Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 16 ~ Issue 2 (Mar. – Apr. 2026) pp: 41-47
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

An Analytical Assessment of Cyber Investigation Processes and the Admissibility of Digital Evidence

Suneeta Rathore
Researc Scholar

Prof (Dr.) Aryendu Dwivedi
Professor
Instute of Legal Studies, Shri Ramswaroop Memorial University Lucknow Deva Road Barabanki Uttar Pradesh

ABSTRACT
The exponential growth of digital technologies has radically changed the nature of the criminal activity, whereby a paradigm shift in the investigative trends and the quality of evidence is required. This paper is an analytical evaluation of the process of cyber investigation and a critical review of legal context in which the admissibility of digital evidence in a courtroom can be presented. The main aims are to assess the efficiency of the digital forensic investigation models and examine the statutory and judicial criteria according to which the electronic evidence can be admissible. The research methodology of the study is doctrinal and analytical, based on the primary legal sources (statutes, judicial pronouncements and international conventions) complemented by the secondary ones (scholarly literature and institutional reports). The results indicate that the digital forensic frameworks have evolved to a considerable extent, but there are major issues surrounding the maintenance of chain of custody, evidence integrity, and alignment of national requirement of law with the transnational requirements of cyber investigation. The paper arrives at the conclusion that an integrated strategy that encompasses sound forensic guidelines and dynamic legal systems is essential in order to have digital evidence pass the test of authenticity, accuracy, completeness, and convincingness by the court of law.

Keywords: *Digital Evidence, Cyber Investigation, Digital Forensics, Admissibility, Chain of Custody*

I. INTRODUCTION

In the twenty-first century, there has been a unanimous integration of human life and digital technology, which has fundamentally transformed the nature, perpetration and detection of criminal behavior. With almost all the areas of human interaction commercial transactions, interpersonal communications, governance, and financial operations switching to the digital platform, the eviary scene of the litigation process has been changing accordingly. Data stored in or transferred through electronic devices, including computers, mobile phones, servers, and cloud systems, has become one of the most important factors affecting the resolution of a criminal and civil case.[1]Digital evidence is not only important in conventional cybercrime but also in practically every type of criminal behavior. Digital footprints such as emails, social media conversations, server logs, metadata, GPS coordinates, CCTV videos, and transactional logs are often the most probative evidence held by the investigating agencies in the modern criminal investigation field.[2]National Institute of Standards and Technology (NIST) has acknowledged that digital evidence refers to any information in a binary form that may be of use in criminal or other judicial inquires and actions, and that the evidentiary importance of such evidence lies in the content and associated information, and not the medium.[3]

[1]Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd edn, Academic Press, 2011).

[2]NIST Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response* (National Institute of Standards and Technology, 2006).

[3]NIST, *Digital Evidence*, National Institute of Standards and Technology, U.S. Department of Commerce.

Nevertheless, the very nature of digital evidence volatility, susceptibility to manipulation, ability to be duplicated and reliance on intermediary devices to make it understandable to human beings puts special burdens on it that make it fundamentally different than the old hard copy evidence. In contrast with a fingerprint or a document that is handwritten, digital evidence can be modified without leaving any visible evidence in case the appropriate forensic standards are not followed. Such a flexibility requires stringent procedural protection during the scene of evidence gathering, storage, analysis and presentation.[4]Legal regulations of digital evidence have been developed as a complicated sequence of legislative acts, judicial interpretation, and international collaboration. Sections 65A and 65B are additions to the Indian Evidence Act, 1872, accomplished by the Information Technology Act, 2000, and which put in place a special regime of electronic records in India[5]This framework has also been updated by enacting the BharatiyaSakshyaAdhiniyam, 2023 replacing the Indian Evidence Act and adding more favorable provisions in Sections 61, 62, and 63 on recognition and admissibility of electronic and digital records.[6]On the international scale, the most extensive multilateral instrument on procedural issues of cyber investigation and the cross-national gathering of evidence is the Convention on Cybercrime of the Council of Europe (Budapest Convention, 2001).[7]Current paper provides a methodical review of the cyber investigative procedure starting with identification of digital evidence up to final delivery in court and a review of legal principles controlling each part of the process. The paper critically analyzes the sufficiency of current legal systems, finds out areas of enduring lapses between forensic practice and legal, and gives a recommendation on how to have a more efficient collaboration between investigative science and evidentiary law.

II. OBJECTIVES

1. To evaluate the procedural framework and operational efficacy of cyber investigation processes, including the stages of identification, preservation, acquisition, analysis, and reporting of digital evidence, and to assess the extent to which existing forensic methodologies comply with legal standards of evidence integrity.
2. To critically analyze the statutory provisions, judicial pronouncements, and international legal instruments governing the admissibility of digital evidence in courts of law, with specific reference to the standards of authenticity, reliability, and chain of custody mandated under Indian and comparative jurisprudence.

III. RESEARCH METHODOLOGY

The conducted study is based on a doctrinal and analytical research approach. The study also relies on primary law making bodies of law such as the Information Technology Act, 2000; the Indian Evidence Act, 1872 (since replaced by BharatibyasiSakshyaAdhiniyam, 2023); the BharatibyasiNagarikSurakshaSanhita, 2023; the Federal Rules of Evidence (United States); and the Convention on Cybercrime (Budapest Convention), 2001. The decision of the Supreme Court of India and High Courts and other concerned foreign courts have been judged to trace the development of the standards applied in digital evidence. The secondary sources dwell upon scholarly articles in peer-reviewed journals, institutional reports by the NIST, the United Nations Office on Drugs and Crime (UNODC), and the International Laboratory Accreditation Cooperation (ILAC) and authoritative treatises in digital forensics and cyber law. The qualitative approach to the analysis is taken through the use of comparative and interpretative approaches to assess the interdependence of the investigative processes and the legal admissibility standards.

IV. CYBER INVESTIGATION PROCESSES: A PROCEDURAL ANALYSIS

4.1 Conceptual Foundation of Digital Forensics

According to the definition made by the U.S. Department of Homeland Security, digital forensics is defined as a process of retrieving and retaining material available in digital devices in the process of conducting criminal investigations."[8]The field works on the boundaries of both computer science and law-enforcement, and

[4]Garfinkel, S.L., "Digital Forensics Research: The Next 10 Years," (2010) 7 *Digital Investigation* S64-S73.

[5]Information Technology Act, 2000 (Act No. 21 of 2000), Section 92 (amending the Indian Evidence Act, 1872 to insert Sections 65A and 65B).

[6]BharatiyaSakshyaAdhiniyam, 2023 (Act No. 47 of 2023), Sections 61, 62, 63.

[7]Convention on Cybercrime, Council of Europe, ETS No. 185, opened for signature November 23, 2001, entered into force July 1, 2004.

[8]U.S. Department of Homeland Security, *Best Practices for Seizing Electronic Evidence* (2007).

investigators in the field must have both technical analysis and legal compliance skills. The core aim of digital forensic investigation is to make a systematic investigation that will preserve a documented chain of evidence, hence, establishing what happened and when it happened on a computing device by whom it happened.[9]It has a number of specialized sub-disciplines such as computer forensics, mobile device forensics, network forensics, database forensics, and malware forensics which require different technical skills and methods.[10]Regardless of specialization, all forensic investigations have one principle in common there must be a method of gathering evidence, preservation, and analysis that lead to its admissibility in court.

4.2 Stages of Cyber Investigation

The process of cyber investigation, standardized and approved by NIST and supported by law enforcement agencies around the world, has five major steps.The first step, identification is the identification of possible sources of digital evidence and the evaluation of their relevance to the investigation. The investigators would have to find out the extent of investigation, legal authorizations that can be used such as search warrants and court orders, and categorize the kind of cybercrime under investigation.[11]Proper identification of the sources of the evidence be it in local devices, on network servers, or cloud servers, or in the mobile devices is the first step towards the integrity of the entire investigation, and it is arguably the most legally significant step.The second stage, preservation is the second most legally significant stage. It asks investigators to isolate, preserve and guard recognized evidence against any manipulation, corruption or demolition. According to the Association of Chief Police Officers (ACPO) guidelines, which are commonly known as a standard in handling digital evidence, no operation executed by law enforcement agencies and its practitioners should modify data in digital devices that can be later referred to in a court of law.[12]Normal preservation measures include physical removal of storage devices, write blockers and making of forensic images.

The third phase, which is also referred to as collection, is the systematic retrieval of data in the identified sources. Strict procedures should be followed in this process in order to make the evidence obtained in a manner that is legally defensible. The optimal acquisition method is to use forensic imaging to produce a bit-to-bit copy of the original storage media since it does not alter the original evidence in any way but instead gives it a working copy to analyze.[13]The process of acquisition has to be effectively documented with records of hardware and software specifications, time stamps, and the name of personnel engaged.The fourth step is analysis and examination which entails the procedures of forensic analysis to obtain useful information out of acquired data. The techniques used by investigators are the use of keywords, analysis of file signature, reconstruction of the timeline, steganography and metadata analysis.[14]The fifth and last stage, which is reporting and presentation, dictates that the investigator summarizes the findings and prepare a comprehensive report that is easily understandable by the legal experts and the officials of the courts. The report should record the procedures used, evidence retrieved, chain of custody and the conclusions made in a manner that can be subject to judicial examination.[15]

4.3 Chain of Custody: The Linchpin of Forensic Integrity

Chain of custody is the foundation of integrity of evidence in forensics. It can be defined as the chronological record of the seizure, custody, control, transfer, analysis and disposition of evidence and provides a continuous line of evidence between the place of occurrence and the courtroom.[16]Any failure in the continuity of custody presents a possibility of the allegation of tampering with the evidence that otherwise can be useful in the courts. In the digital environment, chain of custody has its own peculiarities since the digital evidence can be copied, transmitted, and stored in different jurisdictions and devices at the same time, this is why UNODC highlighted that forensic investigators are continuously being faced with the question of what constitutes the accuracy, authenticity, completeness, and convincing evidence (AACC) in the kind of situations when mutual legal assistance is requested among jurisdictions and devices.[17]The ILAC has also observed that there are no clear

[9]TechTarget, *Computer Forensics Definition*; Norwich University, *5 Steps for Conducting Computer Forensics Investigations*.
[10]NIST Special Publication 800-101, *Guidelines on Mobile Device Forensics* (2014); NIST, *Network Forensics*.
[11]Norwich University, *5 Steps for Conducting Computer Forensics Investigations*.
[12]Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence* (2012).
[13]NIST Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response* (2006), Section 4.
[14]-Council, *Computer Hacking Forensic Investigator (CHFI) Program Framework*.
[15]Ieong, R.S.C., "FORZA – Digital Forensics Investigation Framework that Incorporate Legal Issues," (2006) 3(1) *Digital Investigation* 29-36.
[16]NIST Special Publication 800-86, Section 3.1 on Chain of Custody procedures.
[17]United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013).

guidelines and standardized procedures between crime scene investigation and forensic laboratory analysis, which is a major deterrent to admissibility of evidence, suggesting compliance to ISO/IEC 17020 and 17025 standards of accreditation.[18]

V. LEGAL FRAMEWORK FOR ADMISSIBILITY OF DIGITAL EVIDENCE

5.1 Indian Legal Framework

5.1.1 The Information Technology Act, 2000 and the Indian Evidence Act, 1872

The Information Technology Act, 2000 (hereinafter "IT Act") is the legislative basis of the Indian reaction to the issue of electronic transactions and cybercrime. Section 2(1)(t) of the IT Act refers to electronic record as the data, record or data created, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche."[19]IT Act amendment contained provisions of the Indian Evidence Act, 1872 with the introduction of Sections 65A and 65B providing a specific legal framework on admissibility of electronic evidence.[20]The Indian Evidence Act contained in section 65B(1) stated that any information in an electronic record that has been printed, stored, recorded or copied as a computer output shall be treated as a document and admissible as evidence without additional evidence or production of the original and subject to the conditions in the section.[21]Section 65B(4) required the certification of a certificate which identified the electronic record, gave an account of how it was produced and gave details of the equipment used by the recipient, and was issued by an individual in a responsible official capacity.[22]

5.1.2 Judicial Evolution of Section 65B Standards

The Supreme Court of India has used a lot of judicial debate to explain and narrow down the criteria to be followed in admissibility of electronic evidence. In State (NCT of Delhi) v. The Court first decided that electronic evidence was admissible as secondary evidence pursuant to Sections 63 and 65 of the Evidence Act, regardless of whether Section 65B(4) had been complied with (Navjot Sandhu 2005) 11 SCC 600.[23]This stance was significantly reformulated in the landmark case of Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 when a three-judge Court stated that Sections 65A and 65B represent a complete code of admissibility of electronic evidence, and that the certificate described in 65B(4) is obligatory to secondary electronic evidence.[24]The Court made it clear that the general provisions of Section 63 and 65 are subordinate to the non-obstante clause that is contained in Section 65B and that electronic evidence given in the form of secondary evidence can and must not be admitted unless the stipulations of Section 65B are realized.[25]Later rulings created confusion in the doctrines. In Tomaso Bruno v. A three-judge bench in State of Uttar Pradesh (2015) 7 SCC 178 seemed to reiterate the NavjotSandhus stance without citing *Anvar*.[26]Likewise, in Shafhi Mohammad v. The Court proposed an exception to requirements of Section 65B(4) in case when the accused could not produce the certificate (State of Himachal Pradesh (2018) 2 SCC 801).[27]This was finally decided in Arjun PanditraoKhotkar v. In 7 SCC 1 (2020), in which the Supreme Court expressly reaffirmed the Anvar case, electronic evidence admissibility as secondary evidence to the effect of secondary evidence by the use of a Section 65B(4) certificate is obligatory and a condition precedent.[28]The Court ruled Tomaso Bruno to be per incuriam and explained that Shafhi Mohammad was incorrectly interpreted. More to the point, according to the Court, no compliance with Section 65B(4) is necessary when the original electronic record is created by the owner of the device who gets into the witness box.[29]

5.1.3 The Bharatiya Sakshya Adhiniyam, 2023: A New Paradigm

The BharatiyaSakshyaAdhiniyam, 2023 (BSA)[3], which came into effect on December 25, 2023 and which replaces the Indian Evidence Act, 1872, is a major modernisation of the evidentiary system in India.[30]Illustration (vi) of the BSA specifically acknowledges electronic records such as emails and server logs,

[18]International Laboratory Accreditation Cooperation (ILAC), *ILAC-G19:08/2014, Modules in a Forensic Science Process*, consistent with ISO/IEC 17020 and 17025.
[19]Information Technology Act, 2000, Section 2(1)(t).
[20]Information Technology Act, 2000, Section 92, read with the Second Schedule.
[21]Indian Evidence Act, 1872, Section 65B(1), as inserted by the Information Technology Act, 2000.
[22]Indian Evidence Act, 1872, Section 65B(4).
[23]*(NCT of Delhi) v. Navjot Sandhu alias Afsan Guru* (2005) 11 SCC 600.
[24]*Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473, para 24.
[25]*Ibid.*, para 14.
[26]*Tomaso Bruno v. State of Uttar Pradesh* (2015) 7 SCC 178.
[27]*Shafhi Mohammad v. State of Himachal Pradesh* (2018) 2 SCC 801.
[28]*Arjun PanditraoKhotkar v. KailashKishanraoGorantyal* (2020) 7 SCC 1, para 50.
[29]*Ibid.*, para 72 (per Nariman, J., concurring).
[30]BharatiyaSakshyaAdhiniyam, 2023 (Act No. 47 of 2023), enacted December 25, 2023, effective July 1, 2024.

documents on computers, laptops or smartphones, messages, websites and voicemail messages stored on digital devices as documents."[31]The BSA contains in Section 61 the statement that nothing in the Adhiniyam shall cause an electronic or digital record to be inadmissible on the basis that it is an electronic record, which has created a principle of technological neutrality.[32]Section 62 specifies that the information in electronic records will be evidenced pursuant to the next Section 63, which is very similar to the previous Section 65B but includes significant improvements.[33]Another major improvement made under the BSA is that the Schedule of the Act also required the certifying expert to specify the hash of the electronic or digital record and the algorithm by which the same can be obtained.[34]The hash Number of data content that is generated using hash algorithms like SHA-256, the hash that was recommended by NIST give a mathematical assurance of content integrity, and hence any further modification is unambiguously known.[35]This standard is however a significant improvement on the evidentiary system since it is based on modern forensic practice in the statutory law as it assumes that expert validation increases the probative value of knowledge; which fails because of the lack of Indian Forensic Science Laboratories."[36]The real-world issues of providing the qualified experts throughout the nation are still a serious obstacle to the successful execution of the BSA digital evidence requirements.

5.2 International and Comparative Legal Frameworks

5.2.1 The Budapest Convention on Cybercrime, 2001

The first and most general international convention about cyber investigation and digital evidence is the Council of Europe Convention on Cybercrime which was opened to signature in Budapest, November 23, 2001 and came into force on July 1, 2004.[37]By 2025, there are eighty one states which have ratified the Convention.[38]The Budapest Convention provides unified standards regarding substantive criminal law clauses (Articles 2-13), investigative and evidence collection procedural authorities (Articles 14-21) and the international cooperation schemes (Articles 23-35).[39]Articles 16 and 17 deal with expedited preservation of stored computer data and traffic data and acknowledges the volatility of the digital evidence and the necessity to exercise speed in ensuring that the evidence is not destroyed.[40]Article 19 allows searching and seizing of stored computer information, Parties must come up with legislative provisions that give competent authorities powers to access the computer systems and information stored in those systems.[41]The Second Additional Protocol to the Convention (2022) also increases the cooperation mechanisms on the disclosure of electronic evidence, covering the issues of cloud computing and cross-border data storage.[42]

5.2.2 The United States Framework

The admissibility of the digital evidence in the US is regulated by the Federal Rules of Evidence, especially, the Rules 901 and 902 about authentication and the Rule 702 about expert testimony.[43]The admissibility of expert scientific evidence standard has since replaced the Frye test- which included a general acceptance in the applicable scientific community [44]—to the more accommodating Daubert criterion in Daubert v. and Merrell Dow Pharmaceuticals (1993) 509 U.S. 579 that imposes on the trial judge a gate keeping role to determine the relevance and reliability of scientific evidence.[45]Daubert standard was later applied to technical and specialized knowledge in Kumho Tire Co. v. Carmichael (1999) 526 U.S. 137.[46]

---

[31]BharatiyaSakshyaAdhiniyam, 2023, Section 2(d), Illustration (vi).
[32]BharatiyaSakshyaAdhiniyam, 2023, Section 61.
[33]BharatiyaSakshyaAdhiniyam, 2023, Sections 62 and 63.

[34]BharatiyaSakshyaAdhiniyam, 2023, Schedule (Certificate for electronic or digital record).
[35]NIST, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-4 (2015), recommending SHA-256 as a standard algorithm.
[36]Vidhi Centre for Legal Policy, "The Evolving Enigma" (July 8, 2025), available at vidhilegalpolicy.in.
[37]Convention on Cybercrime, ETS No. 185, preamble and Articles 1-48.
[38]Council of Europe, Treaty Office, Status of Ratifications as of 2025.
[39]Convention on Cybercrime, Articles 2-13 (substantive law), Articles 14-21 (procedural law), Articles 23-35 (international cooperation).
[40]Convention on Cybercrime, Articles 16 and 17.
[41]Convention on Cybercrime, Article 19.
[42]Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, CETS No. 224, opened for signature May 12, 2022.
[43]Federal Rules of Evidence (United States), Rules 901, 902, and 702.
[44]*Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).
[45]*Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
[46]*Kumho Tire Co., Ltd. v. Carmichael*, 526 U.S. 137 (1999).

5.2.3 The United Kingdom Framework

The United Kingdom whose civil evidence act, 1968 initially had power in influencing the drafting of Section 65B in India has subsequently streamlined its procedure to electronic evidence.[47]The computer-generated evidence is now treated just like any other evidence by English law concerning its admissibility or weight to be given to such evidence, a stance that the Supreme Court of India approves in Arjun PanditraoKhotkar.[48]

VI. RESULTS AND DISCUSSION

6.1 Persistent Challenges in Cyber Investigation

Through the analysis, it is observed that there are a number of critical challenges that have continued to hinder the successful integration of the cyber investigation processes and the legal admissibility requirements.First, the problem of jurisdictional complexity is fundamental to the obstructions to the digital evidence collection. The digital evidence may often pass through more than one jurisdictional country, and the information may be stored in servers situated in countries other than the place of the crime and the place of adjudication. Although the framework of the international cooperation is established by the Budapest Convention, its efficiency can be reduced by the fact that several of the most important countries such as India, China and Russia are not the participants of the Convention.[49]Second, there is the deficit of expertise that is also a major practical issue. The UNODC has reported a shortage of trained digital forensic investigators in law enforcement agencies around the world to the extent that it is severe, making it difficult to maintain the integrity of the evidence at the initial phases of investigation.[50]Inadequacy of Forensic Science Lab by both personnel and infrastructural means in India has a direct impact on quality and promptness of forensics examination and certification.[51]Third, digital evidence is volatile and has high volumes, making preservation and analysis a challenge never encountered before. Ephemerality of messages through cloud-based data and encrypted communication means, requires investigators to implement more advanced tools and techniques, usually under extreme time constraints, to stop the destruction of evidence.[52]Fourth, a legal and ethical issue that is still a persistent challenge is the tension between the right to privacy and an investigative necessity. The constitutional right to privacy, which is considered as the basic right in terms of Article 21 of the Constitution of India through the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1,[53]should be weighed against the justifiable interests of the law enforcement in accessing and obtaining digital evidence, requiring the more proportionate and legally authorized investigative authorities.

6.2 The Admissibility Conundrum

This development in jurisprudence on the admissibility of digital evidence shows a basic conflict between the requirement of rigorous procedural protections to guarantee evidence integrity and reality of compliance. The certificate requirement in Section 65B(4) of the Indian Evidence Act (since replaced by Section 63 of the BSA) is a particularly important gatekeeping tool, but has been rigidly applied in some cases to exclude otherwise reliable and probative evidence on the basis of the technicalities of the procedure.[54]The Supreme Court in Arjun PanditraoKhotkar took care of this issue by establishing a viable exception: when one of the parties has exercised all reasonable efforts to obtain the necessary certificate but has been foiled by the deliberate failure of the issuer of the certificate, the compulsory condition can be waived.[55]This is a pragmatic realization that the ultimate goal of the evidentiary rules is the determination of the truth rather than the implementation of procedural formalities.The shift of the Indian Evidence Act to the BSA brings in further complications. Section 170 of the BSA specifies that pending proceedings shall remain under the old Indian Evidence Act which establishes a phase of transition whereby two parallel systems of evidence will run concurrently.[56]This duality brings questions on whether the digital evidence may be unequally treated by the courts in accordance with the courts, depending on when proceedings in the matter were instituted.

[47]Civil Evidence Act, 1968 (United Kingdom), Section 5 (since repealed by the Civil Evidence Act, 1995).
[48]*Arjun PanditraoKhotkar v. KailashKishanraoGorantyal* (2020) 7 SCC 1, para 72 (per Nariman, J.).

[49]Council of Europe, Treaty Office, List of Signatories and Ratifications to ETS No. 185.
[50]UNODC, *Comprehensive Study on Cybercrime* (2013), Chapter 7.
[51]Bharati, R.K. and Nagarale, S., "Digital Forensic Science and Evidentiary Standards in the BharatiyaSakshyaAdhiniyam (BSA) 2023: A Legal Examination of Admissibility," (2024) SSRN 5382703.
[52]Carrier, B. and Spafford, E.H., "Getting Physical with the Digital Investigation Process," (2003) 2(2) *International Journal of Digital Evidence* 1-20.
[53]*Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
[54]*Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473.
[55]*Arjun PanditraoKhotkar v. KailashKishanraoGorantyal* (2020) 7 SCC 1, para 62.
[56]BharatiyaSakshyaAdhiniyam, 2023, Section 170 (Repeal and Savings).

6.3 Towards a Harmonized Framework

The discussion shows an absolute necessity of a unified framework that will be able to involve the forensic best practices with the standards of legal admissibility. These are the aspects that such a framework should take care of: standardized forensic practices consistent with the ISO/IEC 17025 standards of accreditation; mandatory training and certification of digital forensic investigators; the creation of special cyber courts or benches where digital evidence can be assessed by individuals with technical expertise; and mutual legal assistance mechanisms that aid the expedient cross-border gathering and preservation of digital evidence.[57]

VII. CONCLUSION

The critical examination of the processes of cyber investigation and the admissibility of digital evidence shows that it is a field of study where there is a rapid change in technology and the pace of legal adjustment is forced to be rather slow. The paper has shown that even though the digital forensic investigation has evolved into a formal, scientific research-based study, which advances in a recognisable sequence of identification, preservation, acquisition, analysis, and reporting, its success as a justice delivery tool still depends on the ability of the legal system to receive, consider and give due weight to digital evidence. To the wholesale modernization of the BharatiyaSakshyaAdhiniyam, 2023. It is admirable that the BSA introduced the hash value verification and explicitly recognized the various types of the digital records. But the practical effectiveness of these provisions is still subject to the presence of available trained forensic scientists and sufficiently equipped laboratories and a judiciary that are familiar with the technical side of digital evidence.

Internationally, the Budapest Convention is an excellent example of procedural standards and cross-border cooperation that have a harmonized framework, but its scope is restricted due to the lack of global ratification. The study suggests that India is responsive in seeking to explore the accession to the Budapest Convention or bilateral and multilateral agreement that helps to establish effective cooperation in cyber investigations. The final criterion should involve authenticity, accuracy, completeness, and persuasiveness as defined by the AACC model by UNODC that necessitates a comprehensive evaluation which is based on a forensic approach, compliance with the law, and judicial review. The credibility of the justice system in the digital era lies in the ability to make sure that the digital evidencethe silent witness of the cyber realmothersays the truth, is heard correctly, and is judged impartially.

[57]ILAC-G19:08/2014; ISO/IEC 17025:2017, *General Requirements for the Competence of Testing and Calibration Laboratories*.