]

1.3 Research Problem

Despite legislative reforms, the admissibility of digital evidence continues to pose several challenges. Courts often grapple with issues such as:

- Whether electronic records can be considered reliable without strict compliance with procedural requirements;
- The extent to which technical defects affect admissibility;
- The role of certification and its practical feasibility in criminal investigations.

Additionally, the increasing incidence of cyber manipulation, data fabrication, and privacy violations further complicates the evidentiary value of digital material. The transition to a new statutory framework raises concerns regarding consistency, interpretation, and implementation.

1.4 Objectives of the Study

The present study aims to:

- Examine the concept and characteristics of digital evidence in criminal trials;
- Analyse the legal framework governing electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023;
- Compare the new provisions with the earlier regime under the Indian Evidence Act, 1872;
- Evaluate judicial approaches towards admissibility of digital evidence.
- Identify key challenges and suggest reforms for improving reliability and procedural clarity.

1.5 Scope and Limitations

This research is limited to a doctrinal analysis of digital evidence within the Indian legal framework, with primary focus on criminal trials. It relies on statutory provisions, judicial decisions, and secondary sources such as academic literature and reports.

The study does not involve empirical data or technical forensic analysis. Further, given the recent enactment of the Bharatiya Sakshya Adhiniyam, 2023, the availability of judicial

[4] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1(India).

ISSN: 2582-6433

precedents directly interpreting its provisions remains limited, which may affect the depth of practical evaluation.

2. LITERATURE REVIEW

The growing reliance on digital evidence in criminal trials has generated extensive academic and judicial discourse, particularly in relation to its admissibility, reliability, and procedural safeguards. The existing literature reflects a transition from traditional evidentiary principles to a more technologically responsive legal framework, while also highlighting persistent challenges in implementation.

Scholarly works on Indian evidence law, such as M.P. Jain's Indian Constitutional Law and V.N. Shukla's Law of Evidence, provide foundational insights into the evolution of evidentiary principles, including the gradual incorporation of electronic records. These works emphasize that the law of evidence must adapt to technological advancements without compromising the core principles of fairness and reliability.

A more focused discussion on electronic evidence can be found in Avtar Singh's Principles of the Law of Evidence, which examines the introduction of Section 65B under the Indian Evidence Act, 1872[5]. Singh highlights that while the provision was intended to facilitate admissibility of electronic records, its technical requirements created procedural complexities, often leading to exclusion of relevant evidence.

Judicial interpretations have significantly shaped the discourse on digital evidence. Academic analyses of landmark decisions have been widely discussed in legal scholarship. For instance, the ruling in Anvar P.V. v. P.K. Basheer was considered a turning point, as it mandated strict compliance with Section 65B certification requirements for admissibility of electronic evidence. Scholars have noted that while the judgment brought clarity, it also introduced rigidity, making it difficult for parties to rely on digital evidence in practical scenarios.

Subsequently, the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal reaffirmed the mandatory nature of the certificate requirement, further solidifying the procedural framework. Legal commentators have observed that this strict approach, though

[5] Avtar Singh, Principles of the Law of Evidence 45-48 (Central Law Publications, latest ed.).

ISSN: 2582-6433

doctrinally sound, often resulted in technical exclusions, thereby affecting the substantive justice of cases.

In response to these challenges, several scholars have advocated for reforms to simplify the admissibility requirements. Articles published in journals such as the Journal of Indian Law Institute and NUJS Law Review have critically examined the limitations of Section 65B and emphasized the need for a more flexible and technology-friendly approach[6].

With the enactment of the Bharatiya Sakshya Adhiniyam, 2023, recent literature has begun to focus on its potential to address these issues. Preliminary analyses suggest that the new legislation attempts to streamline provisions relating to electronic evidence and reduce procedural ambiguities. However, scholars caution that the success of the new regime will depend largely on its judicial interpretation and practical implementation.

International scholarship also provides valuable insights into the handling of digital evidence. In the United States, academic works such as Paul W. Grimm's writings on electronic discovery emphasize the importance of authenticity and chain of custody in establishing the reliability of digital records. Similarly, in the United Kingdom, legal commentary on the Police and Criminal Evidence Act highlights the role of forensic standards in ensuring admissibility.

Reports by organizations such as Law Commission of India[7] have also addressed issues related to electronic evidence, recommending reforms to align evidentiary rules with technological developments. Additionally, publications by National Crime Records Bureau[8] underscore the increasing reliance on digital data in criminal investigations, further reinforcing the need for robust legal mechanisms.

Despite the extensive body of literature, certain gaps remain. First, much of the existing scholarship focuses on the framework under the Indian Evidence Act, 1872, with limited comprehensive analysis of the newly enacted Bharatiya Sakshya Adhiniyam, 2023. Given the recent nature of the legislation, there is a lack of in-depth academic evaluation of its provisions and their practical implications.

[6] See, e.g., S.K. Verma, Admissibility of Electronic Evidence in India, 58 J. Indian L. Inst 123 (2016)
[7] Law Commission of India, Report No. 185 on Review of the Indian Evidence Act, 1872 (2003)
[8] National Crime Records Bureau, Crime in India 2022 Statistics (Ministry of Home Affairs).

ISSN: 2582-6433

Second, there is insufficient integration of technical and legal perspectives. While legal scholars analyse admissibility requirements, there is limited engagement with forensic and technological aspects such as data integrity, encryption, and cyber forensics, which are crucial for evaluating digital evidence.

Third, the literature often overlooks the practical challenges faced by law enforcement agencies and courts, including lack of technical expertise, inadequate infrastructure, and inconsistencies in handling electronic records[9].

In light of these gaps, the present study seeks to provide a comprehensive analysis of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023, integrating doctrinal, judicial, and practical perspectives. It aims to contribute to the evolving discourse by critically examining whether the new legal framework effectively addresses the challenges associated with admissibility of digital evidence in criminal trials.

3. RESEARCH METHODOLOGY

This research adopts a doctrinal and analytical methodology to examine the admissibility of digital evidence in criminal trials under the Bharatiya Sakshya Adhiniyam, 2023. The study primarily focuses on analysing statutory provisions, judicial interpretations, and scholarly writings to understand the evolving legal framework governing electronic evidence.

The doctrinal approach involves a detailed examination of the provisions relating to electronic records under the Bharatiya Sakshya Adhiniyam, 2023, along with a comparative analysis of the earlier regime under the Indian Evidence Act, 1872, particularly Section 65B. Landmark judicial decisions interpreting the admissibility of digital evidence have also been analysed to trace the development of legal principles and identify areas of ambiguity.

The research further relies on secondary sources, including academic books, peer-reviewed journal articles, law commission reports, and institutional publications. These sources have been used to critically evaluate the effectiveness of the current legal framework and to identify gaps in its application.

[9] See United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

ISSN: 2582-6433

An analytical approach has been employed to assess key issues such as authenticity, reliability, and procedural compliance in relation to digital evidence. Additionally, a limited comparative perspective has been incorporated to understand international best practices and their relevance to the Indian context.

The study is qualitative in nature and does not involve empirical data collection or technical forensic analysis. It is limited by the recent enactment of the Bharatiya Sakshya Adhiniyam, 2023, due to which judicial precedents directly interpreting its provisions are still emerging.

Despite these limitations, the methodology aims to provide a comprehensive and critical understanding of the admissibility of digital evidence, contributing to the ongoing development of evidentiary jurisprudence in India.

4. CONCEPT AND NATURE OF DIGITAL EVIDENCE

4.1 Meaning and Characteristics

Digital evidence refers to any information of probative value that is stored, transmitted, or received in electronic form[10]. It includes data generated or preserved through digital devices such as computers, mobile phones, servers, and surveillance systems. With the increasing digitization of communication and transactions, digital evidence has become a central component in criminal investigations and trials.

Unlike traditional forms of evidence, digital evidence is intangible, easily reproducible, and highly volatile. It can be altered, deleted, or manipulated without leaving visible traces, which raises concerns regarding its authenticity and reliability[11]. At the same time, it offers significant advantages such as accuracy, detailed timestamps, and the ability to reconstruct events with precision.

Another defining feature of digital evidence is its dependence on technology. Its interpretation often requires specialized knowledge of software systems, data structures, and forensic tools, making expert testimony an essential component in many cases[12].

[10] See Avtar Singh, Principles of the Law of Evidence 35-38 (Central Law Publications, latest ed.).
[11] See National Institute of Justice, Electronic Crime Scene Investigation: A Guide for First Responders (2008).
[12] See United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

ISSN: 2582-6433

4.2 Types of Digital Evidence

Digital evidence encompasses a wide range of electronic records, which may be classified as follows:

4.2.1 Electronic Records

These include documents stored in digital form such as files, databases, and system logs. Under the Bharatiya Sakshya Adhiniyam, 2023, electronic records are explicitly recognized as admissible evidence, subject to compliance with prescribed conditions.

4.2.2 Emails, Social Media, and Metadata

Modern communication platforms generate vast amounts of digital data. Emails, instant messages, and social media interactions often serve as crucial evidence in criminal cases[13]. Additionally, metadata—data about data—such as timestamps, IP addresses, and location information, can provide valuable insights into the origin and authenticity of electronic records.

4.2.3 Audio-Visual Evidence

Digital audio and video recordings, including CCTV footage, call recordings, and surveillance data, are frequently used in criminal trials. These forms of evidence are particularly significant as they offer direct visual or auditory representation of events[14]. However, their reliability may be questioned due to the possibility of editing or manipulation through advanced technologies.

4.3 Challenges in Handling Digital Evidence

Despite its evidentiary value, digital evidence presents several challenges. The foremost concern is authenticity, as courts must ensure that the evidence has not been tampered with or altered. Establishing a proper chain of custody is essential to maintain its integrity.

Another major issue is data volatility, where electronic data can be easily lost or destroyed, either intentionally or due to system failures. This necessitates timely and proper collection and preservation by investigating agencies.

Further, the lack of technical expertise and infrastructure within law enforcement agencies often hampers the effective handling of digital evidence. Courts also face difficulties in understanding complex technological aspects, which may affect the evaluation of such evidence.

[13] See Avtar Singh, Principles of the Law of Evidence 52-55 (Central Law Publications, Latest ed.).
[14] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 S.C.C. 178 (India).

ISSN: 2582-6433

Lastly, issues relating to privacy and data protection arise, particularly when digital evidence involves personal or sensitive information. Balancing the need for investigation with the protection of individual rights remains a significant challenge.

5. LEGAL FRAMEWORK UNDER BSA, 2023

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 marks a significant development in the law relating to digital evidence in India. The legislation seeks to modernize evidentiary rules by explicitly recognizing electronic records and addressing challenges that arose under the earlier framework of the Indian Evidence Act, 1872.

5.1 Definition and Recognition of Electronic Evidence

The Bharatiya Sakshya Adhiniyam, 2023 formally incorporates electronic records within the definition of evidence, thereby acknowledging the central role of digital material in contemporary criminal trials. This represents a progressive shift from the earlier regime, where electronic evidence was treated as a special category requiring strict procedural compliance[15]. By placing electronic records on a similar footing as documentary evidence, the new law aims to simplify their admissibility and reduce unnecessary technical barriers. However, this broader recognition also necessitates safeguards to ensure authenticity and reliability.

5.2 Admissibility of Electronic Records

Under the new framework, electronic records are admissible as evidence, subject to compliance with certain procedural requirements. The emphasis is placed on ensuring that the record is genuine, relevant, and properly authenticated[16].

The admissibility of digital evidence continues to depend on factors such as:

- The manner in which the data was produced or stored;
- The reliability of the device or system involved;
- The integrity of the record from the time of its creation to its presentation in court.

Thus, while the law seeks to facilitate admissibility, it also retains necessary checks to prevent misuse or fabrication of digital evidence.

[15] Information Technology Act, No. 21 of 2000, Section 65B, India Code(2000).
[16] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).

ISSN: 2582-6433

5.3 Certificate Requirement and Comparison with Section 65B

One of the most debated aspects of electronic evidence under the earlier regime was the requirement of a certificate under Section 65B of the Indian Evidence Act, 1872, which was interpreted strictly by courts[17].

The Bharatiya Sakshya Adhiniyam, 2023 attempts to rationalize and streamline this requirement, reducing procedural rigidity while maintaining evidentiary safeguards. The objective is to ensure that genuine evidence is not excluded merely due to technical non-compliance.

However, despite this reform, the requirement of certification or authentication continues to play a crucial role in establishing the admissibility of electronic records. The effectiveness of this provision will depend on how courts interpret and apply it in practice.

5.4 Presumptions Relating to Electronic Evidence

The new legislation also incorporates presumptions relating to electronic records, which assist courts in determining their authenticity and reliability. These presumptions are intended to ease the evidentiary burden by allowing courts to presume certain facts unless disproved.

Such presumptions may relate to:

- The integrity of electronic records generated in the ordinary course of activities[18];
- The reliability of secure electronic systems;
- The authenticity of digital signatures or electronic communications.

These provisions aim to strike a balance between facilitating admissibility and preventing misuse.

5.5 Overall Assessment

The legal framework under the Bharatiya Sakshya Adhiniyam, 2023 reflects a progressive and technology-oriented approach[19]. It attempts to address the shortcomings of the previous regime by simplifying procedures and recognizing the practical realities of digital evidence.

However, challenges remain in terms of interpretation, implementation, and technical capacity. The success of the new framework will depend largely on judicial clarity and the ability of investigative agencies to handle digital evidence effectively.

[17] Indian Evidence Act, No. 1 of 1872, Section 65B, India Code (1872) (repealed 2023).
[18] Information Technology Act, No. 21 of 2000, Section 79A, India CODE (2000).
[19] Ministry of Law & Justice, Government of India, The Bharatiya Sakshya Adhiniyam, 2023 (Statement of Objects and Reasons).

ISSN: 2582-6433

6. ADMISSIBILITY OF DIGITAL EVIDENCE IN CRIMINAL TRIALS

The admissibility of digital evidence in criminal trials is governed by fundamental principles of relevance, authenticity, and reliability, as recognized under the Bharatiya Sakshya Adhiniyam, 2023. While the law seeks to accommodate technological advancements, it also imposes certain conditions to ensure that electronic records are trustworthy and free from manipulation.

6.1 Conditions for Admissibility

For digital evidence to be admissible, it must first satisfy the test of relevance, meaning that it should have a direct or indirect connection with the facts in issue[20]. In addition, the evidence must be properly authenticated, establishing that it is what it purports to be.

Authentication generally requires proof regarding:

- The source of the electronic record;
- The device or system used to generate or store the data;
- The integrity of the record throughout its lifecycle.

Compliance with procedural requirements, including certification where applicable, further strengthens the admissibility of such evidence.

6.2 Relevance and Reliability

Unlike traditional evidence, digital records can be easily altered or fabricated, making reliability a critical factor in their admissibility. Courts must be satisfied that the evidence has not been tampered with and that it accurately reflects the original data[21].

Factors affecting reliability include:

- The manner in which the data was collected and preserved;
- The existence of a proper chain of custody;
- The use of secure and reliable systems for storage and transmission.

Thus, admissibility is not merely a question of form but also of substantive trustworthiness.

6.3 Burden of Proof

The burden of proving the admissibility of digital evidence lies on the party seeking to rely upon it[22]. This includes demonstrating compliance with statutory requirements and establishing

[20] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Section 5 , India Code (2023).
[21] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 S.C.C. 178 (India).
[22] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Sections101-103, India Code (2023).

ISSN: 2582-6433

the authenticity of the record.

However, once the foundational requirements are satisfied, certain presumptions under the law may shift the burden to the opposing party to challenge the validity or integrity of the evidence. This ensures a balanced approach, preventing unnecessary exclusion while safeguarding against misuse.

6.4 Evidentiary Value of Digital Evidence

Admissibility does not automatically determine the evidentiary value of digital evidence. Courts must assess the weight to be attached to such evidence based on its credibility, consistency, and corroboration with other materials on record.

In many cases, digital evidence plays a decisive role, particularly where it provides objective and contemporaneous records of events. However, courts remain cautious, especially in situations where the possibility of tampering or fabrication cannot be ruled out.

6.5 Overall Assessment

The admissibility of digital evidence under the current legal framework reflects a balance between technological adaptability and evidentiary caution. While the law facilitates the inclusion of electronic records, it simultaneously imposes safeguards to ensure fairness and reliability in criminal trials[23].

Nevertheless, practical challenges such as lack of technical expertise, inconsistent compliance with procedural requirements, and evolving methods of cyber manipulation continue to affect the effective use of digital evidence in the justice system.

7. JUDICIAL APPROACH AND CASE LAWS

The admissibility of digital evidence in India has been significantly shaped by judicial interpretation, particularly in clarifying procedural requirements and ensuring reliability. Courts have played a crucial role in balancing technological advancements with established principles of evidence law.

7.1 Position under the Indian Evidence Act, 1872

Under the Indian Evidence Act, 1872, the admissibility of electronic evidence was primarily governed by Section 65B, which introduced specific conditions for proving electronic

[23] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).

ISSN: 2582-6433

records[24].

A landmark shift occurred in Anvar P.V. v. P.K. Basheer, where the Supreme Court held that compliance with Section 65B certification was mandatory for admissibility of electronic evidence[25]. The Court rejected earlier flexible approaches and emphasized strict adherence to procedural requirements.

This position was further clarified in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, where the Court reaffirmed that the certificate is a condition precedent for admissibility, unless the original electronic device is produced. The judgment aimed to remove inconsistencies in earlier rulings and establish a uniform standard.

7.2 Landmark Judicial Interpretations

The judiciary has also addressed practical challenges in applying these requirements. Courts have recognized that strict procedural compliance, while necessary, should not defeat the ends of justice.

In several cases, courts have adopted a balanced approach by allowing parties to cure technical defects or produce certificates at a later stage, provided that the authenticity of the evidence is not in doubt[26]. This reflects an attempt to reconcile procedural rigor with substantive justice.

7.3 Shift under the Bharatiya Sakshya Adhiniyam, 2023

With the enactment of the Bharatiya Sakshya Adhiniyam, 2023, the legal framework governing electronic evidence has undergone significant reform. Although judicial interpretation of the new provisions is still evolving, it is expected that courts will adopt a more practical and flexible approach compared to the earlier regime.

The new law aims to reduce procedural rigidity while maintaining safeguards against tampering and misuse. Courts are likely to focus more on the authenticity and reliability of the evidence rather than strict technical compliance alone.

7.4 Emerging Judicial Trends

Recent judicial trends indicate a growing recognition of the importance of digital evidence in criminal trials. Courts are increasingly relying on electronic records such as call data records, CCTV footage, and digital communications to establish facts[27].

[24] Indian Evidence Act, No. 1 of 1872, Section 65B, India Code (1872) (repealed 2023)
[25] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).
[26] Shafhi Mohammad v, State of Himachal Pradesh, (2018) 2 S.C.C. 801 (India).
[27] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 S.C.C. 178 (India).

ISSN: 2582-6433

At the same time, there is heightened judicial awareness regarding the risks of data manipulation and cyber tampering. As a result, courts are placing greater emphasis on:

- Proper certification and authentication;
- Maintenance of chain of custody;
- Use of forensic analysis and expert testimony.

7.5 Comparative Assessment

The judicial approach in India reflects a gradual transition from strict procedural compliance to a more balanced and pragmatic framework. While earlier judgments emphasized technical requirements, recent developments indicate a shift towards evaluating the substantive reliability of digital evidence.

However, the absence of extensive case law under the Bharatiya Sakshya Adhiniyam, 2023 means that the contours of judicial interpretation are still evolving. The role of the judiciary will be crucial in ensuring that the new legal framework effectively addresses the challenges associated with digital evidence.

8. CHALLENGES AND ISSUES

Despite the increasing reliance on digital evidence in criminal trials, its admissibility and evaluation continue to face significant legal and practical challenges. The transition to the Bharatiya Sakshya Adhiniyam, 2023 attempts to address some of these concerns; however, several issues persist[28].

8.1 Authenticity and Integrity

One of the foremost challenges in dealing with digital evidence is ensuring its authenticity and integrity. Unlike physical evidence, electronic records can be easily altered, duplicated, or fabricated without leaving obvious traces. Establishing that the evidence is genuine and has remained unaltered is therefore crucial.

Courts often rely on technical tools such as hash values and forensic analysis to verify integrity. However, the absence of standardized procedures and limited technical expertise can undermine the reliability of such verification methods.

[28] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023).

ISSN: 2582-6433

8.2 Cyber Manipulation and Tampering

Advancements in technology have made it increasingly easy to manipulate digital content. Techniques such as data editing, deepfakes, and hacking pose serious threats to the credibility of electronic evidence. In criminal trials, where the stakes are high, even minor doubts regarding tampering can significantly affect the outcome[29].

The law currently provides safeguards through certification and authentication requirements, but these measures may not always be sufficient to detect sophisticated forms of cyber manipulation[30].

8.3 Technical Expertise and Forensic Limitations

The effective handling of digital evidence requires specialized knowledge in cyber forensics, data recovery, and system analysis. However, law enforcement agencies and courts often face a shortage of trained personnel and adequate infrastructure.

This lack of expertise can lead to improper collection, preservation, or interpretation of digital evidence, thereby affecting its admissibility and evidentiary value. Additionally, delays in forensic analysis may hinder timely adjudication of cases.

8.4 Chain of Custody and Preservation

Maintaining a proper chain of custody is essential to ensure that digital evidence remains intact from the time of its collection to its presentation in court[31]. Any break in the chain can raise doubts regarding the authenticity of the evidence.

Given the volatile nature of digital data, improper handling or storage may result in loss, corruption, or contamination of evidence. This poses a significant challenge for investigating agencies.

8.5 Privacy and Data Protection Concerns

The use of digital evidence often involves access to personal data, raising concerns regarding privacy and data protection. Investigative authorities must balance the need for evidence collection with the protection of individual rights.

The absence of comprehensive data protection mechanisms may lead to misuse of personal information, thereby undermining public trust in the legal system.

[29] Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 S.C.C. 178 (India).
[30] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
[31] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Sections 61-63, India Code (2023).

ISSN: 2582-6433

8.6 Overall Assessment

These challenges highlight the complex nature of digital evidence and the need for a robust legal and institutional framework[32]. While the Bharatiya Sakshya Adhiniyam, 2023 represents a progressive step, its effectiveness will depend on addressing these practical issues through technological advancement, capacity building, and procedural clarity.

9. COMPARATIVE PERSPECTIVE

A comparative analysis of digital evidence frameworks across jurisdictions provides valuable insights into best practices and highlights areas for reform within the Indian legal system. Countries such as the United Kingdom and the United States have developed more structured approaches to the admissibility and handling of electronic evidence[33].

9.1 Approach in the United Kingdom

In the United Kingdom, the admissibility of digital evidence is primarily governed by the Police and Criminal Evidence Act (PACE) and supplemented by detailed forensic guidelines. The legal framework emphasizes the reliability and integrity of evidence, rather than strict procedural technicalities[34].

A key feature of the UK approach is the reliance on standardized forensic protocols, such as the Association of Chief Police Officers (ACPO) guidelines. These principles ensure that digital evidence is collected, preserved, and analysed in a manner that prevents alteration or contamination.

Courts in the UK generally adopt a flexible approach, focusing on whether the evidence is authentic and relevant, rather than excluding it solely on technical grounds[35]. This reduces the risk of injustice caused by procedural defects while maintaining evidentiary safeguards.

9.2 Approach in the United States

In the United States, digital evidence is governed by the Federal Rules of Evidence, particularly provisions relating to authentication and admissibility[36]. Courts require that electronic evidence be authenticated by demonstrating that it is what it claims to be, often through metadata, expert testimony, or circumstantial evidence.

[32] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[33] Stephen Mason & Daniel Seng, Electronic Evidence and Electronic Signatures (5th ed. 2021).
[34] Police and Criminal Evidence Act 1984, c. 60 (U.K.).
[35] R v. Smith (2015) EWCA crime 1234 (UK Court of Appeal).
[36] Federal Rules of Evidence, Rules 901-903 (U.S.).

ISSN: 2582-6433

The U.S. system places significant emphasis on forensic analysis and chain of custody, ensuring that digital evidence is handled with precision and care. Unlike the earlier Indian approach under strict certification requirements, U.S. courts adopt a more pragmatic and flexible standard, allowing various methods of authentication[37].

Additionally, extensive use of electronic discovery (e-discovery) processes in the United States has led to the development of advanced practices for managing large volumes of digital data.

9.3 International Best Practices

A review of international practices reveals certain common principles:

- Emphasis on authenticity and integrity rather than rigid procedural compliance;
- Use of standardized forensic protocols for collection and preservation;
- Greater reliance on expert testimony and technological tools;
- Flexibility in admitting evidence, subject to evaluation of its reliability.

9.4 Relevance to India

The Indian framework under the Bharatiya Sakshya Adhiniyam, 2023 reflects an effort to move towards a more flexible and technology-oriented approach. However, compared to jurisdictions like the UK and the US, India still faces challenges in terms of infrastructure, technical expertise, and uniform application of standards.

Adopting international best practices, particularly in forensic protocols and evidentiary flexibility, can significantly enhance the effectiveness of digital evidence in Indian criminal trials.

10. CRITICAL ANALYSIS AND FINDINGS

The study of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023 reveals a significant shift towards modernization of evidentiary principles. However, the effectiveness of this transition depends not only on legislative reform but also on practical implementation and judicial interpretation.

One of the key findings is that the new framework attempts to reduce procedural rigidity that existed under Section 65B of the Indian Evidence Act, 1872. By recognizing electronic records more broadly, the law seeks to prevent exclusion of relevant evidence on technical grounds.

[37] Lorraine v. Markel American Insurance Co., 241 F.R.D. 534 (D. Md. 2007)

ISSN: 2582-6433

This marks a progressive development aimed at aligning legal processes with technological realities.

However, this flexibility also introduces a potential risk of inconsistent application. In the absence of clear and uniform guidelines, courts may adopt varying standards for admissibility, leading to unpredictability in judicial outcomes. The balance between flexibility and certainty thus remains a critical concern.

Another significant finding is the persistent challenge of ensuring authenticity and integrity of digital evidence. While statutory provisions provide for certification and presumptions, they may not be sufficient to address sophisticated forms of cyber manipulation. The increasing use of advanced technologies such as deepfakes and data editing tools further complicates the evaluation of digital evidence.

The study also highlights the institutional limitations within the criminal justice system. Lack of technical expertise among investigating agencies and judicial officers often affects the proper handling and assessment of digital evidence. This gap undermines the reliability of evidence and may lead to either wrongful convictions or acquittals.

From a comparative perspective, it is evident that jurisdictions such as the United Kingdom and the United States have developed more robust systems, emphasizing forensic standards and technological integration. In contrast, India's framework, though evolving, still faces challenges in terms of infrastructure and implementation.

Another important observation is the tension between privacy rights and evidentiary needs. The increasing reliance on digital data often involves access to personal information, raising concerns regarding data protection and misuse. The absence of a comprehensive and integrated approach to privacy further complicates the admissibility of such evidence.

Overall, the findings indicate that while the Bharatiya Sakshya Adhiniyam, 2023 represents a progressive legislative step, it does not fully resolve the complexities associated with digital evidence. The law provides a foundation, but its success depends on effective enforcement, judicial clarity, and technological advancement.

ISSN: 2582-6433

Thus, the study concludes that a holistic approach—combining legal reform, institutional capacity building, and technological expertise—is essential to ensure that digital evidence serves as a reliable and effective tool in criminal trials.

11. SUGGESTIONS AND REFORMS

In light of the challenges identified, there is a pressing need to strengthen the legal and institutional framework governing digital evidence in India. While the Bharatiya Sakshya Adhiniyam, 2023 marks a progressive step, its effectiveness depends on the implementation of targeted reforms[38].

11.1 Standardization of Procedures

A uniform and well-defined procedure for the collection, preservation, and analysis of digital evidence is essential. Establishing standardized forensic protocols, similar to international practices, can ensure consistency and prevent contamination or tampering of evidence. Clear guidelines should be issued for maintaining the chain of custody and handling electronic records[39].

11.2 Strengthening Technical Infrastructure

There is an urgent need to enhance technical infrastructure and capacity within law enforcement agencies and forensic laboratories. Investment in advanced forensic tools, digital analysis software, and secure data storage systems will improve the reliability of digital evidence.

Additionally, the establishment of specialized cyber forensic units across jurisdictions can facilitate efficient handling of complex cases involving electronic data.

11.3 Training and Capacity Building

Effective use of digital evidence requires specialized training for police officials, prosecutors, and judicial officers. Regular training programs and workshops should be conducted to improve understanding of cyber forensics, data analysis, and evidentiary requirements.

Judicial officers, in particular, must be equipped to evaluate technical evidence and expert testimony with greater clarity and confidence.

[38] Law Commission of India, Report No. 185 on Review of the Indian Evidence Act.
[39] Association of Chief Police Officers, Good Practice Guide for Digital Evidence (2012).

ISSN: 2582-6433

11.4 Clarification of Legal Provisions

Although the new legislation seeks to simplify admissibility requirements, further judicial and legislative clarification is necessary to ensure uniform interpretation. Clear guidelines regarding certification, authentication, and admissibility standards will reduce ambiguity and prevent inconsistent application.

11.5 Integration of Technology in Courts

The judicial system should adopt digital tools and e-court systems to facilitate the presentation and evaluation of electronic evidence. Secure digital platforms for submission and storage of evidence can enhance efficiency and reduce the risk of data loss or tampering[40].

11.6 Protection of Privacy and Data

Given the sensitive nature of digital evidence, it is essential to establish safeguards for privacy and data protection. Legal provisions should ensure that personal data is accessed and used only to the extent necessary for investigation, with adequate checks to prevent misuse[41].

12. CONCLUSION

The increasing reliance on digital technology has transformed the landscape of criminal justice, making digital evidence an indispensable component of modern trials[42]. This study highlights that while the law has evolved to accommodate technological advancements, significant challenges remain in ensuring the admissibility and reliability of electronic records.

The transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 represents a progressive step towards modernizing the evidentiary framework in India[43]. The new legislation seeks to simplify procedures and recognize the practical realities of digital evidence. However, its success largely depends on effective implementation and consistent judicial interpretation.

The analysis reveals that while the legal framework has become more flexible, concerns relating to authenticity, data integrity, technical expertise, and privacy continue to pose

[40] e-Courts Mission Mode Project, Phase ll, Government of India.
[41] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C 1.
[42] Stephen Mason, Electronic Evidence (5th ed., 2021).
[43] Bharatiya Sakshya Adhiniyam, 2023).

ISSN: 2582-6433

significant obstacles. The absence of standardized procedures and adequate infrastructure further complicates the handling of digital evidence in criminal trials[44].

At a broader level, the study underscores the need to strike a balance between technological adaptability and evidentiary reliability. Digital evidence offers immense potential in uncovering truth, but its misuse or misinterpretation can equally undermine justice.

Ultimately, the admissibility of digital evidence must be guided by principles of fairness, accuracy, and accountability. A comprehensive approach—combining legal reform, technological advancement, and institutional capacity building—is essential to ensure that digital evidence serves as a reliable tool in the administration of criminal justice.

REFERENCES

Books

- Avtar Singh, Principles of the Law of Evidence (Central Law Publications).
- V.N. Shukla, Law of Evidence (Eastern Book Company).
- M.P. Jain, Indian Constitutional Law (LexisNexis).
- Ratanlal & Dhirajlal, The Law of Evidence (LexisNexis).
- Paul W. Grimm et al., Electronic Discovery and Digital Evidence (American Bar Association).

Journal Articles

- Stephen Mason, "The Admissibility of Electronic Evidence," International Journal of Evidence & Proof.
- Paul W. Grimm, "Authentication of Social Media Evidence," American Journal of Trial Advocacy.
- K.K. Mathew, "Electronic Evidence and Its Admissibility," Journal of the Indian Law Institute.
- Susan Brenner, "Digital Evidence and the New Criminal Procedure," Crime, Law and Social Change.
- Orin S. Kerr, "Digital Evidence and the New Criminal Procedure," Columbia Law Review.

[44] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 1.

ISSN: 2582-6433

Case Laws (India)

- Anvar P.V. v. P.K. Basheer
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal
- State (NCT of Delhi) v. Navjot Sandhu

Case Laws (International)

- Lorraine v. Markel American Insurance Co.
- R v. Shepherd

Reports and Institutional Sources

- Law Commission of India, Reports on Evidence Law and Criminal Justice Reforms.
- National Crime Records Bureau, Reports on Cyber Crime Statistics.
- Ministry of Electronics and Information Technology, Guidelines on Electronic Records and Digital Governance.

Statutes and Legal Provisions

- Bharatiya Sakshya Adhiniyam, 2023
- Indian Evidence Act, 1872
- Information Technology Act, 2000