NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

CYBERCRIME INVESTIGATIONS AND ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIA: ADDRESSING PARADIGM SHIFT WITH DIGITAL FORENSICS INTEGRATION

Akash Bag, Prof. (Dr.) Saurabh Chaturvedi

Abstract: *The increase in cybercrime and the role of electronic evidence have heavily influenced the way criminal investigations are conducted in India nowadays. It is essential to examine the shifts in policies and practices related to digital forensics, the acceptance of electronic evidence, and the investigation of cybercrime. When electronic evidence first emerged, the Information Technology Act, 2000, and the Indian Evidence Act, 1872 (IEA), were used to guide its use in courts. The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), introduced new changes that expanded the scope for handling electronic evidence. This paper, employing a qualitative legal and case study methodology, examines the rise of electronic evidence in courts and its legal implications. It examines how the BSA, 2023, compares to the provisions of the IEA, 1872. Digital forensics primarily assists in managing and verifying electronic evidence presented in such cases. Retaining control over the chain of custody and using proper tools for electronic evidence stabilises and secures the collected electronic evidence. However, the field faces challenges such as imbalanced infrastructure, stringent regulations, and a shortage of well-qualified forensic experts. It analyses current challenges in both cybercrime investigation and admissibility, and recommends reforms geared towards solving complex cases and permitting the use of electronic evidence in courtrooms. Because modern cybercrime is highly complex, the solution lies in strengthening the relationships between laws and forensic practices.*

Keywords: *Cybercrime Investigation, Electronic Evidence, Admissibility of Evidence, Bharatiya Sakshya Adhiniyam (BSA) 2023, Indian Evidence Act 1872, Information Technology Act 2000, Digital Forensics, Chain of Custody.*

I. INTRODUCTION

India is not exempt from the rising cybercrime, particularly in the area of financial fraud, which has caused significant losses to the country. The country is increasingly struggling against cybercrime, mainly due to administrative barriers and legal restrictions. Investigating cybercrime presents numerous challenges, including jurisdictional complexity, the anonymity of online identities, and extradition issues, as not all countries consider cybercrime a criminal offence. Indians are more susceptible to cybercrime, resulting in significant financial losses. The Central Government's Indian Cybercrime Coordination Centre (I4C) reported cybercrime damages of approximately Rs 11,300 crore in the first nine months of 2024. Bengaluru-based cybersecurity firm Cloudsek has analysed data from over 5,000 malicious website domains and abuse instances involving more than 16,000 brands, forecasting that Indians and Indian organisations may lose Rs 20,000 crore to cybercrimes in 2025. The dynamic nature of cybercrime and its diverse interpretations across various fields make it difficult to get a universal definition. With projections showing its worldwide cost will exceed $8 trillion by 2022 and $9.89 trillion by 2024, the World Economic Forum ranks cybercrime as the 12th most considerable global risk.

Figure 1- Cyber Crimes/Cases Registered and Persons Arrested under the IT Act during 2014 – 2024 (source: NCRB)

Globally, law enforcement agencies, including Interpol, the FBI, and the World Customs Organisation, are working together to tackle cybercrime by destroying systems that coordinate cyberattacks, therefore reflecting this trend. Usually described as illegal activities carried out using computer networks, electronic technologies, or networked devices, cybercrime investigations and admissibility become difficult due to their volatile nature. Among other things, these activities include identity theft, fraud, cyber espionage, and the distribution of malware, also known as viruses. Cybercriminals cause harm, disrupt services, and gain unauthorised access through system

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

flaws. Their reasons could be political, personal, or economic ones. The development of digital technology extends the field of cybercrime and poses significant challenges for law enforcement departments. Earlier, the Indian Evidence Act, 1872, the Information Technology Act, 2000, the Indian Penal Code, 1860, and the Code of Criminal Procedure, 1973, were used to form the primary statutory foundation in India for combating cybercrime. Still, these laws are insufficient to fully address the complexities of cybercrime, underscoring the need for more powerful tools, strategies, and approaches for investigation and admissibility. The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (hereinafter BSA) in India has significantly altered the rules, superseding the Evidence Act of 1872 (hereinafter IEA) to address the handling of electronic evidence.

The paradigm shift from IEA to BSA has yet to be tested in the complexities of cybercrime and its evolving nature. Handling, preserving, and analysing electronic evidence is rather crucial to ensure a solid "chain of custody." These challenges are typical; therefore, it is crucial to continually update the guidelines for electronic evidence to ensure they align with technological advancements and evolving cybercrime threats. Digital forensics is becoming increasingly crucial in criminal investigations, as it facilitates the collection of evidence for both prosecution and defence. The BSA insists on closely preserving, acquiring, and evaluating digital evidence in conformity with digital forensic standards. Officials find it more difficult to conduct investigations since law enforcement lacks the appropriate tools and direction, and since there are few specialised devices accessible for managing and storing electronic data. The updated BSA, along with various certifications and electronic evidence, is now acknowledged, which facilitates the use of evidence in courts and meets the high standards in digital forensics. With the help of qualitative legal and case analysis, this paper aims to answer one question: How does the Bharatiya Sakshya Adhiniyam, 2023 (BSA) impact the admissibility of electronic evidence in Indian cybercrime investigations, and what role does digital forensics play in enhancing the reliability and authenticity of such evidence?

II. REDEFINING ELECTRONIC EVIDENCE: FROM IEA TO BSA AND THE ROLE OF DIGITAL FORENSICS

Initially, the BSA could appear to be nothing more than a new arrangement of IEA elements. Upon closer examination of these regions, we observe significant changes. According to Section 2(1)(d) of the BSA, a "document" now encompasses "electronic and digital records," thereby broadening the scope of the law. This development is essential for handling the role of digital evidence in today's court system. Earlier, following Section 3 of the IEA, an electronic or digital record could not be considered a document because it did not fall under the definition. Today, since much information is maintained and shared online, the traditional use of "primary records" in courts under the IEA is often insufficient. Likewise, BSA adds electronic and digital records to the definition, now treated as documents. As a result, experts are given a greater standing in the process. The distinction between "primary and secondary documentary evidence" is another essential part of development. It is commonly believed that primary evidence has more importance than secondary evidence. According to Section 65-B of the IEA and Section 63(4)(c) of the BSA, electronic records must be authenticated under strict standards. It addresses the need for certificates under Section 65-B (4) of the IEA, a subject that has sparked controversy in various court cases.

Previously, Section 65-B of the IEA only covered "computer outputs." Section 63 of the BSA was updated to include "semiconductor memory" and "communication devices" to reflect the evolving and broad nature of the electronic evidence. BSA's expanded view provided investigators with the opportunity to utilise tools such as Cellebrite for mobile devices and Wireshark or NetFlow for network data, allowing them to collect, record, and validate evidence from various electronic sources. The BSA has altered the use of electronic evidence in courts compared to the IEA provisions. While the IEA helped make electronic evidence acceptable, the BSA adds more procedures to manage the new digital challenges. Section 65-A of the IEA permits judicial officers to accept electronic records without requiring additional proof. Additionally, if a certificate is provided showing that an authorised person produced the electronic record, the e-signature falls under

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Section 65-B and is valid. Admissibility was thoroughly examined in the case of Anvar P.V. vs. P.K. Basheer & Ors, 2014 (hereinafter Anvar P.V). The ruling helps courts decide which types of electronic evidence they can include. The BSA employs a broader definition when identifying what constitutes a "document." In the BSA, electronic and digital records are recognised with similar authority as traditional paper-based documents.

This move enables courts to consider electronic and digital records as evidence, thereby recognising the value of electronic evidence in the modern justice system. It also made the investigation process easier, as experts can utilise data carving tools like R-Studio or PhotoRec, which can recover permanently deleted files from various electronic devices, including hard drives, memory cards, and other storage devices. This was not easy to prove in court due to the IEA's narrower approach to the issue. IEA Section 65-B lays rigorous guidelines for verifying electronic and digital records. Furthermore, Section 65-B of the IEA required the electronic device's record to include a certificate from the person in charge of the device identifying it and providing its specific details. This helped verify and ensure the authenticity of the evidence. Now, under BSA, investigators can utilise cloud forensics tools like ElcomSoft Cloud Explorer, which enables them to retrieve, store, and analyse data from cloud services, a practice commonly employed by cybercriminals to store illicit data. As BSA has increased the involvement and role of expert opinion, experts can utilise tools such as Cellebrite UFED (used for mobile device forensics) or Oxygen Forensics Detective (used for mobile and cloud evidence) to testify and validate their statements in court regarding how the electronic evidence was collected.

The BSA enhanced this provision. Apart from the rules in Section 65-B, Section 63 of the BSA also specifies that an "expert certificate" is needed. The certificate consists of two main parts. The presenting party created Part A, while an expert created Part B. With this dual certification, evidence is more reliable and comes with increased accountability. BSA also points out that electronic records must be "tamper-proof" and kept free from changes as established by the chain of custody. You will need to use tools made for such tasks, such as X1 Social Discovery or Magnet AXIOM. They are designed to gather and study metadata that comes from social media and digital sources. They can store the hash value of electronic data, which helps detect if any alterations have been made to it. The BSA meets cybersecurity changes and trends through digital signatures and hash values, which help maintain the authenticity of electronic data. Under the BSA, the use of cryptographic hash functions, such as SHA-256 or MD5, is permitted. With these tools, you can trust the integrity of electronic evidence at any stage of the case, which is crucial for the investigation. Improvements to the BSA have made digital forensics more significant and needed. EnCase and FTK Imager are two tools that experts use to create forensic images of electronic devices. The chain of custody is maintained because the evidence is adequately protected and regularly checked. The growing number of cybercrimes in India made it important to ensure both legal reliability and technical integrity in software.

III. CYBERCRIME INVESTIGATIONS AND INTEGRATION OF DIGITAL FORENSICS

This section will discuss the process of investigating cybercrimes by statutory provisions and the integration of new-age digital forensics technology, which can enhance the process.

A. Who is authorised to investigate?

Section 78 of the Information Technology Act, 2000 (hereinafter IT Act) grants police personnel special powers to investigate cybercrimes. It states that investigations of cybercrimes have to be carried out by a police officer of the rank of Inspector or above, 'notwithstanding' the restrictions in the Code of Criminal Procedure, 1973 (now Bharatiya Nagarik Suraksha Sanhita, 2023 or BNSS). This clause clarifies that, under the Act, only a senior officer is permitted to investigate significant cybercrimes. The Karnataka High Court emphasised that while a police officer below the rank of Inspector may record an FIR for violations under Section 66E of the IT Act, the inquiry must be conducted by an officer of Inspector rank or higher. In the case of Neha Rafiq Chachadi vs. The State of Karnataka, 2023, the court confirmed the decision, emphasising that the offence under Section 66E is categorised as cognisable, meaning it relates to serious crimes requiring a prompt investigation. Chachad was accused of creating a phoney Instagram account and distributing offensive

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

content. Reversing any petitions challenging the registration process, the court confirmed the FIR's registration but directed that an Inspector investigate. The court noted that Cyber Police Stations have authority only for offences under the IT Act, therefore excluding their capacity to investigate crimes under other laws. This distinction ensures that specific police officers, skilled in handling technology and internet-related offences, oversee cybercrimes.

B. Procedure for search and arrest

Any investigation relies on the collection of material evidence, which is typically conducted through search and seizure processes. Regarding cybercrimes and computer-related offences, these procedures are significantly more technical than those linked with traditional crimes. A court-issued search warrant grants the police permission to search, thereby allowing them to potentially violate a citizen's right to privacy under certain conditions. Search warrants are Tools of great importance for carrying out search and seizure operations. Regarding cybercrime, investigative agencies must obtain a warrant to look over digital environments and seize electronic data. Section 96 of the BNSS, 2023 (Section 93 of the CrPC, 1973) authorises a judicial officer to issue a warrant upon reasonable grounds, thereby providing the legal basis for the issuance of search warrants in criminal proceedings in India. The officer could specify the area or set of papers to review. Furthermore, Section 80(1) of the Information Technology Act (IT Act) grants law enforcement officials the authority to examine buildings and access locations in cases involving computer-related offences. Notwithstanding the general provisions stated in the BNSS, 2023, this section specifies that any police officer ranking as Inspector or an officer authorised by the Central or State Government has the authority to enter public locations, conduct searches, and arrest persons without a warrant, given reasonable suspicion of an offence under the IT Act. Should a non-police authority arrest an individual? Section 80(2) of the IT Act mandates that the person who arrests the suspect must present the suspect to the officer-in-charge of a police station or a magistrate. Further challenges arise from the volume of data to be investigated in cybercrime investigations. Unlike traditional crimes, where evidence is generally more readily recognised, investigators looking at a computer system may find an overwhelming number of irrelevant files, making it cumbersome to separate the relevant from the extraneous at the search location. Computers can retain enormous amounts of data; however, recovering even a small portion of pertinent evidence can be pretty tricky given the technical nature of the data. This poses a significant obstacle for investigators, as they may accidentally come across incriminating material when reviewing irrelevant files, thereby complicating the search and seizure of digital evidence in cybercrime investigations.

C. Integration of Digital Forensics

There is no doubt that India needs to intensify its efforts in the digital forensics sector to combat the growing menace of cybercrime in the country. Before delving into the legal aspects, let us examine the process of a digital forensics investigation. Figure 2 illustrates the process typically followed in digital forensics investigations. Though the exact technique may vary depending on the nature of the case, a digital forensics investigation usually follows a set of defined phases. The admissibility of digital evidence in court depends on the integrity and scientific validity of the entire process being followed. Each of the four fundamental stages—preservation, acquisition, analysis, and reporting—which are crucial for ensuring the admissibility of evidence in court, has relevance.

Figure 2: The process of Digital Forensics

1. Preservation

The first part, preservation, involves protecting the identified digital evidence at the crime scene. This encompasses the recognition, recording, collection, and transportation of tangible electronic devices, thereby maintaining the integrity of the data within. Good preservation is crucial, as any flaw at this level could compromise the whole research. Mishandling of evidence could result in the court declaring it inadmissible, therefore compromising the research. During this phase, the forensic investigator supervises adherence to correct procedures. The first and basic stage of digital forensics, namely preservation, aligns with Section 61 of the BSA, which stipulates that electronic or digital records cannot be disallowed in admissibility per se because they are electronic. Section 105 of the BNSS, 2023, both reiterates and solidifies the procedural rigour of this stage by deciding that a legal

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

mandate exists under the BNSS to preserve the integrity of evidence during search and seizure activities. However, to maintain a legally sound chain of custody, it is necessary to document and forward the evidence to the relevant judicial authorities for their review and evaluation.

2. Acquisition

is extracted from the preserved digital devices during the second stage, acquisition. The goal is to retrieve possibly encrypted, erased, or difficult-to-locate data. Devising passwords, bypassing encryption, and recovering deleted files all depend on digital forensic technologies. The type of device under investigation determines the tools and techniques used at this step. For example, gathering data from mobile devices is usually more difficult than from the hard drive of a computer. Customised for the specific phone type, mobile forensics solutions designed for data extraction from smartphones must ensure effective data recovery. While acquisition is typically carried out in a controlled laboratory environment, on-site acquisition may be necessary occasionally to prevent data loss resulting from device failure or battery depletion. This stage is completed through Section 63 of the BSA, 2023, which stipulates a format and certification for electronic records. The division of the certificate into Part A (for parties presenting records) and Part B (for experts) ensures that the data is acquired in a technically robust and legally valid manner. The hope is that the dual-layer certificate will address concerns about tampering and provide a credible source of notice.

3. Analysis

The analysis phase begins after effective data collection has been completed. The gadget's raw data is carefully examined. This stage includes methodical data set analysis and organisation to identify relevant evidence connecting a suspect to a criminal activity. A majority of the data is Unstructured or proprietary data; hence, forensic investigators need specific techniques for its organisation and evaluation. At this point, human expertise is vital, as the investigator's awareness of the case background helps them distinguish between key pieces of data and irrelevant extra data. The developers need to put in a great deal of effort and rely on various resources. If the number of cases increases, forensic experts may struggle to handle all the responsibilities. Since gathering information requires specialised knowledge and careful analysis, forensic experts play a crucial role in the process. Due to BSA's emphasis on authentication, extracting and analysing large amounts of data can be done more effectively using digital signatures and hash values. Thanks to these systems, the evidence is guaranteed to be credible, which enables forensic experts to draw accurate conclusions. Section 176(3) of BNSS mandates the collection of forensic evidence for severe offences, further underscoring the need for digital forensic experts supported by robust legal provisions.

4. Reporting

The reporting stage is compiling the carried-out activities and the findings of the investigation into a comprehensive report. A thorough report relies on the careful recording of the entire process, including notes, pictures, and outputs from forensic tools. Modern digital forensic tools often include integrated reporting features that help investigators create consistent and accurate reports. These reports include data on the evidence, tangible records, and relevant findings from questions or additional investigations. Since it supports the validity of the digital evidence and strengthens the case against the defendant, the final report is crucial for the prosecutor's court presentation. Executing a competent and legally compliant digital forensics investigation depends on each of these stages. The integrity of the evidence is maintained through preservation, careful acquisition, thorough analysis, and final reporting, thereby enabling admissibility in a court of law. Failing to consider these phases could render the evidence vulnerable to legal review, thereby compromising the entire investigation. Table 2 outlines the entire process by which digital forensics can be integrated into the current legal system to address the growing threat of cybercrimes in India.

Digital Forensics Phase Description Relevant Legal Sections/ Framework under BSA, 2023/ BNSS 2023 Investigation Tools & Techniques Admissibility in the Courts

Preservation Collecting and protecting electronic evidence at the crime scene to maintain integrity

Primary concern: Integrity and Authenticity Section 61 BSA- Admissibility of electronic and digital records

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Section 105 BNSS- Integrity during search and seizure	Tools like write blockers, EnCase forensic imager, prevent write access (alteration and tampering) to drives during imaging (e.g. CRU, Wiebe tech and Tableau)
Maintaining the chain of custody and Physical evidence Handling	Evidence must be preserved to be "tamper-proof", and proper documentation must be established to establish a chain of custody
Acquisition	Extraction of data, including encrypted and permanently deleted files, from preserved devices can be performed on-site. Section 63 BSA: Dual Certification format with (Part A- by filer and Part B- by expert) Tools like Oxygen Forensics Detective (mobile/cloud forensics), R-Studio, Cellebrite URED, NetFlow (network forensics), Cloud Explorer (cloud forensics), PhotoRec (Data Carving), Certification will include hash values (MD5, SHA-256, SHA-1) to verify the integrity of the data. Dual certification ensures legal robustness.
Analysis	Examining raw data, filtering of relevant evidence and linkage with suspects Section 176(3) BNSS: Forensic evidence collection for serious offences
Section 39 BSA: relevance of opinions of experts Tools like magnet Axiom, Hash verification tools, social discovery (social media data mining and metadata analysis)	Opinion of expert validation required for certification (part b of dual certification rule under u/s 63 BSA Note: The Opinion of an expert can be ambiguous sometimes
Reporting	Compilation of a detailed report, documenting the process, evidence and findings Section 63 BSA: Certificate attached to the report; admissibility depends on thorough documentation Tools like Magnet AXIOM (integrated report generation, XI social media Discovery (Social media data collection and reporting), and Nuix (case management and report generation) The report must include values and a certificate from an expert.

Table 1: Digital Forensics Stages, Tools, and Admissibility under Indian Law (Source: Author's creation)

IV. THE JUDICIAL DECISIONS ON CYBER-CRIME INVESTIGATION

In Vijesh v. The State of Kerala, the court acted on a notification from the Examiners of Electronic Evidence and addressed electronic evidence under Section 79A of the Information Technology Act, 2000. The Court ruled that once a notification is received, individuals analysing electronic evidence are presumed competent, and no requirement for them to prove expert knowledge before the court. Nevertheless, experts may need to confirm their qualifications to the judge, depending on the judge's discretion. Since the evidence could be questioned, the court ensured that its integrity was maintained throughout the entire process of making copies. The court noted that in crimes involving mobile phones, law enforcement agencies are required to protect any data they find. The person must record the phone's condition, turn off the battery if the phone is powered on, and confirm that the device's data has not been remotely erased. The phone should be sealed and sent to an expert for inspection. The case revealed that the investigating officer failed to follow proper procedures, urging state police to ensure that law enforcement agencies receive clear instructions and the necessary training to handle electronic evidence in combating cybercrimes.

In the case of Abdul Rahaman Kunji v. State of West Bengal, considering the increase in electronic communication crimes, the court emphasised that having trained professionals in the cyber police is crucial. It noted that prompt results and convictions depend on the early involvement of capable digital forensics experts. The court suggested that the prosecution trace IP addresses from the emails to identify the devices precisely. This is a handy option when sending emails from cybercafés or public sites with access to LAN, Wi-Fi, or mobile networks. It is still possible to track the sender's location in these situations. The court noted a growing trend of installing CCTV cameras in areas connected to the internet. The cameras record footage that can be used to identify people who send messages from these restricted areas. The ruling suggested that authorities responsible for gathering evidence should utilise the latest available technology under the IEA.

In the case Dilipkumar Tulsidas Shah v. UOI, Tulsidas Shah filed a Public Interest Litigation

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

(PIL) in the Supreme Court. Based on Articles 14, 19 and 21 of the Constitution of India, according to the petition, the court should assist in framing laws, rules, and standards to enhance cybercrime investigations and address existing issues within the legal system. According to the PIL, there are numerous examples of mistreatment of citizens due to the system's lack of sufficient protections. Regarding cybercrime, as explained in the 2008 amendment to the Information Technology Act, 2000, he argued that using outdated methods is insufficient and that the judicial officers and staff should require training to deal with electronic evidence professionally. In the case of State of Punjab v. Amritsar Beverages Ltd., the case highlighted the challenges law enforcement faces in handling electronic evidence due to a lack of sufficient scientific knowledge to deal with sophisticated electronic evidence. The court held that the growth of the internet and other technology has resulted in unexpected difficulties in determining what is required by existing laws. Lawmakers were not able to foresee every change in society. Changes have been made to the Information Technology Act, 2000, regarding cybercrimes and their penalties; however, law enforcement still finds it challenging to utilise these provisions. The court emphasised that law enforcement agencies must acquire new skills because modern technology is causing increased difficulty in dealing with electronic evidence.

V. JUDICIAL INTERPRETATIONS OF ELECTRONIC EVIDENCE ADMISSIBILITY IN INDIA

Many have observed the new revisions to the IEA, as per the BSA, which have sparked debates on whether these laws still retain traces of colonisation or if they represent a fresh arrangement of already existing institutions. Still, no thorough study has been done on the BSA, which replaced the IEA. Legal and forensic professionals are examining shifts and improvements in the BSA, which helps forensic experts work more effectively. BSA defines "document" to include "electronic and digital records" as per Section 2(1)(d) of the BSA. Section 3 of the IEA defines a document as "any matter expressed or described upon any substance" when such matter is so expressed or described by way of "letters, figures or marks", which is a narrower interpretation. Establishing this idea as the fundamental principle helped prevent electronic and digital records from being considered in the courts. The BSA definition now includes digital records, including "computer outputs" and electronically recorded documentation. The IEA's shift in emphasis highlights the growing importance of digital evidence in court proceedings and the need for a robust digital forensics' investigation infrastructure.

A. Electronic evidence is secondary documentary evidence

According to the law of evidence, primary documentary evidence takes precedence over secondary documentary evidence. Essentially, Section 56 of the BSA (Section 61 of the IEA), in that primary documentary evidence can be used to demonstrate the validity of their contents. However, secondary documents can also be utilised for this purpose. Secondary evidence can only be introduced in specific situations as per Section 60 of the BSA (Section 65 of the IEA) and Section 58 of the BSA (Section 63 of the IEA). Under the IEA, electronic and digital records have a distinct standing from documents. However, in court, these can be used as documentary evidence. Section 3 of the IEA lists secondary documentary evidence. After weighing the significance of these data, the court will verify whether they can be admitted under Section 63(1) of the BSA (Section 65-B (1) of the IEA) and also ensure that the submitting party provides appropriate proof in support of the evidence. The BSA states that electronic and digital records may be considered "documents," the same as primary documentary evidence, provided they are duly proved. This legal fiction renders electronic and digital records equivalent to primary documentary evidence. Hence, once the criteria in Section 63 are satisfied, the requirement of the primary evidence, i.e., computer output, will be waived. It can be presented to courts, as the electronic and digital records are recognised as primary evidence. This shift has made digital evidence equivalent to traditional forms of evidence.

B. Divergent Paths to Admitting Electronic Evidence

As a result of Section 65-B(4)'s necessity for a certificate accompanying the electronic and digital record, doubts arose about how Sections 65-A and 65-B should be applied. Most of the debate centred around whether submitting such a certificate was compulsory or an optional step. The Supreme Court had to clarify whether these

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

two sections constitute special laws that differ from other general rules, based on secondary documentary evidence under Sections 63 and 65 of the IEA. The exclusivity of Sections 65-A and 65-B would render them the only rules applicable to the acceptance of secondary documentary evidence, making it unnecessary to rely on the general rules, Sections 63 and 65. However, if they were not exclusive, then it would still be possible to present secondary evidence under the general rules of IEA. In that case, parties may still provide secondary documentary evidence, as per the standard requirements of the IEA, when their specific submission falls short of those outlined in Sections 65-A and 65-B. In the landmark case State (NCT of Delhi) v. Navjot Sandhu, the Supreme Court ruled that secondary evidence must be admitted if it complies with the requirements outlined in Sections 65-A and 65-B. The court also stated that the absence of the required certificate would not bar the evidence from being admissible.

The court stated that the word "may" in Section 65-A affords sufficient autonomy to the parties to present electronic evidence under Sections 65-A and 65-B, or such evidence may be submitted to the court as per the general rules outlined in Sections 63 and 65. Such a method permitted the acceptance of electronic evidence without requiring a procedural electronic certificate. For almost a decade, courts had been admitting electronic evidence, as established by the Navjot Sandhu ruling, regardless of whether specific procedural conditions were met. This approach was reviewed because it conflicted with the primary objective of Sections 65-A and 65-B, which aimed to supersede the general rules stated in Sections 65 and 63. This decision was based on the principle "generalia specialibus non derogant," as clearly stated in the case of Anvar P.V. The Court stated that the two sections form a "complete code" and require the mandatory submission of the certificate along with electronic evidence. Failing to provide this particular certificate would render the evidence unacceptable. This ruling emphasises the importance of adhering to proper protocols for electronic evidence to ensure its admissibility in the courts.

VI. THE PRESENT SCENARIO AND CHANGES BROUGHT UNDER BSA, 2023

The Court reverted to the approach established in Shafhi Mohammad v. State of HP, returning to the approach in Navjot Sandhu. The court holds that the provisions under challenge cannot qualify as special laws. The Court emphasised its authority to relax procedural requirements in the pursuit of justice. The application of the certificate requirement for each document would be detrimental to the objectives outlined in the rules governing the admission of electronic evidence when seeking to admit evidence held by the opposing party. Certification becomes mandatory only when a party is responsible for the device used to generate or store digital information. The Court recognised that situations might exist where certificate submission is unnecessary because the electronic document is not under the party's control. In such circumstances, such information becomes secondary documentary evidence. However, the decision in the Shafhi Mohammad could not establish a clear precedent, as it was based on the authority of only a two-judge bench, whose findings were not finalised by a bench of three judges, as granted to the panel. In Anvar P.V., Justice Nariman constituted the bench that affirmed the Anvar P.V. position in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, deciding that all three judges agreed. The Court held that the Shafhi Mohammad opinion was misguided and thus ordered the legal validation of evidence. If a party does not obtain the electronic record, they have recourse to the trial court to enforce its production. The Court decided that the electronic evidence forms a "complete code," requiring the filing of certificates as a fundamental step in authorising their use. Under these requirements, electronic data is evaluated as primary documentary evidence rather than secondary evidence. However, the exact measures required may sometimes lead to the rejection of evidence, thereby enhancing reliability and authenticity by ensuring a complete and unbroken "chain of custody." As a result, there is a danger that delays and extra expenses caused by this degree of formality could jeopardise the availability of justice for many citizens.

The BSA only introduces minor amendments to the legislation on electronic evidence. The legislation aligns with established principles in

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

the law of electronic evidence. As a result, the new provisions and the redefined term "document," which explicitly covers electronic and digital records, have considerable implications. Focusing on the three changes, firstly, the principles of electronic evidence law have been reinforced, specifically in Section 65-B (1), which outlines the conditions that permit electronic evidence to be admitted as primary documentary evidence. It is aligned with the provisions of Sections 62 and 65 of the IEA. Secondly, Section 65-B in the Indian Evidence Act formalises the procedural requirements for the admissibility of electronic evidence. The Supreme Court, recognising the integral role of electronic evidence in the legal framework, has mandated that certificates accompany this form of evidence under Section 65-B (4) of the IEA. Thirdly, the rules regarding the relevance of facts of electronic evidence have evolved. Section 20 of the BSA now consolidates the criteria set out in Sections 22-A and 61 of the IEA to determine the factual validity of electronic and digital records. These amendments harmonise the regulations around the admissibility of electronic evidence in specific situations.

Modern law of evidence places the most significant emphasis on the criteria for accepting electronic evidence. Explicit rules enable electronic evidence, which has traditionally been classified as secondary documentary evidence, to attain the status of primary documentary evidence under specific conditions. Once the specified conditions are fulfilled, electronic evidence is officially viewed as a "document," equivalent to primary documentary evidence such as computer output or the devices used to create it. Section 61 of the BSA, newly inserted along with Sections 62 and 63 (65-A and 65-B of the IEA), establishes a pathway for recognising the same 'probative value' for electronic evidence as that of primary evidence. Explanations 4–6 are appended to Section 57 of the BSA (Section 62 of the IEA), introducing potential conflicts. This conflict can be resolved by 'harmonious interpretation' of the preconditions of admissibility, excluding the preconditions outlined in the explanation of Section 57 from the scope of Section 63 of the BSA. The methodological shift outlined above aligns with the provisions that govern qualification processes and maintains the precise objectives outlined in Section 57. However, ambiguities arise due to the uncertainty surrounding the interpretation of the term "proper custody" as explained in Explanation 5. A clear understanding of the term is lacking within the parameters of Section 57, which can lead to doubt when applying it. At the same time, basing the evaluation of electronic evidence on the appropriateness of its custody contradicts the fundamental concept in electronic evidence laws, which focuses on confirming the validity of the evidence without verifying the authenticity of the person presenting it. The IEA provisions under Section 65-B (2) reflect the central principle underlying the admissibility of electronic evidence.

The procedural requirements for electronic evidence align with fundamental legal principles. The Supreme Court concluded that a certificate must precede any electronic evidence. This decision enhances the validity and reliability of the procedure for verifying electronic evidence. The BSA now requires a certificate of authenticity to be signed by both the person in charge of the device and the expert. The development is consistent with the central legal principle established in the case of Arjun Panditrao Khotkar and upholds the credibility and admissibility of electronic evidence. Section 39(1) of the BSA introduces new flexibility by aligning with the language of Section 45 of the IEA regarding expert testimony by inserting the residuary phrase "any other field." Expertise from any field may now be legally considered. The revision of the BSA is in contrast with Section 45 in the IEA, which now allows expertise from virtually any field to be admissible, given the rapid evolution of multiple disciplines. Electronic evidence is considered secondary documentary evidence and thus has limited value regarding the contents of an electronic record. Section 22-A of the IEA has been rendered obsolete now that the BSA recognises electronic and digital records as falling within the scope of "documents." As indicated by Section 22-A of the IEA, oral admission about the contents of a document typically has no value unless the record's authenticity is challenged. Section 22 of the IEA provides two alternative conditions under which oral admissions concerning the contents of a document may be considered relevant. Firstly, the party presenting the oral admission is permitted to provide secondary evidence of the content or secondly, when the authenticity of the document is in question. Section 20 of the BSA (Section 22 of the IEA), but the redefined term "document" has rendered Section 22-A of the IEA obsolete. The new definition encompasses both traditional and new forms of documents under the same

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

counterpart conditions for accepting oral disclosures.

The expanded scope of secondary evidence in Section 58 of the BSA (Section 63 of the IEA) must be understood first in order to evaluate the effects of these changes. Under Section 58 of the BSA, permit oral admissions regarding the contents of an original document as secondary evidence in cases covered by clause (i) of the Explanation to Section 60 of the BSA (Section 65 of the IEA). This provision applies only when the original document, which is in the possession of the opposing party, is not readily accessible or has been lost, destroyed, or otherwise unavailable. Electronic or digital records may be considered primary evidence in certain situations mentioned in Section 57 of the BSA. An oral admission is admissible as secondary evidence for an electronic or digital record, provided that it has been declared primary evidence as per the new Explanation added to Section 57. A significant problem arises whenever the party attempting to use these records cannot produce valid documentation proving their proper ownership and possession, as discussed by the court in the case of Shafhi Mohammad. In such situations, parties may obtain and use electronic or digital records without first applying to the court as per the Arjun Khotkar ruling, which overruled the Shafhi Mohammad ruling. As a result, parties may now have a means to prove the authenticity of electronic or digital records as primary evidence. By including these documents within the definition of primary evidence, this new approach helps ensure that they are subject to less onerous procedural requirements typically applicable to electronic evidence. In certain circumstances, Parliament permitted the use of electronic evidence, even though the Arjun Khotkar decision typically prohibits the application of ordinary methods used for other documentary evidence. It follows that the balanced approach introduced in the Shafhi Mohammad ruling has now been integrated into the statutes which regulate the handling of electronic evidence.

VII. DISCUSSION

The court in the Arjun Khotkar case held that the admissibility of electronic evidence forms a "complete code." As a result of the ruling, two procedural routes previously used in electronic evidence law are no longer in effect. After Navjot Sandhu and Shafhi Mohammad approached the issue in different ways, Arjun Khotkar clarified the law to make it more uniform. However, the implementation of the BSA, 2023, remains unclear. The BSA brings needed progress, but it is unclear whether courts would consider prior rulings to determine if rejected approaches could now qualify as viable alternatives. The judiciary has the option to take prompt action or wait patiently for the court's response. In a time when he could save the world, Einstein estimated that he would first discuss the problem for fifty-nine minutes and then propose a solution in the last minute. Therefore, at this stage, it would be beneficial to identify and explain the problems. As criminals increasingly use digital devices, digital forensic exams are in higher demand. This boost in stimulants creates significant problems for police departments everywhere. Evaluating digital evidence is made difficult by a lack of understanding and training among law enforcement agencies, limited resources to conduct the work, and the increasing number of devices being used. Digital forensic investigations are now, in some cases, handled by automated systems powered by machine learning, which raises concerns about whether people can depend on these systems when the information involved is sensitive and volatile. Digital forensics requires accuracy, dependability and verifiability. Obtaining evidence that reveals criminals while keeping them anonymous remains a challenge. As technology now allows for vast storage, investigations often lead to the discovery of a large amount of unimportant data. Finding irrelevant data about suspects or victims is a privacy concern.

The high level of difficulty in digital forensic investigations often makes it challenging for law enforcement agencies to manage the increasing volume of digital forensic evidence. It happens because data is increasing at a rate that is becoming increasingly difficult to manage. There has been a significant increase in storage capacity over the past two decades, and as data storage is now less costly, it is easier to analyse information. Forensic staff, laboratories, police departments, and the courts are strained by the backlog, resulting in delays in investigations. Cases could thus be delayed. Faster and more efficient computer analysis will help address the large backlog of cases by reducing the time humans need to spend on the process. One of the unique problems India faces is that the population speaks multiple languages. The National Cybercrime Reporting Portal is available in both English and Hindi, which

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

unintentionally excludes a large portion of the population who do not speak either of these languages and may fail to navigate the system. Having many cases on waiting lists results in delays for testing, which makes it harder to find evidence and pushes offenders to continue committing crimes. Since resources are limited, important cases are given priority over the others by law enforcement. Backlogs that are not being resolved lead to a loss of faith among the public regarding safety and the fairness of judgments. Due to the variety of digital devices involved in many crimes, it is essential to rely on specialised techniques. As per Section 75 of the IT Act, 2000, India can prosecute individuals for cybercrimes if their actions affect any computer system located in India; however, the complex extradition laws hinder the implementation of this section.

VIII. CONCLUSION AND SUGGESTIONS

With each new scientific advancement, the methods by which crimes are committed evolve. If we want to preserve peace and control crimes, the criminal justice system must adapt appropriately. Because of this, victimisation and criminalisation policies change the way they work. To respond to these progresses, legislative rules must be changed and supported by actions such as the National Cybersecurity Strategy (NCCS). Building a secure and safe cyberspace is crucial to protecting citizens, businesses, and government agencies from cyberattacks. Cybersecurity laws outline the vision, goals, and core values necessary to achieve these results. Policing and investigating cybercrimes will only be effective if the investigative modules are improved, investigators receive practical training, and state forensic laboratories have the necessary equipment and tools. As crime has become increasingly complex in recent years, with some aspects now occurring online, advanced tools and methods are necessary in electronic forensics. India is facing numerous challenges as electronic forensics is still a developing and emerging field. If investigations rely on outdated or nonsensical methods, it becomes more difficult to gather sufficient evidence to utilise advanced technology in the pursuit of justice. With limited training and equipment, many law enforcement agents struggle to investigate cybercrimes effectively and manage electronic evidence.

Even the most skilled cyber police officers struggle to understand electronic evidence and perform forensic analysis because they often lack sufficient guidance and training. Often, complex investigations or those requiring sophisticated methods rely on forensic labs, such as the NCFL, or consult outside forensic experts. There is no set process at investigating agencies for handling and storing electronic evidence. Because agencies employ various methods for gathering data, inconsistencies arise in criminal investigations, which in turn impact the criminal justice system. Although the International Organisation for Standardisation (ISO) recommends steps to manage electronic information, these are not sufficient for India. Additionally, many Indian forensic workers are unaware of the rules governing the admissibility of electronic evidence, which can lead judges to reject the evidence in court. There is also an issue because there are no standard credentials for professionals in electronic forensics or evidence management. A degree is typically the minimum requirement. Experienced research in the area is not broad enough. The unique challenges of establishing jurisdiction complicate investigations of cybercrimes that occur across state or national borders, as offenders can often act anonymously online. The events of February 1991 necessitated well-designed steps to avoid violating the laws of any country or compromising justice. Addressing these issues requires stronger cooperation from both national and international organisations. To address these issues, India can either implement a nationwide solution or create specialised rules tailored to its specific needs. They should establish minimum credentials for those managing digital evidence, along with the needed educational programs. As a result, investigators in digital forensics can trust that evidence remains stable and can be admitted into the legal system.