DIGITAL EVIDENCE IN THE ERA OF ARTIFICIAL INTELLIGENCE: A DOCTRINAL STUDY OF ADMISSIBILITY, AUTHENTICITY, AND EVIDENTIARY INTEGRITY UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Rudra Prasad Rimal, LLM (Criminal Law), Faculty of Law, the ICFAI University, Gangtok, Sikkim.

Dr. Joshika Thapa, Assistant Professor, Faculty of Law, the ICFAI University, Gangtok, Sikkim.

ABSTRACT

The increasing digitisation of human activity has fundamentally transformed the administration of criminal justice. Electronic records such as emails, mobile phone data, social media communications, surveillance footage, cloud-based records, and digital transactions have become indispensable sources of evidence in contemporary criminal investigations. Recognizing this technological transformation, the Parliament enacted the Bharatiya Sakshya Adhiniyam, 2023, replacing the Indian Evidence Act, 1872 and introducing a modern evidentiary framework for the digital era. While the new legislation represents a significant step towards accommodating electronic records within judicial proceedings, the rapid emergence of artificial intelligence, deepfake technology, synthetic media, and algorithmic manipulation has created unprecedented challenges relating to evidentiary authenticity and reliability. This article examines the evolution of electronic evidence in India, analyses the treatment of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023, and evaluates the implications of artificial intelligence for criminal adjudication. It argues that the future of evidence law must move beyond questions of admissibility and focus increasingly upon authenticity. The article further proposes an authenticity-centred evidentiary framework that integrates legal doctrine, forensic science, technological expertise, and institutional preparedness to ensure the continued integrity of judicial truth-finding in the age of artificial intelligence.

Keywords: Digital Evidence, Bharatiya Sakshya Adhiniyam, Artificial Intelligence, Deepfakes, Electronic Records, Criminal Justice, Forensic Science, Authentication

1. Introduction

The law of evidence occupies a central position within the criminal justice system. It provides the framework through which courts determine the relevance, admissibility, reliability, and probative value of information presented during judicial proceedings. For more than a century, Indian evidence law operated under the Indian Evidence Act, 1872, a statute drafted during a period when information existed predominantly in physical form and technological modes of communication were limited in scope and complexity.[1] The emergence of the digital age has fundamentally altered this evidentiary landscape. Modern criminal investigations increasingly rely upon information generated through electronic devices, internet communications, digital transactions, surveillance technologies, and social media platforms. Mobile phones have become repositories of extensive personal and transactional information. Emails have replaced traditional correspondence. Cloud computing enables storage and transmission of vast quantities of data across national boundaries. Social networking platforms preserve records of communications, relationships, and behavioural patterns. Consequently, electronic records now constitute some of the most significant forms of evidence presented before courts.[2] Recognizing these developments, the Parliament enacted the Bharatiya Sakshya Adhiniyam, 2023 (hereinafter "BSA"), replacing the Indian Evidence Act, 1872. One of the principal objectives of the new legislation is to modernize evidentiary principles and align them with the realities of a technology-driven society. The statute acknowledges the centrality of electronic records within contemporary litigation and seeks to simplify the legal framework governing their admissibility and evidentiary value.[3] However, technological advancement has simultaneously generated new challenges. The rapid development of artificial intelligence (AI) has transformed the nature of digital evidence itself. Deepfake videos, synthetic audio recordings, AI-generated images, algorithmically created documents, and sophisticated manipulation technologies have made it increasingly difficult to distinguish authentic evidence from fabricated content. Traditional assumptions regarding the reliability of audiovisual records can no longer be taken for granted.[4] The challenge confronting courts today is therefore fundamentally different from that which existed even a decade ago. Earlier debates concerning electronic evidence focused primarily upon admissibility and

[1] Sir James Fitzjames Stephen, *The Indian Evidence Act with an Introduction on the Principles of Judicial Evidence* 12 (Macmillan, London, latest ed.)
[2] Avtar Singh, *Principles of the Law of Evidence* 801 (Central Law Publications, Allahabad, 25th edn., 2024).
[3] Bharatiya Sakshya Adhiniyam, 2023, Statement of Objects and Reasons.
[4] Lyria Bennett Moses, "Artificial Intelligence in Courts and Tribunals" (2023) 46 *UNSW Law Journal* 75, 79.

procedural compliance. Contemporary concerns increasingly revolve around authenticity, reliability, and technological trustworthiness. The central question is no longer whether electronic records should be admitted into evidence, but whether such records accurately reflect reality or not.[5] This article examines the transformation of evidence law in India through the lens of digital technology and artificial intelligence. It argues that while the Bharatiya Sakshya Adhiniyam, 2023 represents a significant step towards modernization, and future evidentiary frameworks must increasingly focus upon authentication mechanisms capable of addressing emerging technological threats. The article further contends that preserving the integrity of criminal adjudication in the age of artificial intelligence requires a synthesis of legal doctrine, forensic science, technological expertise, and institutional preparedness.

2. Evolution of Digital Evidence in India

a. Traditional Evidentiary Framework

The Indian Evidence Act, 1872 was enacted at a time when documentary evidence consisted primarily of written records maintained in physical form. The evidentiary framework established by Sir James Fitzjames Stephen reflected nineteenth-century assumptions regarding the creation, preservation, and transmission of information. Documentary evidence was largely synonymous with paper-based records, while oral testimony constituted the principal means through which facts were established before courts.[6] For much of its history, the Act functioned effectively within a legal environment characterized by physical documentation. However, the latter half of the twentieth century witnessed rapid technological developments that fundamentally transformed methods of communication, information storage, and record creation. The emergence of computers, electronic databases, digital communications, and internet technologies exposed significant limitations within the traditional evidentiary framework.[7] Unlike physical documents, electronic records are intangible. They may be copied, altered, transmitted, encrypted, or deleted without visible indications of modification. A single digital file may exist simultaneously in multiple locations, making conventional notions of originality and possession increasingly difficult to apply.

[5] Orin S. Kerr, "Digital Evidence and the New Criminal Procedure" (2005) 105 *Columbia Law Review* 279, 281.
[6] Sir James Fitzjames Stephen, *supra* note 1 at 2.
[7] M. Monir, *Principles and Digest of the Law of Evidence* 1142 (Universal Law Publishing, New Delhi, 14th edn., 2023).

Consequently, courts faced growing challenges when attempting to evaluate the admissibility and reliability of electronic evidence.[8]

b. The Information Technology Act, 2000 and the Recognition of Electronic Records

India's first comprehensive legislative response to digital technology emerged through the Information Technology Act, 2000. Enacted primarily to facilitate electronic commerce and digital communications, the legislation also introduced important amendments to the Indian Evidence Act.[9] The Information Technology Act recognized electronic records and electronic signatures, thereby providing legal validity to digital transactions and communications. Simultaneously, amendments were introduced to the Indian Evidence Act through the insertion of Sections 65A and 65B, which established special rules governing the admissibility of electronic evidence.[10] Section 65B represented a significant departure from traditional evidentiary principles. It created a self-contained mechanism for the admission of electronic records and required the production of a certificate specifying the manner in which the electronic record was produced, the device involved, and the conditions ensuring reliability.[11] Although intended to address concerns relating to authenticity and integrity, the provision subsequently generated substantial judicial controversy.

c. Judicial Development of Electronic Evidence Jurisprudence

The Supreme Court's jurisprudence concerning electronic evidence evolved through a series of landmark decisions that sought to reconcile statutory provisions with practical realities. In *State (NCT of Delhi) v. Navjot Sandhu*, commonly known as the Parliament Attack Case, the Court adopted a relatively liberal approach towards electronic evidence. It held that even in the absence of a certificate under Section 65B, electronic records could be admitted through other provisions of the Evidence Act.[12] The decision was widely perceived as facilitating access to digital evidence, particularly in criminal proceedings. However, this position was subsequently reconsidered in *Anvar P.V. v. P.K. Basheer*. The Supreme Court held that Section 65B constituted a complete code governing the admissibility of electronic records and that compliance with its certification requirements was mandatory whenever

[8] Eoghan Casey, *Digital Evidence and Computer Crime* (Academic Press, 4th edn., 2020) 48.
[9] Information Technology Act, 2000.
[10] Information Technology Act, 2000, ss. 91–94.
[11] Indian Evidence Act, 1872, s. 65B.
[12] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

electronic evidence was produced in the form of secondary evidence.[13] The judgment significantly altered the evidentiary landscape and introduced a stricter approach towards digital evidence. The practical implications of *Anvar* soon became apparent. In many cases, parties encountered difficulties obtaining certificates from third parties who controlled relevant electronic systems. These concerns prompted reconsideration in *Shafhi Mohammad v. State of Himachal Pradesh*, where a two-judge Bench suggested that the certificate requirement could be relaxed in circumstances where the party seeking to produce evidence lacked control over the device in question.[14] The resulting uncertainty was ultimately resolved by a three-judge Bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. The Court reaffirmed the correctness of *Anvar* and held that Section 65B certification remained mandatory, subject only to limited exceptions recognised by law.[15] Collectively, these decisions illustrate the judiciary's efforts to address the unique challenges posed by electronic evidence while balancing concerns relating to reliability, authenticity, and procedural fairness.

d. Need for Legislative Reform

By the second decade of the twenty-first century, it had become increasingly apparent that the legal framework governing electronic evidence required comprehensive reconsideration. The proliferation of smartphones, cloud computing, social media platforms, digital payment systems, and internet-based communications has transformed the nature of criminal investigations. Electronic evidence was no longer exceptional. It had become routine. Investigative agencies increasingly relied upon call detail records, WhatsApp communications, GPS data, CCTV footage, digital financial transactions, and internet activity logs. Courts were required to evaluate complex technological evidence on a regular basis. The procedural difficulties associated with Section 65B certification generated concerns regarding both efficiency and access to justice.[16] At the same time, emerging technologies such as artificial intelligence, machine learning, and synthetic media began creating entirely new evidentiary challenges that had not been contemplated when Section 65B was originally enacted. The enactment of the Bharatiya Sakshya Adhiniyam, 2023 must therefore be understood within this broader context of technological transformation and legal adaptation.

[13] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[14] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[15] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[16] Batuk Lal, *The Law of Evidence* 987–995 (Central Law Agency, Allahabad, 28th edn., 2023).

3. Bharatiya Sakshya Adhiniyam, 2023 and the Reconceptualization of Electronic Evidence

a. Electronic Records as Primary Evidence

One of the most significant innovations introduced by the Bharatiya Sakshya Adhiniyam, 2023 is the recognition of electronic records as primary evidence. This development reflects a conscious legislative attempt to align evidentiary doctrine with the realities of contemporary communication and information storage. The distinction is important because under traditional evidence law, primary evidence occupied a superior evidentiary position owing to its direct connection with the original source of information.[17] Historically, courts viewed electronic records with caution because digital information often existed in forms that could be copied, transmitted, and reproduced with ease. Consequently, concerns relating to originality and authenticity shaped judicial treatment of electronic evidence. The legal framework that evolved under the Indian Evidence Act, particularly through Section 65B, sought to address these concerns by introducing certification requirements designed to establish reliability.[18] However, technological developments have rendered many traditional assumptions regarding originality increasingly difficult to sustain. In the digital environment, the concept of an "original" record is often functionally meaningless. A digital file may be replicated perfectly without any degradation in quality. Multiple identical versions may exist simultaneously across different devices, servers, and cloud-storage systems. The evidentiary significance of a digital record therefore lies less in its physical form and more in its integrity and authenticity.[19] The Bharatiya Sakshya Adhiniyam acknowledges this reality by treating electronic records as legitimate forms of primary evidence. This legislative shift recognizes that digital information has become the dominant medium through which contemporary society communicates, transacts, and records events. As a consequence, courts are no longer required to treat electronic evidence as exceptional or inherently inferior to traditional documentary evidence.[20] The significance of this reform extends beyond procedural convenience. By formally recognizing electronic records as primary evidence, the statute acknowledges the transformation of evidentiary reality itself. The law is no longer adapting to technology as an

[17] Vepa P. Sarathi, *Law of Evidence* 402 (Eastern Book Company, Lucknow, 9th edn., 2022) .
[18] Indian Evidence Act, 1872, s. 65B.
[19] George L. Paul and Jason R. Baron, *Information Inflation: Can the Legal System Adapt?*61 (American Bar Association, Chicago, latest edn.)
[20] Bharatiya Sakshya Adhiniyam, 2023.

external phenomenon; rather, it is recognizing technology as an integral component of modern evidentiary systems.

b. Expanding Scope of Digital Evidence

The concept of electronic evidence encompasses a vast range of information sources. Contemporary criminal investigations routinely involve:

i. Mobile phone records;

ii. Emails and electronic correspondence;

iii. Social media communications;

iv. Instant messaging applications;

v. Surveillance footage;

vi. GPS and location data;

vii. Cloud-based records;

viii. Digital financial transactions;

ix. Internet browsing histories;

x. Metadata and system logs.[21]

These sources frequently provide critical information regarding motive, intent, identity, movement, communication patterns, and criminal conduct. In many cases, electronic evidence constitutes the most reliable and objective source of information available to investigators. For example, location data generated through mobile devices may establish a suspect's presence at a crime scene. Financial transaction records may reveal patterns of fraud or corruption. Surveillance footage may identify perpetrators and reconstruct events. Digital communications may provide direct evidence of criminal conspiracy or planning.[22] The increasing reliance upon

[21] Eoghan Casey, *supra* note 8 at 6.
[22] Kathryn Inman and Norah Rudin, *Digital Evidence in Criminal Investigation and Proceedings* 145–175 (CRC Press, latest edn.)

such evidence demonstrates that criminal adjudication has entered an era in which digital information is often more significant than traditional testimonial evidence. Consequently, evidentiary law must ensure not only that electronic records are admissible but also that they are evaluated through principles capable of addressing their unique technological characteristics.

c. Continuing Relevance of Certification

Although the Bharatiya Sakshya Adhiniyam modernizes the treatment of electronic records, questions relating to certification continue to occupy an important place within evidentiary analysis. Certification serves several functions. It identifies the source of the electronic record, explains the manner in which it was produced, and provides assurances regarding the functioning of the relevant device or system. Certification may therefore assist courts in assessing reliability and authenticity.[23] However, experience under Section 65B demonstrated that certification can also become excessively procedural. In many instances, litigation focused less upon the substantive reliability of evidence and more upon technical compliance with statutory requirements. The Supreme Court's decision in *Arjun Panditrao Khotkar* reaffirmed the mandatory nature of certification while recognizing that practical difficulties may arise in obtaining certificates from third parties controlling relevant devices or systems.[24] These challenges remain relevant under the new evidentiary framework. The central question is therefore whether certification should be regarded as an end in itself or merely as one mechanism among several for establishing authenticity. This narrow focus upon procedural compliance risks the broader objective of evidence law, namely the discovery of truth. A certificate may demonstrate compliance with statutory requirements, but it does not necessarily guarantee that a digital record accurately reflects reality. This distinction becomes particularly significant in the age of artificial intelligence.

4. Certification versus Authenticity: The Changing Nature of Evidentiary Reliability

a. The Traditional Approach to Authenticity

Traditionally, authenticity was often inferred from the physical characteristics of evidence. A handwritten document could be examined for signatures, handwriting patterns,

[23] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[24] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

paper quality, and other identifying features. Photographs and audiovisual recordings were generally presumed to depict actual events unless evidence suggested otherwise.[25] The transition to digital technology complicated these assumptions. Electronic records possess none of the physical attributes associated with conventional documentary evidence. Their authenticity must therefore be established through alternative means. Section 65B certification was intended to address this challenge by creating a mechanism through which electronic records could be authenticated. Judicial practice consequently came to treat certification as the principal safeguard against manipulation and unreliability.[26] Yet technological developments have revealed the limitations of this approach.

b. Certification is not Synonymous with Authenticity

An assumption that certification guarantees authenticity is increasingly difficult to sustain. A certificate may establish the source of a record and the manner in which it was generated, but it cannot independently verify the truthfulness of the underlying content. A fabricated digital file may satisfy procedural requirements while remaining substantively false. Conversely, a genuinely reliable electronic record may encounter evidentiary obstacles owing to procedural deficiencies unrelated to its authenticity.[27] This distinction illustrates a broader conceptual problem within contemporary evidence law. Procedural admissibility and substantive reliability are not identical concepts. While admissibility determines whether evidence may be considered by a court, authenticity concerns whether that evidence accurately represents reality. The growing sophistication of digital technologies has made this distinction increasingly important.

c. Artificial Intelligence and the Collapse of Traditional Assumptions

Artificial intelligence represents perhaps the most significant challenge to evidentiary authenticity in modern legal history. Recent advances in machine learning and generative AI have enabled the creation of highly realistic synthetic media. Contemporary AI systems can generate text, images, videos, audio recordings, and digital documents that are often indistinguishable from genuine materials.[28] Deepfake technology provides a particularly

[25] Avtar Singh, *supra* note 2 at 4.
[26] Batuk Lal, *supra* note 16 at 7.
[27] Orin S. Kerr, *supra* note 5 at 8.
[28] Matthew Lavy and Daniel Sokol, *Artificial Intelligence and the Law* 122 (Cambridge University Press, Cambridge, 2023).

striking example. By analyzing vast datasets of audiovisual information, AI systems can produce realistic videos depicting individuals saying or doing things that never actually occurred. Similar technologies can replicate human voices with remarkable accuracy, creating convincing audio recordings from minimal source material.[29] These developments fundamentally undermine traditional assumptions regarding audiovisual evidence. Historically, courts often regarded photographs and recordings as particularly persuasive because they appeared to provide direct access to factual reality. Artificial intelligence challenges this evidentiary foundation. A video recording can no longer be presumed genuine merely because it appears authentic. An audio recording can no longer be accepted solely because it sounds convincing. A document can no longer be trusted simply because it resembles a legitimate record. The implications for criminal justice are profound.

d. The Emergence of the "Liar's Dividend"

Artificial intelligence creates a paradoxical evidentiary problem often described as the "liar's dividend."[30] The concept refers to the ability of individuals to deny genuine evidence by claiming that it has been fabricated through artificial intelligence. As public awareness of deepfake technology increases, even authentic recordings may become vulnerable to challenge. A defendant confronted with genuine surveillance footage may allege that the recording is a deepfake. A public official may deny an authentic recording by claiming technological manipulation. Witnesses may dispute genuine evidence by invoking the possibility of AI-generated fabrication. The liar's dividend therefore operates in two directions: First, fabricated evidence may be accepted as genuine. Secondly, genuine evidence may be dismissed as fabricated. Both outcomes undermine the truth-seeking function of judicial proceedings. The challenge confronting evidence law is therefore not merely technological but epistemological. Courts must develop mechanisms capable of distinguishing reality from increasingly sophisticated forms of digital fabrication.

e. Towards an Authenticity-Centred Framework

The developments discussed above suggest that future evidentiary systems must move beyond a narrow focus upon admissibility and embrace a broader concern with authenticity.

[29] Andrew Murray, "Artificial Intelligence and Evidentiary Challenges" (2024) 40 *Computer Law & Security Review* 102, 107.
[30] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security" (2019) 107 *California Law Review* 1753, 1764.

Certification remains important, but it should be regarded as only one component of a comprehensive authentication framework. Digital forensic techniques, metadata analysis, hash-value verification, chain-of-custody documentation, expert testimony, and technological verification mechanisms must increasingly complement traditional evidentiary safeguards.[31] The future of evidence law will depend upon the ability of legal institutions to evaluate not merely whether digital evidence has been properly produced, but whether it can genuinely be trusted. The age of artificial intelligence requires a corresponding evolution in evidentiary thought.

5. Artificial Intelligence, Deepfakes and the New Evidentiary Crisis

a. Artificial Intelligence and the Transformation of Evidence

The twenty-first century has witnessed technological developments that have transformed not merely the collection and storage of evidence but the very nature of evidentiary material itself. Artificial intelligence systems are now capable of generating text, images, audio recordings, videos, and digital documents that closely resemble authentic human-created content. The emergence of generative artificial intelligence has therefore created unprecedented challenges for legal systems across the world.[32] Historically, evidence law operated on the assumption that certain categories of evidence possessed inherent indicators of authenticity. A photograph was presumed to represent an actual scene. A video recording was treated as a visual account of real events. An audio recording was generally regarded as a faithful reproduction of spoken words. Although these forms of evidence could be manipulated, such alterations typically required specialised expertise and were often detectable through careful examination.[33] Artificial intelligence has fundamentally altered this equation. Modern AI systems can create highly convincing synthetic media with minimal technical expertise and relatively modest resources. The democratisation of such technology means that fabrication is no longer confined to sophisticated state actors or specialised experts. Individuals with ordinary computing resources may now generate content capable of deceiving both human observers and conventional verification mechanisms. This development poses a direct challenge to the foundational objective of evidence law, the accurate reconstruction of past events.

[31] Jason Sachowski, *Implementing Digital Forensic Readiness* 85-92 (Syngress Publishing, 2019).
[32] Matthew Lavy and Daniel Sokol, *Artificial Intelligence and the Law* 120 (Cambridge University Press, Cambridge, 2023).
[33] Susan Brenner, "Cybercrime and Digital Evidence" (2011) 16 *Journal of Technology Law & Policy* 1, 8.

b. Deepfake Technology and Criminal Adjudication

Deepfake technology represents one of the most significant manifestations of artificial intelligence within the evidentiary domain. The term "deepfake" generally refers to synthetic audiovisual content created through machine-learning techniques that enable the realistic manipulation or generation of images, videos, and audio recordings.[34] The legal implications of deepfakes are profound. Criminal proceedings frequently depend upon visual and audio evidence. Surveillance footage, body-camera recordings, mobile phone videos, intercepted communications, and digital recordings often play a decisive role in establishing guilt or innocence. Deepfake technology undermines the reliability traditionally associated with such evidence. For example, a fabricated video may depict an individual participating in criminal activity that never occurred. A synthetic audio recording may falsely attribute incriminating statements to an accused person. Manipulated visual evidence may be used to fabricate alibis, distort timelines, or implicate innocent individuals. The risk extends beyond deliberate fabrication. Even the possibility that evidence may be artificially generated introduces uncertainty into judicial fact-finding. Courts can no longer assume that visual or audio realism necessarily corresponds with factual reality.[35] The evidentiary challenge therefore lies not merely in detecting fabricated content but in preserving confidence in authentic evidence.

c. Impact on Criminal Investigations

The proliferation of AI-generated content may significantly affect investigative processes. Investigating agencies traditionally rely upon digital evidence to establish timelines, identify suspects, corroborate witness testimony, and reconstruct events. However, the presence of synthetic media within digital ecosystems complicates these functions. Investigators may encounter fabricated evidence intentionally introduced to mislead inquiries. Digital platforms may contain manipulated recordings designed to influence public opinion or interfere with legal proceedings. Cybercriminals may exploit artificial intelligence to generate fraudulent records capable of misleading investigators.[36] Furthermore, the volume of digital information generated by contemporary society presents practical difficulties. Investigators increasingly confront vast quantities of data requiring analysis and verification. Artificial

[34] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security" (2019) 107 *California Law Review* 1753, 1758.
[35] Andrew Murray, "Artificial Intelligence and Evidentiary Challenges" (2024) 40 *Computer Law & Security Review* 102, 109.
[36] Pavan Duggal, *Cyber Law and Emerging Technologies* 301 (Universal Law Publishing, latest edn.)

intelligence simultaneously contributes to and complicates this process by producing content at unprecedented speed and scale. The future effectiveness of criminal investigations will therefore depend upon the development of sophisticated verification mechanisms capable of distinguishing genuine evidence from synthetic content.

6. Digital Chain of Custody, Forensic Integrity and the Science of Authentication

a. Importance of Digital Forensics

As artificial intelligence challenges traditional assumptions regarding evidentiary reliability, digital forensic science assumes increasing significance. The authenticity of electronic evidence cannot depend solely upon visual inspection or procedural certification. Instead, courts must increasingly rely upon scientific methods capable of establishing integrity and provenance.[37] Digital forensics involves the identification, preservation, examination, analysis, and presentation of electronic evidence. The discipline provides methodological safeguards designed to ensure that electronic records remain reliable throughout investigative and judicial processes. Unlike traditional documentary evidence, digital information is particularly vulnerable to alteration. Consequently, forensic protocols emphasize preservation and verification at every stage of evidence handling.

b. Hash Values and Integrity Verification

One of the most important forensic tools is hash-value analysis. A hash value is a unique alphanumeric output generated through mathematical algorithms applied to digital data. Even a minor alteration to a file results in a different hash value.[38] Consequently, hash verification enables investigators to demonstrate that an electronic record has remained unchanged from the moment of acquisition through its presentation before a court. Hash values function as digital fingerprints. Their use has become a widely accepted method of establishing integrity within digital forensic investigations. Courts increasingly recognize hash verification as an important indicator of reliability and authenticity.

[37] Kathryn Inman and Norah Rudin, *Digital Evidence in Criminal Investigation and Proceedings* 205 (CRC Press, latest edn.).
[38] Jason Sachowski, *Implementing Digital Forensic Readiness* 85 (Syngress Publishing, 2019).

c. Metadata Analysis

Metadata refers to information embedded within digital files that describes characteristics such as creation dates, modification histories, authorship details, device information, and transmission records.[39] Metadata frequently provides critical insights into the provenance and history of electronic evidence. For example, discrepancies between alleged creation dates and metadata records may indicate manipulation. Similarly, metadata may reveal whether a file has been edited, copied, transferred, or accessed by unauthorized individuals. The forensic examination of metadata has therefore become an indispensable component of modern evidentiary analysis.

d. Chain of Custody

The concept of chain of custody occupies a central position within evidence law. It refers to the documented history of possession, control, transfer, analysis, and preservation of evidence from collection to courtroom presentation.[40] In the context of digital evidence, maintaining a reliable chain of custody is particularly important because electronic records may be altered without visible signs of modification. A properly documented chain of custody enables courts to assess whether evidence has been tampered with, substituted, or compromised. Conversely, deficiencies in chain-of-custody documentation may undermine confidence in evidentiary integrity. As digital evidence becomes increasingly central to criminal adjudication, chain-of-custody protocols must be strengthened and standardized across investigative agencies.

7. Comparative Analysis

Comparative analysis reveals that jurisdictions across the world are confronting similar challenges relating to digital evidence and artificial intelligence. In the United States, Rule 901 of the Federal Rules of Evidence requires proponents of evidence to establish that a document or recording is what it purports to be. Increasingly, courts have relied upon expert testimony and forensic analysis when assessing disputed digital evidence.[41] The United Kingdom similarly emphasizes reliability and judicial scrutiny. Courts possess broad powers to evaluate

[39] Eoghan Casey, *supra* note 8 at 6.
[40] Kathryn Inman and Norah Rudin, *supra* note 37 at 14.
[41] Federal Rules of Evidence, Rule 901 (United States).

evidentiary authenticity and exclude unreliable material where necessary. Legislative and judicial developments have increasingly recognized the challenges associated with digital manipulation and synthetic media.[42] Singapore has emerged as a leader in technological governance and judicial modernization. Its courts have invested significantly in technological literacy and digital readiness, recognizing that future litigation will increasingly involve complex electronic evidence.[43] The European Union has adopted a broader regulatory approach through initiatives aimed at governing artificial intelligence and mitigating risks associated with synthetic content. Transparency obligations, accountability mechanisms, and risk-based regulation have become important features of the European response.[44] Although specific approaches vary, a common theme emerges: authenticity is increasingly regarded as the defining challenge of modern evidence law.

8. Conclusion and Way Forward

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 marks an important milestone in the evolution of Indian evidence law. By recognizing electronic records as primary evidence, the legislation reflects the realities of a society increasingly shaped by digital technology. Yet technological progress has simultaneously created new threats to evidentiary reliability. Artificial intelligence, deepfake technology, synthetic media, and algorithmic manipulation have fundamentally challenged traditional assumptions regarding authenticity. The future of criminal justice will therefore depend upon the ability of courts to move beyond an admissibility-centred framework and embrace a more sophisticated authenticity-centred approach. Certification, while important, cannot by itself guarantee reliability. Scientific verification, digital forensics, metadata analysis, chain-of-custody safeguards, and technological expertise must become integral components of modern evidentiary practice. Ultimately, evidence law exists to assist courts in discovering the truth. The preservation of that objective in an age of artificial intelligence represents one of the most significant legal challenges of the twenty-first century. Whether the justice system succeeds in meeting this challenge will determine not only the future of digital evidence but also the future credibility of judicial truth-finding itself.

[42] Police and Criminal Evidence Act, 1984 (UK); Criminal Justice Act, 2003 (UK).
[43] Supreme Court of Singapore, *Technology and the Future of Justice* (Judicial Education Materials, 2023).
[44] European Parliament, Artificial Intelligence Act, 2024.

Nevertheless, the rapid evolution of artificial intelligence necessitates further reform. First, statutory recognition should be provided to AI-generated and AI-manipulated evidence. Courts require clear legislative guidance regarding the evaluation of synthetic media and algorithmically generated content.[45] Secondly, forensic authentication should be encouraged whenever the authenticity of electronic evidence is seriously disputed. Courts should possess clear authority to require technical verification through accredited forensic laboratories. Thirdly, a National Digital Evidence Protocol should be developed to establish uniform standards governing collection, preservation, examination, and presentation of electronic records. Fourthly, investment in forensic infrastructure must be prioritized. The increasing volume and complexity of digital evidence demand specialized expertise and technological resources. Finally, judicial education and professional training should receive sustained attention. Judges, prosecutors, investigators, and defence counsel must develop familiarity with emerging technologies if they are to effectively evaluate electronic evidence. These reforms would strengthen the capacity of Indian courts to address future evidentiary challenges while preserving public confidence in the administration of justice.

[45] NITI Aayog, *National Strategy for Artificial Intelligence* (Government of India, New Delhi, 2023).