A Critical Analysis on Challenges of Admissibility and Reliability of Digital Evidence in Legal Proceedings

Dr. N. D. Gowda[1], Pradeep. K. N[2]
[1]*Assistant Professor, Saraswathi Law College, Chitradurga, Karnataka, India*
[2]*Assistant Professor, R.L. Law College, Davanagere, Karnataka, India*

Abstract*—In today's world, Digital Evidence is a very helpful tool in criminal investigations and legal cases. Valuable Information about crimes and the behavior of suspects can be found in digital information from smartphones, computers, cloud storage and social media. However, legal professionals face many challenges when dealing with Digital Evidence, such as making sure it can be used in court, that it is real and that it has not been changed. The recognition of Digital Evidence in Indian judicial proceedings faces numerous hurdles, including the possibility of manipulation, difficulties in preserving the chain of custody and the absence of a standardized procedure for verifying the reliability of the information saved in electronic records. Despite these obstacles, the judiciary acknowledges the necessity of Digital Evidence in preventing cybercrime and has taken steps to update the legal infrastructure to make better use of Digital Evidence. The admissibility of Digital Evidence is subject to legal and technical complexities. Ensuring its authenticity, reliability and integrity is essential for admissibility. Collecting, preserving and analyzing Digital Evidence requires rigorous protocols and expertise. This Article discusses a comprehensive understanding of the current state of admissibility standards and challenges associated with Digital Evidence in legal proceedings.

***Index Terms*—Digital Evidence, Legal Proceedings, Admissibility, Reliability, Technology.**

I. INTRODUCTION

The 21st Century has brought with it thrilling metamorphoses and developments in technology in the world and India is no exception to this change. Digital Evidence refers to any information stored or transmitted in digital form, including data from computers, smartphones, emails, social media and sound storage. While Digital Evidence plays a crucial role in modern investigations, its admissibility in court poses significant legal challenges, primarily around its authenticity, chain of custody and relevance. The admissibility of Digital Evidence is a pivotal concern in modern legal proceedings, given the widespread integration of technology in various aspects of life. One major issue has been the legitimacy and reliability of Digital Evidence, which remains a subject of intense debate. Unlike traditional evidence, Digital Evidence requires specialized training and knowledge in cyberspace for proper investigation and evaluation[1]. The process of presenting such evidence in court necessitates specific protocols to ensure its authenticity and reliability.

The amendments to the Evidence Act and the IT Act have significantly advanced the use of electronic records in court proceedings. While judicial precedents emphasize the importance of certification, ambiguity remains about certain requirements under Section 65B (now Section 63 BSA). Bharatiya Nyaya Sanhita 2023 has allowed Digital records to be accepted as evidence and stipulates that they must have the same legal weight, validity and enforceability as paper records. Courts must keep pace with evolving technologies, fostering trust in electronic records while addressing functional challenges. Clear guidelines and regular updates will ensure that Digital Evidence maintains its integrity and reliability in the judicial system. Courts must assess the correctness, validity and dependability of Digital Evidence in each case[2]. To ensure the integrity of records, courts must prioritize safeguarding against unauthorized use,

[1] Harsh Mahaseth, When can Electronic Evidence be Admitted in a Court of Law? , Commonwealth Law Review Journal: Vol. 8 (2022)

[2] https://www.lawinsider.com/dictionary/electronic-evidence (Last Visited on December 19, 2025}

alteration or corruption of electronic data during its creation and use in legal proceedings. Over time, Indian courts have recognized alternative technologies and established precedents for the admissibility of Digital Evidence.

The most significant challenge in the legal context concerning Digital Evidence is ensuring its admissibility in court. Digital Evidence faces unique challenges compared to traditional forms of evidence, such as physical documents or witnesses. Issues related to authenticity, tampering, preservation and privacy concerns make it difficult for courts to accept Digital Evidence without careful scrutiny. The Indian legal framework, particularly the Bharatiya Nyaya Sanhita 2023 and the Information Technology Act, 2000, provide some guidelines but also face significant challenges in addressing these issues effectively[3]. As the use of Digital platforms has exploded, so too has the role of Digital Evidence in both criminal and civil cases. For example, in cybercrime cases, Digital Evidence is often the core piece of evidence that links the defendant to a crime, while in family law, Digital records such as text messages or social media interactions can be vital to resolving disputes. The widespread adoption of the internet and mobile technology has made Digital Evidence a cornerstone of modern legal practice in India.

II. ADMISSIBILITY AND RELIABILITY OF DIGITAL EVIDENCE IN INDIAN COURTS

Digital Evidence has been instrumental in various high-profile cases in India. In cybercrimes, fraud cases and even terrorism related cases, Digital Evidence can play a pivotal role in establishing guilt or innocence. Courts increasingly rely on Digital records, such as emails, call logs and chat histories, to establish a chain of events. However, due to the complex nature of Digital Evidence and its vulnerability to tampering, it requires rigorous procedures for authentication and handling[4]. A recent attempt is made through enacting Bhartaiya Sakshya Adhiniyam, 2023 to exhaustively provide for technological advancements as a means of evidence having admissibility and relevancy in the Courts of Criminal Justice in India. However, still concerns with respect to lack of proper safeguards, Digital ignorance and likelihood of privacy breaches were raised.

The BSA first brought changes to the Definition of 'Document' under Section 2(d) of the Act, including Digital records and electronic records as a part of document. This section further encapsulates the illustrations defining what electronic records are. Furthermore, Section 61 of the BSA provides that both kind of evidence, Electronic or Digital Evidence and Documentary Evidence shall be treated equally with respect to their legal effect, validity, and enforceability. The Information Technology Act, 2000, was enacted to deal with issues arising from the use of computers and Digital platforms. The Act governs issues related to electronic records, Digital signatures and cyber security and serves as the foundational law governing Digital transactions and communications in India.

2.1 In Indian Courts, Digital Evidence must satisfy certain technical requirements to be considered legally admissible:

2.1.1. Relevancy:
The Digital Evidence must be directly connected to the facts of the case at hand.

2.1.2. Authenticity:
It must be established that the Digital Evidence is genuine and has not been tampered with.

2.1.3. Reliability:
The source of the Digital Evidence must be trust worthy and appropriate procedures must have been followed during its acquisition and preservation.

2.1.4. Integrity:
The Digital Evidence must be protected from any unauthorized modifications or corruption throughout the process.

2.2 To meet legal requirements for Digital Evidence in court:

[3] Thomson, Lucy L. "Mobile devices: New challenges for admissibility of electronic evidence." SciTech Lawyer 9.3 (2013): 32.

[4] International Journal of Innovative Research In Technology, Volume 12, Issue 2 July 2025, P.3050.

2.2.1. Chain of Custody:
Keep a record of who handled the evidence from when it was seized to when it was presented in court.

2.2.2 Certificate:
Get a certificate signed by a qualified person saying the evidence is real and hasn't been changed.

2.2.3. Expertise:
Make sure qualified people handle collecting, storing and presenting the evidence.

2.2.4. Documentation:
Write down in detail how the evidence was collected, stored and presented.

III. LEGAL ASPECTS AND ADMISSIBILITY OF DIGITAL EVIDENCE

The legality of Digital Evidence depends on certain technical and legal requirements. In many countries, gathering and analysing Digital Evidence must follow legal procedures like search warrants or court orders. If these procedures are not followed, accept the evidence may not in court. They must make sure that the collection and examination of Digital Evidence do not violate anyone's right to privacy. Before admitting Digital Evidence, the court must determine its relevance, truthfulness and authenticity. Additionally, the evidence must satisfy three key legal requirements, i.e., authenticity, reliability and integrity.

The advent of Digital technology has revolutionized every aspect of modern-day society, including the judicial landscape. Often, technological advancements lead to an imbalance of power in favour of the party with the most access to technology and the most adept use of it in legal proceedings. This imbalance of power has a severe impact on the fairness of legal proceedings[5]. For instance, those who have access to the most up to date technology are in an advantageous position to collect, analyse and present evidence more effectively and efficiently than those who do not, giving an unfair advantage in the courtroom. In addition, Digital advancements like Chat GPT have allowed for the introduction of automated systems that can analyse and interpret legal documents. These automated systems are often able to make decisions and render judgments more quickly than human lawyers and they can often do so with less bias. This has led to an increase in the number of cases being decided by automated systems, which can lead to more unfair outcomes.

Admissibility of evidence is a very crucial stage in any civil or criminal trial and substantially affects its outcome. Technological advancements keep on presenting new and unique challenges before the courts and judiciary by offering the various new forms of Digital Evidences. Another challenge that is faced in regards to Digital Evidence is the ease with which it can be forged, fabricated and manipulated and makes it all the more difficult to decide about the admissibility and veracity[6]. Legal principles, technological up gradation and ethical problems must all be carefully looked upon while deciding whether Digital Evidence is admissible or not. To maintain the equitable and efficient administration of justice in the Digital age, legal authorities must be cautious in their adaptation as Digital technologies continue to progress. Admissibility of Digital Evidence is majorly impacted by privacy and data protection affairs, especially when it is a matter of sensitive or personal data.

IV. BENEFITS OF DIGITAL EVIDENCE IN LEGAL PROCEEDINGS

The Digital Evidence plays an important role in establishing the facts in legal proceedings. Earlier it was stuck to physical evidence. As a result of rapidly growing technology, various transactions are carried out in Digital mode. Digital Evidence has many benefits some of the important merits are as follows:

4.1 Digital Evidence can be sourced from a variety of formats and devices. Devices like laptops, mobiles, hard disks, software and documents like PDF JPG,

[5] International Journal of Communication Networks and Information Security (IJCNIS), Vol.16, No.1 (Special Issue), (2024),p.1

[6] Richa Gupta, Prof. (Dr.) Puneet Bafna, Digital Evidence and it's Admissibility under the Indian Legal Regime, *16*(1 (Special Issue), 1436–1444. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/7142

image and audio formats like mp3, mp4 and many others. These formats and devices can easily be carried in legal proceedings. Thus, it will help to widen the scope of investigations.

4.2 Digital Evidence is stored or transmitted in binary form. In computing, it's the fundamental language of electronic devices. This system forms the basis for encoding and processing information inclined every text, image, audio and video. Digital Evidence is the binary nature of data that allows the accurate, reliable representation. This will add more value to the evidence before the court.

4.3 Digital Evidence can be more secure as it prescribes certain passwords and security reluctantly, there is less chance of violating private information with strong passwords.

4.4 The Digital data can be easily found, organized and shown in court. This evidence is like information on computers or phones and is helpful in court because it is easily found in different documents, easily copy pasted and executed in legal proceedings. The digital files not only contain the main information but also keep the record of when it was created, modified and viewed[7]. In cases where in legal proceedings any money matters are involved, Digital Evidence is very important. It serves as a document, showing how money moves around. This proof is helpful in situations of fraud or any financial wrongdoing.

4.5 Digital technologies such as encryption, digital signatures, block chain technology timestamps and logging technology help to maintain the originality and authenticity of the data. Thus, it will be considered as more reliable in court.

4.6 Digital technology will provide real time information. This will help lawyers and other legal experts to have access to the most recent and relevant information when dealing with on going cases in the court.

4.7 Instead of dealing with lots of paperwork, storing physical documents and handling everything manually, Digital Evidence allows, doing things more efficiently. This means with less printing, less physical storage space and less manual work. It makes the whole legal process more cost effective.

4.8 The Digital clues like metadata, timestamps and other Digital footprints help the experts to investigate more accurately. It provides structured information to get a better and complete picture of the case. This helps to understand the sequence of events and gather more information related to the case.

4.9 Extra details contained in the Digital Evidence help to verify facts. This might include information like geological data, device identification and user authentication details. These additional details make the evidence more reliable.

V. CHALLENGES IN HANDLING DIGITAL EVIDENCE IN INDIA

Though there are immense benefits of using Digital Evidence, there are many challenges associated in handling Digital Evidence in India. In India, Digital Evidence got prominence after the amendment made in the year 2000 to the Indian Evidence Act 1872. But, even today there are numerous complexities in managing Digital Evidence.

5.1. Legal framework

Initially, Digital Evidence did not bear any legal recognition before the court. However, amendment of the Indian Evidence Act in 2000 has given legal recognition to the Digital Evidence as admissible before the court. However, this Act does not consider electronic evidence as primary evidence, though it is admissible as evidence before the Court. The Digital Evidence is considered as the secondary evidence as per the Indian Evidence Act 1872.

The major issue is as secondary evidence it may affect its credibility in court. Primary evidence is considered as more reliable and has more evidentiary value compared to secondary evidence. Moreover, treating

[7] Sharma, A., & Patel, R. (2023). Digital Evidence in Indian Courts: An Analysis of the BSA 2023. Indian Journal of Law and Technology, 15(2), P. 45-62

Digital Evidence as secondary evidence will place an extra burden on the person to establish their claims. Thus, parties need to overcome additional hurdles for establishing the authenticity of the digital records[8]. In order to combat these issues later some changes were made in the new Act called Bharatiya Sakshya Adhiniyam 2023. The Act has treated Digital Evidence as the primary evidence. The Act is lacking in sufficient safeguards to prevent tampering or contamination of electronic records during investigations. This will raise questions about the integrity of Digital Evidence in legal proceedings. The Act requires the need for an expert's certificate to authenticate specific electronic evidence. While this certification is indeed to ensure the accuracy of Digital Evidence, it may pose a challenge in terms of the ease of producing such evidence in court[9].

5.2. Data protection and privacy

Digital Evidence can have both positive and negative impacts. Digital Evidence is very important for the investigation of Cybercrimes. However, it can also cause threats to people's privacy rights. Such rights are protected under Article 21 of the Constitution that states that every individual has the right to life and liberty. The same contention was upheld in Justice *K.S Puttaswamy vs. Union of India* case[10]. For instance, Digital Evidence is like a detective tool that will be used in order to catch online criminals. It has the capacity to track and analyse activities on the internet. However, this can be misused to the rights of the individual. Because tracking their online movement without their permission is a clear way of violation of privacy.

5.3. Search, Seizure and Search Authority

The court will admit the Digital Evidence if the methods used to obtain Digital Evidence is in line with legal procedures. The challenge arises when Digital Evidence is obtained without proper authority. If the evidence is obtained without a valid search warrant is also one of the challenges. In such cases, where the procedural requirements stated in the BNSS are not met, the defence has the right to challenge the admissibility of such evidence. If there is a failure to follow the correct protocols like maintaining a properly documented record of evidence handling, it can lead to challenges regarding the reliability of the evidence.

5.4. Forensic Challenges

Digital Evidence often undergoes forensic examination in order to determine its authenticity. However, challenges can arise due to the rapidly growing technology. Out dated forensic tools present a challenge during the examination, potentially impacting the court's confidence in the accuracy of Digital Evidence. Digital forensics experts must stay updated to address these challenges and ensure that forensic procedures align with legal standards for the admissibility of evidence[11].

The Digital forensic challenges fall into three main categories that include:

Technical Challenges –

Means issues like anti-forensic techniques, cloud operations, skill gaps and stenography.

Legal Challenges –

Involve presenting digital evidence, lack of proper guidelines, and inadequate electronic evidence collection and acquisition.

Resource Challenges –

Include the power required for collecting digital evidence and analysing a running computer. In order to maintain the integrity and admissibility of digital evidence in legal proceedings, there is a need to overcome these challenges.

5.5. Technological Advancement

The evolving technology has posed many challenges for defining and controlling Digital technologies like artificial intelligence, block chain and other internet things. Because of this progress, courts have to get used to dealing with proof or information that comes

[8] Gupta, S. Challenges in Implementing the Bharatiya Sakshya Adhiniyam: A Critical Review. National Law School of India Review, 36(1), (2024). P.78-95.

[9] International Journal of Law and Information Technology, 31(3), P.301-318.

[10] (2017) 10 SCC 1

[11] Reddy, K., & Joshi, M. Forensic Challenges in Authenticating Digital Evidence: Technological and Legal Perspectives. Digital Investigation, (2024). P,38

from these very advanced technologies. It's like they need to learn and understand these new technologies to make fair decisions when such evidence is involved in legal cases.

VI. CONCLUSION

Digital Evidence is very important in today's investigation. Due to the rapid growth in technology, the scope of Digital Evidence is increasing. The Indian judiciary has given legal recognition to Digital Evidence by adopting Digital Evidence in many cases. After knowing the importance of Digital Evidence Parliament made necessary enactment with regard to Digital Evidence admissibility in Bharatiya Sakshya Adhinyam 2023. The Act considered Digital Evidence as primary evidence. On the other hand, Digital Evidence has its own set of challenges. It is important to keep this evidence safe and unchanged by including strong passwords and some digital security measures. Digital Evidence faces some challenges like software privacy, Cyber hacking, Cyber fraud and Cyber theft. To address these challenges legal systems, need to continually update legislation. The Government had to provide clear guidelines for securing and creating awareness regarding this evidence. Digital Evidence is getting legal recognition in different countries. When use of technology increases, the information stored on digital devices also increases. This may lead to the misuse of technology often tends to be crimes. Everyone involved in the legal system, such as lawyers, and judges, need to understand how to handle and use this Digital Evidence properly. Working together is needed to make sure that this kind of evidence is used correctly, by meeting the ethics of law and justice is served properly.

REFERENCES

[1] Sharma and R. Patel, “Digital evidence in Indian courts: An analysis of the BSA 2023,” *Indian Journal of Law and Technology*, vol. 15, no. 2, pp. 45–62, 2023.

[2] S. Gupta, “Challenges in implementing the Bharatiya Sakshya Adhiniyam: A critical review,” National Law School of India Review, vol. 36, no. 1, pp. 78–95, 2024.

[3] V. Mehta and A. Kumar, “Blockchain and AI in legal evidence: Implications of the BSA 2023,” International Journal of Law and Information Technology, vol. 31, no. 3, pp. 301–318, 2023.

[4] R. Singh, “Comparative analysis of digital evidence laws: India’s BSA 2023 and global perspectives,” Comparative Law Quarterly, vol. 73, no. 2, pp. 412–435, 2024.

[5] P. Nair, “Privacy concerns in the era of digital evidence: Balancing justice and individual rights under the BSA 2023,” Journal of Constitutional Law and Policy, vol. 8, no. 1, pp. 55–72, 2023.

[6] K. Reddy and M. Joshi, “Forensic challenges in authenticating digital evidence: Technological and legal perspectives,” Digital Investigation, vol. 38, p. 301026, 2024.

[7] OECD, “Digital evidence in legal proceedings: A comparative study of OECD countries,” OECD Digital Economy Papers, no. 324, 2024.

[8] S. Lal, “Blockchain technology and digital evidence authentication: Opportunities and challenges in light of the BSA 2023,” Journal of Blockchain Research, vol. 6, no. 2, pp. 78–95, 2024.

[9] Computer Law & Security Review, vol. 39, no. 4, p. 105706.

[10] N. Rao, “Constitutional implications of the BSA 2023: Due process and digital evidence,” Supreme Court Cases, vol. 12, no. 7, pp. 1–18, 2024.