DIGITAL EVIDENCE IN CYBERCRIME INVESTIGATION: CHALLENGES UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Dr. Harsh Sharma, Assistant Professor, Government Law College, Dungarpur.

ABSTRACT

This study explores the admissibility of digital evidence under the *Bharatiya Sakshya Adhiniyam, 2023*, with particular emphasis on the legal and practical challenges involved in its implementation within the Indian judicial system. Employing a doctrinal research methodology, the study examines relevant statutory provisions, judicial precedents, and academic literature to evaluate the evolving framework governing electronic evidence. It analyses critical aspects such as the authentication of digital records, certification requirements, maintenance of the chain of custody, and the significance of digital forensic techniques in establishing evidentiary credibility. The research also assesses the implications of emerging technologies, including cloud computing and encryption, on the collection, preservation, and admissibility of electronic evidence. The findings suggest that although the *Bharatiya Sakshya Adhiniyam, 2023* represents a significant step towards modernising the law of evidence by formally recognising electronic records, several practical concerns, including inadequate technical expertise, infrastructural limitations, and procedural complexities, continue to impede its effective implementation. The study concludes that a balanced framework combining robust legal safeguards with technological innovation is essential for ensuring the reliability and effectiveness of digital evidence in judicial proceedings.

Keywords: Digital Evidence; Bharatiya Sakshya Adhiniyam, 2023; Admissibility of Evidence; Electronic Records; Cybercrime; Digital Forensics; Chain of Custody; Authentication; Electronic Evidence; Legal Framework.

Introduction

Rapid technological advancements and the digitisation of human activities have profoundly influenced the transformation of evidentiary paradigms in contemporary legal systems. In India, this transition has culminated in the enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaces the colonial-era *Indian Evidence Act, 1872* and seeks to modernise evidentiary standards in accordance with the realities of the digital age. The increasing reliance on electronic records, including emails, digital documents, metadata, server logs, mobile communications, CCTV footage, and social media content, has fundamentally reshaped the law of evidence. Digital evidence has evolved from being merely corroborative in nature to serving as primary evidence capable of determining the outcome of both civil and criminal proceedings. Nevertheless, its unique characteristics, such as intangibility, ease of duplication, vulnerability to alteration, and dependence on technological systems, have created complex legal issues relating to admissibility, authenticity, integrity, and evidentiary value. The Bharatiya Sakshya Adhiniyam, 2023, addresses these concerns by expressly recognising electronic and digital records as "documents" and "evidence," thereby placing them on par with conventional documentary evidence. The admissibility of digital evidence under the Bharatiya Sakshya Adhiniyam is principally governed by Sections 61, 62, and 63, which collectively establish the statutory framework for the recognition and proof of electronic records. Section 61 affirms that electronic records shall not be denied admissibility merely because they exist in digital form, thereby reinforcing their evidentiary legitimacy. Section 62 provides that the contents of electronic records must be proved in the manner prescribed under Section 63, which lays down specific procedural and technical requirements for establishing their authenticity and reliability. These provisions reflect the legislature's intention to strike a balance between embracing technological developments and maintaining procedural safeguards necessary for ensuring fairness in judicial proceedings. Although these provisions substantially correspond to Sections 65A and 65B of the Indian Evidence Act, 1872, they also represent a progressive legislative effort to accommodate emerging forms of digital evidence within the Indian legal framework. Judicial decisions and academic scholarship consistently emphasise that electronic evidence must satisfy rigorous standards of authenticity, integrity, and reliability, given the ease with which digital information may be altered, manipulated, or fabricated. Despite these legislative reforms, the practical implementation of digital evidence continues to pose significant challenges for the Indian legal system. One of the foremost concerns relates to the authentication of electronic records, as the absence of a tangible medium often complicates the

establishment of authorship, originality, and integrity. The certification requirement prescribed under the law, although designed to ensure evidentiary reliability, has frequently been criticised for its procedural rigidity and its potential to exclude otherwise relevant and reliable evidence. In addition, issues concerning the preservation of digital data, maintenance of the chain of custody, forensic acquisition, and examination of electronic devices introduce further complexities, particularly in cases involving cloud storage, encrypted communications, and multiple service providers. The rapid increase in cybercrime and the growing sophistication of digital manipulation techniques have further intensified these challenges, highlighting the need for specialised forensic expertise and stronger institutional capacities. Studies have shown that investigating agencies and courts often encounter technical limitations, inadequate infrastructure, and a shortage of trained digital forensic professionals, which may adversely affect the effective utilisation of electronic evidence during investigation and trial. Against this backdrop, the Bharatiya Sakshya Adhiniyam, 2023 represents a significant milestone in the evolution of Indian evidence law by providing statutory recognition to digital evidence and establishing a comprehensive legal framework for its admissibility. However, the effectiveness of these reforms ultimately depends upon their practical implementation, judicial interpretation, technological preparedness, and institutional capacity. Accordingly, this study critically examines the admissibility of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023, with particular emphasis on the statutory framework, judicial developments, procedural safeguards, and contemporary challenges. It further explores the role of digital forensics, evolving technologies, and emerging best practices in ensuring the reliability and integrity of electronic evidence, while proposing measures to strengthen the administration of justice in an increasingly digital environment.

Defining Digital Evidence in the Modern Legal Framework

Evidence forms the cornerstone of every judicial proceeding, as it enables courts to determine the existence or non-existence of facts in issue. With the rapid digitisation of communication, commerce, and governance, electronic information has become an indispensable source of evidence in both civil and criminal litigation. Digital evidence refers to any information of evidentiary value that is created, stored, processed, transmitted, or received in electronic form. It encompasses a wide range of electronic records, including emails, text messages, digital photographs, audio and video recordings, computer files, metadata, website records, server logs, CCTV footage, cloud-stored information, mobile phone data, and social media

communications. The Information Technology (Amendment) Act, 2008 recognises electronic records and provides the legal foundation for the admissibility of digital evidence in India. Electronic evidence includes any information or data generated, stored, or transmitted through electronic devices or computer systems, such as computer data, digital audio and video files, mobile phone records, electronic documents, and other forms of digitally stored information. The growing dependence on electronic transactions and digital communication has significantly increased the evidentiary value of such records in judicial proceedings. The statutory framework governing the admissibility of digital evidence has been substantially strengthened under the Bharatiya Sakshya Adhiniyam, 2023. Section 2(1)(e) defines "evidence" broadly to include all documents, including electronic and digital records, produced before the court for inspection. This provision reflects a clear legislative intent to place electronic records on the same footing as conventional documentary evidence, thereby recognising their increasing importance in the administration of justice. Further, Section 32 of the Bharatiya Sakshya Adhiniyam addresses issues relating to electronic records that involve foreign jurisdictions or are generated outside India. As cross-border digital transactions, cloud computing, and international data storage become increasingly common, this provision facilitates the consideration of electronic evidence having transnational elements while ensuring compliance with applicable legal standards. It thereby strengthens India's ability to deal with electronic evidence in cases involving cybercrime, international commercial disputes, and cross-border investigations. The enactment of the Bharatiya Sakshya Adhiniyam, 2023 marks a significant shift from the evidentiary framework under the Indian Evidence Act, 1872. While the earlier legislation was subsequently amended to accommodate electronic evidence through Sections 65A and 65B, the Bharatiya Sakshya Adhiniyam integrates digital evidence directly into the principal statute, thereby providing a more comprehensive and technologically responsive legal framework. This legislative reform reflects the evolving nature of evidence in the digital era and aims to enhance certainty, efficiency, and reliability in judicial proceedings involving electronic records.

Cybercrime and the Growing Importance of Digital Evidence

Cybercrime has emerged as one of the most significant threats in the digital era, encompassing unlawful activities involving computers, computer systems, networks, or other digital devices. Unlike conventional crimes, cybercrimes transcend geographical boundaries and exploit technological vulnerabilities to achieve unlawful objectives, including financial gain,

espionage, political interference, identity theft, and disruption of critical infrastructure. The increasing dependence on digital technologies for communication, commerce, banking, and governance has expanded the scope and complexity of cybercrime, making effective legal regulation and the admissibility of digital evidence indispensable for the administration of justice. Cybercrime manifests in numerous forms, each involving the creation or use of electronic evidence. One of the most prevalent categories is cyber fraud, which includes phishing attacks designed to obtain confidential information through deception, identity theft involving the unauthorised use of personal data, online financial fraud, and fraudulent e-commerce transactions.[4] These offences frequently generate digital evidence in the form of emails, IP addresses, server logs, transaction records, browser histories, and communication metadata, all of which play a crucial role during criminal investigations and judicial proceedings.

Another significant category comprises unauthorised access and cyberattacks, including hacking, malware distribution, ransomware attacks, denial-of-service (DoS) attacks, and data breaches. Malware such as viruses, worms, Trojan horses, spyware, and ransomware is frequently deployed to steal confidential information, disrupt computer systems, or encrypt data until a ransom is paid. Ransomware attacks have become particularly destructive due to their ability to cripple businesses, government agencies, healthcare institutions, and other critical infrastructure. The investigation of these offences largely depends upon digital forensic techniques capable of recovering deleted files, analysing system logs, tracing network activity, and establishing the authenticity and integrity of electronic records. The widespread use of social media platforms, messaging applications, and digital communication technologies has also resulted in a significant rise in cyberstalking, online harassment, cyberbullying, revenge pornography, and the dissemination of obscene or defamatory content. These offences often involve electronic records such as chat histories, emails, screenshots, photographs, videos, voice recordings, and social media posts, which frequently constitute primary evidence before courts. Ensuring the authenticity, integrity, and admissibility of such electronic records has therefore become increasingly important under the Bharatiya Sakshya Adhiniyam, 2023. Combating cybercrime requires a comprehensive and multi-layered approach involving individuals, organisations, and governments. At the individual level, cybersecurity awareness, strong password management, multi-factor authentication, cautious online behaviour, and regular software updates significantly reduce cyber risks. Organisations must implement robust cybersecurity measures, including firewalls, intrusion detection and prevention systems,

encryption technologies, anti-malware software, access control mechanisms, periodic security audits, incident response plans, and employee awareness programmes. Simultaneously, governments play a critical role by enacting effective cyber laws, establishing specialised cybercrime investigation units, enhancing digital forensic infrastructure, and promoting international cooperation for investigating cross-border cyber offences. The rapid advancement of emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), blockchain technology, cloud computing, and quantum computing has further transformed the cyber threat landscape. While these innovations offer significant social and economic benefits, they also create new avenues for cybercriminal activities, requiring continuous adaptation of cybersecurity practices and legal frameworks. Consequently, ongoing research, technological innovation, specialised digital forensic capabilities, and dynamic legislative reforms are essential to address evolving cyber threats and ensure the effective collection, preservation, authentication, and admissibility of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023.

Role of Digital Evidence in Proving Cybercrimes

Digital evidence has evolved from a supplementary form of proof into one of the most significant sources of evidence in the investigation and prosecution of cybercrimes. In contemporary criminal justice systems, cyber offences are typically committed within digital environments and often leave no conventional physical evidence. Instead, they generate electronic traces that serve as the "silent witnesses" of criminal activity. Consequently, digital evidence bridges the gap between invisible cyber activities and legally admissible proof by enabling investigators and courts to reconstruct the sequence of events with a high degree of accuracy.

Unlike traditional evidence, digital evidence provides an objective and chronological record of criminal conduct. Electronic records such as IP addresses, server logs, metadata, browser histories, mobile device records, email communications, blockchain transaction histories, CCTV footage, and cloud-based records enable investigators to establish how, when, and by whom a cyber offence was committed. For example, in cases involving online banking fraud or cryptocurrency theft, while the victim may establish the occurrence of financial loss, digital evidence including IP logs, transaction records, and device identifiers can directly connect the accused to the unauthorised transaction, thereby establishing both identity and participation in

the offence.

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 has significantly strengthened the evidentiary status of electronic records by expressly recognising digital evidence as documentary evidence capable of being produced before courts. This legislative reform reflects the growing importance of electronic records in modern litigation and facilitates their admissibility, subject to compliance with statutory requirements relating to authenticity, integrity, and reliability.[8] The recognition of electronic records under the Bharatiya Sakshya Adhiniyam ensures that courts are better equipped to adjudicate disputes arising from digital transactions, cyber offences, electronic communications, and technologically driven commercial activities. Digital evidence also plays a crucial role in establishing the essential ingredients of criminal liability, including actus reus (the prohibited act) and mens rea (the guilty mind). Through forensic examination of metadata, system logs, deleted files, browser histories, access records, file timestamps, and network activity, investigators can demonstrate deliberate actions such as unauthorised access, data manipulation, malware deployment, or attempts to conceal digital footprints.

The evidentiary value of digital records, however, depends upon maintaining their authenticity and integrity throughout the investigative process. Because electronic data can be easily modified, copied, or deleted, digital forensic investigators must strictly adhere to established procedures relating to the collection, preservation, examination, and documentation of electronic evidence. The maintenance of an unbroken chain of custody, together with the use of cryptographic hash values, write blockers, forensic imaging, and specialised forensic software, ensures that electronic records remain unaltered from the time of seizure until their production before the court. Any compromise in these procedures may affect the reliability and admissibility of the evidence. In the digital age, where sophisticated cybercriminals frequently erase physical traces of their activities, digital footprints including timestamps, geolocation data, communication records, device identifiers, metadata, and cloud storage logs often constitute the most reliable evidence available to investigating agencies. As cybercrimes continue to evolve with advances in artificial intelligence, cloud computing, blockchain technology, and encrypted communications, the effective collection, preservation, forensic analysis, and admissibility of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023, have become indispensable for ensuring successful investigation, prosecution, and the fair administration of justice.

Comparative Analysis of the Admissibility of Digital Evidence Across Nations

The admissibility of digital evidence has become a defining feature of contemporary legal systems as technological advancements continue to transform the nature of criminal and civil litigation. Across jurisdictions, electronic records are increasingly recognised as valuable sources of evidence; however, the legal standards governing their admissibility vary depending on each country's legislative framework and judicial approach. While some jurisdictions prioritise authentication and reliability, others emphasise procedural safeguards, the integrity of electronic records, or statutory presumptions regarding the functioning of computer systems. A comparative examination of different legal systems provides valuable insights into global best practices and highlights the evolving nature of digital evidence law.

India

India has significantly modernised its evidentiary framework through the enactment of the Bharatiya Sakshya Adhiniyam, 2023, which replaces the Indian Evidence Act, 1872. The legislation expressly recognises electronic and digital records as documentary evidence and provides a comprehensive legal framework governing their admissibility. Unlike the previous regime, which relied heavily on the certification requirements under Sections 65A and 65B of the Indian Evidence Act, the Bharatiya Sakshya Adhiniyam integrates digital evidence into the primary statutory framework while continuing to emphasise authenticity, integrity, and procedural compliance. The Act seeks to balance technological advancement with legal safeguards by requiring proper verification, forensic examination where necessary, and adherence to the chain of custody to ensure the reliability of electronic records.

United States

In the United States, the admissibility of digital evidence is governed primarily by the Federal Rules of Evidence, particularly Rules 901 and 902. The American legal system places considerable emphasis on the authentication of electronic evidence rather than imposing rigid statutory certification requirements. Digital evidence is admissible once the party presenting it establishes sufficient proof that the electronic record is what it purports to be. Authentication may be achieved through witness testimony, metadata analysis, digital signatures, system logs, hash values, or self-authenticating electronic records. This flexible approach enables courts to adapt to rapidly evolving technologies while preserving the integrity of judicial proceedings.

United Kingdom

The United Kingdom follows a pragmatic approach to the admissibility of electronic evidence. Although the Police and Criminal Evidence Act, 1984 (PACE) initially contained specific provisions relating to computer-generated evidence, the repeal of Section 69 removed mandatory requirements for proving the reliability of computer systems before admitting electronic records. Under the present common law approach, courts generally presume that computer systems were functioning correctly unless evidence suggests otherwise. This presumption reduces unnecessary procedural barriers while allowing the opposing party to challenge the reliability or authenticity of digital evidence where appropriate.

European Union

Within the European Union, the admissibility of digital evidence is supported by harmonised legal instruments such as the eIDAS Regulation and the Convention on Cybercrime (Budapest Convention). These legal frameworks promote mutual recognition of electronic records across Member States and establish common standards relating to electronic identification, electronic signatures, electronic seals, trusted timestamps, and digital authentication. Particular emphasis is placed on maintaining the integrity of electronic records and preserving an uninterrupted chain of custody. The European approach is especially significant in facilitating cross-border investigations and judicial cooperation in cases involving cybercrime and international digital transactions.

Singapore

Singapore has developed one of the most technologically advanced legal frameworks governing electronic evidence through the Evidence Act (Cap. 97). The legislation adopts a presumption of reliability for electronic records generated in the ordinary course of business, provided that the source of the information is credible and the integrity of the electronic system can be established. Courts retain the discretion to examine the authenticity and reliability of electronic evidence where disputes arise. This balanced approach reduces procedural complexity while ensuring that only trustworthy digital records are admitted into evidence.

Judicial Pronouncements on Digital Evidence

The admissibility of digital evidence in India has undergone significant judicial evolution over

the past two decades. The Supreme Court has played a pivotal role in interpreting the legal framework governing electronic records by clarifying the procedural requirements for their admissibility and determining the evidentiary value of digital materials. Judicial decisions have progressively balanced technological advancements with the need to preserve the authenticity, integrity, and reliability of electronic evidence. Three landmark decisions, *State (NCT of Delhi) v. Navjot Sandhu*, *Anvar P.V. v. P.K. Basheer*, and *Tomaso Bruno v. State of Uttar Pradesh* have substantially influenced the development of Indian jurisprudence relating to digital evidence.

In *State (NCT of Delhi) v. Navjot Sandhu*[1], popularly known as the Parliament Attack Case, the Supreme Court considered the admissibility of mobile phone call records and other electronic evidence relied upon by the prosecution following the terrorist attack on the Indian Parliament. The principal issue before the Court was whether electronic records could be admitted in evidence without the certificate prescribed under Section 65B(4) of the Indian Evidence Act, 1872. The Supreme Court adopted a liberal interpretation by holding that electronic records could still be admitted through the general provisions governing secondary evidence even in the absence of a Section 65B certificate. The Court reasoned that where the original electronic record was unavailable, secondary evidence could be admitted under the ordinary evidentiary rules. This decision considerably relaxed the procedural requirements relating to electronic evidence and facilitated the admission of digital records during criminal trials. However, this approach generated legal uncertainty and was subsequently overruled by the Supreme Court in *Anvar P.V. v. P.K. Basheer*[2], which restored the mandatory nature of statutory certification.

The judgment in *Anvar P.V. v. P.K. Basheer*[3] represents a watershed moment in the jurisprudence governing electronic evidence in India. The dispute arose from an election petition in which the admissibility of electronic records, including compact discs (CDs) containing speeches and campaign materials, was questioned. The Supreme Court was required to determine whether electronic evidence could be admitted without compliance with Section 65B of the Indian Evidence Act. The Court unequivocally held that Section 65B constitutes a complete and self-contained code governing the admissibility of electronic records. It ruled that any electronic record produced as secondary evidence must be accompanied by the certificate prescribed under Section 65B(4), failing which it would be inadmissible. The

[1] (2005) 11 SCC 600.
[2] Ibid.
[3] (2014) 10 SCC 473.

judgment expressly overruled the earlier position adopted in *Navjot Sandhu* and established strict compliance with the statutory requirements as an essential condition for the admissibility of electronic evidence. This decision significantly strengthened procedural safeguards intended to ensure the authenticity and reliability of digital evidence presented before courts.

In *Tomaso Bruno v. State of Uttar Pradesh*[4], the Supreme Court examined the evidentiary significance of electronic records in a criminal prosecution relating to the murder of a foreign national in Varanasi. During the investigation, the prosecution failed to produce crucial electronic evidence, including CCTV footage and other relevant technical records that could have assisted in establishing the sequence of events. Although the Court did not directly revisit the principles laid down in *Anvar P.V. v. P.K. Basheer*[5], it emphasised the growing importance of electronic evidence in modern criminal investigations. The Court observed that where technological evidence such as CCTV footage is readily available, investigating agencies are expected to collect, preserve, and present such evidence before the court. The failure to produce or properly preserve available electronic evidence may create serious deficiencies in the prosecution's case and give rise to adverse inferences regarding the fairness and completeness of the investigation. Since the prosecution failed to establish guilt beyond a reasonable doubt, the accused were acquitted. The decision reinforced the principle that effective investigation and proper preservation of digital evidence are indispensable to ensuring a fair criminal trial.

The landmark decision in *K.S. Puttaswamy v. Union of India*[6] fundamentally transformed Indian constitutional jurisprudence by unanimously recognising the right to privacy as an intrinsic part of the right to life and personal liberty guaranteed under Article 21 of the Constitution of India. A nine-judge Constitution Bench held that privacy is a fundamental right and that any restriction imposed by the State must satisfy the constitutional principles of legality, legitimate state purpose, necessity, and proportionality. This judgment has far-reaching implications for the investigation of cybercrimes and the collection of digital evidence, particularly in an era where personal information is extensively stored on electronic devices and digital platforms. The principles laid down in *Puttaswamy* require that every exercise of governmental authority involving the seizure of electronic devices, interception of communications, surveillance, or extraction of digital data must comply with the doctrine of proportionality. Accordingly, investigative agencies must demonstrate that the interference

[4] (2015) 7 SCC 178.
[5] Ibid at 7.
[6] (2017) 10 SCC 1.

with an individual's privacy is authorised by law, pursues a legitimate public objective, is necessary for achieving that objective, and represents the least restrictive means available. These constitutional safeguards ensure that the collection of electronic evidence does not result in arbitrary or excessive intrusion into an individual's private digital sphere. The judgment assumes particular significance in relation to the powers conferred upon investigating authorities under Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) governing search and seizure, and Section 69 of the Information Technology Act, 2000, which authorises the interception, monitoring, or decryption of electronic information under specified circumstances.[36] [37] Although these provisions empower law enforcement agencies to obtain digital evidence for the investigation of offences, the exercise of such powers must remain consistent with the constitutional standards established in *Puttaswamy*. Consequently, indiscriminate seizure of electronic devices or unrestricted access to personal digital data without adequate procedural safeguards may be vulnerable to constitutional challenge.

The enactment of the Digital Personal Data Protection Act, 2023, further strengthens the legal framework governing the processing and protection of personal data in India. Although the Act primarily regulates the collection, processing, and protection of digital personal data, the rules framed under it are expected to provide greater clarity regarding the manner in which investigating agencies may access, extract, retain, and process electronic data while respecting the privacy rights of individuals. Such safeguards are particularly important in ensuring that the collection of digital evidence remains proportionate, transparent, and legally accountable. The *Puttaswamy* judgment therefore establishes an essential constitutional balance between effective criminal investigation and the protection of individual privacy. While digital evidence has become indispensable for investigating cyber offences and other technologically driven crimes, its collection and use must always be guided by constitutional guarantees, procedural fairness, and respect for fundamental rights. As the Bharatiya Sakshya Adhiniyam, 2023 increasingly facilitates the admissibility of electronic records, the principles laid down in *Puttaswamy* continue to serve as a constitutional safeguard against arbitrary state action and reinforce the need for privacy-conscious digital investigations.

Critical Analysis: Lacunae and Challenges

A. The "Expert" Conundrum under Section 63(4)

One of the most significant shortcomings of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) is

the absence of a clear statutory definition of the term "expert" for certification under Section 63(4). Although the provision envisages expert certification to establish the authenticity and integrity of electronic records, it does not prescribe the qualifications, accreditation, experience, or institutional affiliation required for such experts. This legislative ambiguity creates uncertainty regarding the competence of individuals authorised to certify digital evidence and may result in frequent challenges to the admissibility of electronic records during trial. At the same time, the absence of uniform standards increases the possibility of inadequately qualified persons certifying technically complex electronic evidence, thereby undermining judicial confidence in the certification process. The problem is further aggravated by the limited availability of digital forensic infrastructure in India. Despite the increasing incidence of cybercrime, the country continues to face an acute shortage of notified forensic laboratories and qualified digital forensic experts. Reports indicate that only a limited number of forensic laboratories have been notified under Section 79A of the Information Technology Act, 2000, resulting in substantial delays in the examination of electronic devices. In several States, forensic analysis of digital evidence often requires many months before reports are made available to investigating agencies. Consequently, the mandatory involvement of experts under Section 63(4) may further burden an already overstretched forensic system, delaying criminal investigations and judicial proceedings. Unless the government substantially enhances forensic infrastructure and establishes uniform accreditation standards for digital experts, the practical implementation of the certification framework may remain challenging.

B. Practical Challenges in Maintaining the Chain of Custody

The maintenance of an uninterrupted chain of custody is fundamental to ensuring the authenticity and integrity of digital evidence. Recognising its importance, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) requires investigating agencies to properly document the collection, preservation, transfer, examination, and production of electronic evidence. Although this statutory requirement represents a significant procedural safeguard, its effective implementation remains a major practical challenge. Many investigating agencies, particularly at the district and State levels, continue to face shortages of specialised training, forensic equipment, and standard operating procedures for handling electronic evidence. Establishing the integrity of digital evidence frequently requires specialised forensic tools such as FTK Imager, Cellebrite, EnCase, or similar software capable of generating forensic images and verifying cryptographic hash values. However, such facilities are not uniformly available

across cybercrime police stations and forensic laboratories. The Supreme Court has consistently emphasised the importance of preserving the chain of custody to ensure evidentiary reliability. In *State of Rajasthan v. Kashi Ram*[7], the Court reiterated that proper preservation of evidence is essential for maintaining its evidentiary value. In the context of electronic evidence, however, compliance with this requirement depends not only upon legal procedures but also upon the availability of sophisticated technological infrastructure and trained forensic personnel.

C. Transitional Challenges under the Bharatiya Sakshya Adhiniyam, 2023

The transition from the Indian Evidence Act, 1872, to the Bharatiya Sakshya Adhiniyam, 2023, presents several procedural and practical difficulties. The savings clause contained in the new legislation provides that investigations, inquiries, trials, appeals, and other proceedings pending prior to the commencement of the Bharatiya Sakshya Adhiniyam shall continue to be governed by the provisions of the Indian Evidence Act as though the new legislation had not been enacted. While this transitional arrangement preserves legal certainty and protects pending proceedings from procedural disruption, it simultaneously creates two parallel evidentiary regimes operating within the judicial system. As a result, courts, prosecutors, defence counsel, and investigating agencies must apply different evidentiary standards depending upon the date on which proceedings commenced. Such dual application increases the possibility of procedural confusion and inconsistent judicial practices. Furthermore, attempts to retrospectively adapt electronic records collected under the earlier legal framework to satisfy the procedural requirements of the Bharatiya Sakshya Adhiniyam may invite allegations of manipulation or compromise the integrity of digital evidence. The Supreme Court's observations in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[8] reinforce the importance of preserving the authenticity of electronic records and ensuring strict compliance with statutory certification requirements throughout this transitional period.

D. Privacy, Surveillance, and Digital Due Process

The growing reliance upon digital evidence has significantly expanded the investigative powers of law enforcement agencies. Provisions relating to the search and seizure of electronic devices under the Bharatiya Nagarik Suraksha Sanhita, 2023, together with the interception,

[7] (2006) 12 SCC 254.
[8] (2020) 7 SCC 1.

monitoring, and decryption powers contained in Sections 69 and 69A of the Information Technology Act, 2000, enable investigating agencies to obtain digital evidence in cybercrime investigations. While these powers are essential for combating technologically sophisticated offences, their exercise must remain consistent with constitutional guarantees relating to privacy and personal liberty. The Supreme Court's decision in *K.S. Puttaswamy v. Union of India* established that any interference with an individual's privacy must satisfy the constitutional requirements of legality, necessity, proportionality, and procedural safeguards. Consequently, indiscriminate seizure of electronic devices or unrestricted access to personal digital information may violate the fundamental right to privacy under Article 21 of the Constitution. Moreover, the absence of a mandatory judicial warrant requirement in certain categories of cases has generated concerns regarding excessive executive discretion. The principles laid down in *Arnesh Kumar v. State of Bihar* [9]further require investigating agencies to exercise restraint and avoid unnecessary coercive measures. These constitutional safeguards assume even greater significance in cybercrime investigations, where electronic devices frequently contain highly sensitive personal and professional information unrelated to the alleged offence.

E. Deepfakes and AI-Generated Digital Evidence

One of the most significant emerging challenges confronting the Bharatiya Sakshya Adhiniyam is the absence of specific provisions governing the admissibility and authentication of artificial intelligence-generated or synthetic digital evidence, including deepfakes. Advances in generative artificial intelligence have enabled the creation of highly realistic fabricated images, videos, audio recordings, and digital documents that are increasingly difficult to distinguish from genuine electronic records. Although Indian courts have issued directions in cases involving deepfake content and personality rights, the existing statutory framework does not prescribe specialised standards for verifying the authenticity of AI-generated material during criminal or civil proceedings. The certification mechanism under Section 63(4), which primarily focuses on verifying the integrity of conventional electronic records through hash values and expert certification, may not adequately address the complexities associated with synthetic media. Unlike traditional electronic records, deepfakes often originate through sophisticated machine learning algorithms that require advanced forensic techniques capable of identifying digital manipulation, source provenance, and algorithmic artefacts. Furthermore,

[9] (2014) 8 SCC 273.

the procedural framework under the Bharatiya Nagarik Suraksha Sanhita, 2023, which permits expert reports to be relied upon unless specifically challenged, may reduce judicial scrutiny of expert certifications in cases involving manipulated digital content. Given the increasing prevalence of artificial intelligence in generating fabricated electronic evidence, there is an urgent need for legislative reforms establishing specialised forensic standards, expert accreditation mechanisms, and evidentiary guidelines to ensure that courts can reliably distinguish authentic digital evidence from technologically sophisticated fabrications.

Recommendations

The Bharatiya Sakshya Adhiniyam, 2023 marks a significant milestone in the evolution of India's law of evidence by aligning the evidentiary framework with the realities of an increasingly digital society. By expressly recognising electronic records as documentary evidence, prohibiting discrimination against digital evidence, and introducing a comprehensive statutory mechanism for proving electronic records, the Act substantially strengthens the legal framework governing the admissibility of digital evidence. When read together with the Bharatiya Nagarik Suraksha Sanhita, 2023, which provides for digital investigation techniques, mandatory documentation of the chain of custody, audio-video recording of searches and seizures, and greater reliance on forensic investigation, the new legislative regime reflects India's commitment to modernising criminal justice in response to technological advancement and the growing prevalence of cybercrime. Despite these progressive reforms, the study identifies several legal and practical challenges that continue to affect the effective implementation of the Bharatiya Sakshya Adhiniyam. The absence of clearly defined qualifications and accreditation standards for experts involved in the authentication of electronic evidence creates uncertainty regarding the credibility and admissibility of digital records. Similarly, inadequate forensic infrastructure, shortage of trained digital forensic professionals, delays in forensic examination, and inconsistent implementation of chain of custody protocols significantly reduce the efficiency of cybercrime investigations. The transitional coexistence of proceedings governed by both the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023 further contributes to procedural complexity and may create interpretational difficulties for courts and investigating agencies.

The constitutional dimension of digital evidence also requires careful consideration. The increasing powers of search, seizure, surveillance, interception, and extraction of electronic

data must always be exercised in conformity with the principles laid down by the Supreme Court in *K.S. Puttaswamy v. Union of India*, particularly the requirements of legality, necessity, proportionality, and procedural fairness. As digital devices contain extensive personal and sensitive information, the protection of individual privacy must remain an essential component of every cybercrime investigation. Strengthening judicial oversight, establishing transparent procedural safeguards, and ensuring accountability in the exercise of investigative powers are therefore indispensable for maintaining public confidence in the criminal justice system. Another emerging concern is the rapid advancement of artificial intelligence, deepfake technology, blockchain-based transactions, encrypted communication platforms, and cloud computing.

Based on the findings of this study, the following measures are recommended:

1. **Statutory Clarification of Expert Qualifications:** The Central Government should prescribe uniform qualifications, accreditation standards, and certification procedures for experts authorised to authenticate electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023.

2. **Strengthening Digital Forensic Infrastructure:** Additional forensic laboratories should be established across the country, accompanied by increased investment in digital forensic tools, laboratory capacity, and specialised training for forensic experts, police officers, prosecutors, and judicial officers.

3. **Standardised Chain of Custody Protocols:** Uniform national guidelines should be formulated for the identification, collection, preservation, transportation, forensic examination, and presentation of electronic evidence to minimise procedural inconsistencies.

4. **Enhanced Privacy Safeguards:** Clear procedural safeguards, including judicial oversight wherever appropriate, should regulate the seizure, extraction, interception, and analysis of electronic data to ensure compliance with constitutional privacy principles.

5. **Legislative Response to Emerging Technologies:** The Bharatiya Sakshya Adhiniyam should be periodically reviewed and updated to address evolving technologies such as

artificial intelligence, deepfakes, blockchain, cloud computing, and quantum technologies, ensuring that evidentiary standards remain technologically relevant.

6. **Capacity Building and Judicial Training:** Regular training programmes should be conducted for judges, prosecutors, investigators, and legal practitioners on digital forensics, cybersecurity, emerging technologies, and the evolving jurisprudence relating to electronic evidence.

Conclusion

The Bharatiya Sakshya Adhiniyam, 2023, marks a significant advancement in the modernisation of India's law of evidence by providing statutory recognition to electronic and digital records and aligning the evidentiary framework with the realities of an increasingly digital society. As cybercrimes continue to proliferate and digital transactions become integral to everyday life, the admissibility of digital evidence has assumed unprecedented importance in ensuring effective investigation and fair adjudication. By recognising electronic records as documentary evidence and prescribing a structured framework for their authentication and admissibility, the Act strengthens the legal foundation for addressing technology-driven offences while enhancing the efficiency of judicial proceedings. The study demonstrates that although the Bharatiya Sakshya Adhiniyam, 2023 introduces progressive reforms, several practical and legal challenges continue to affect its implementation. Ambiguities regarding expert certification, inadequate digital forensic infrastructure, inconsistencies in maintaining the chain of custody, procedural complexities during the transitional phase, and the absence of comprehensive standards for emerging technologies such as artificial intelligence and deepfakes pose significant obstacles to the effective use of electronic evidence. In addition, the increasing investigative powers relating to search, seizure, interception, and extraction of digital data must be exercised in accordance with constitutional guarantees of privacy, proportionality, and due process as recognised by the Supreme Court in *K.S. Puttaswamy v. Union of India*. A comparative analysis of international legal frameworks reveals that jurisdictions such as the United States, the United Kingdom, the European Union, and Singapore have developed distinct mechanisms for ensuring the authenticity and reliability of electronic evidence through flexible authentication standards, statutory presumptions, and technologically advanced forensic practices. These comparative approaches provide valuable guidance for further strengthening India's legal framework while preserving procedural fairness

and evidentiary integrity. The success of the Bharatiya Sakshya Adhiniyam, 2023 ultimately depends not only upon legislative reform but also upon effective implementation through robust forensic infrastructure, specialised training of investigators and judicial officers, uniform procedural guidelines, and continuous adaptation to technological advancements. As cybercrime continues to evolve with innovations such as cloud computing, blockchain technology, encrypted communications, and artificial intelligence, India's evidentiary framework must remain dynamic and responsive to emerging challenges. In conclusion, the Bharatiya Sakshya Adhiniyam, 2023, establishes a comprehensive legal framework for the admissibility of digital evidence and represents an important milestone in the evolution of Indian evidence law. However, sustained institutional reforms, technological preparedness, judicial consistency, and periodic legislative review will be essential to ensure that digital evidence remains reliable, authentic, and capable of supporting the fair administration of justice in the digital era. By maintaining an appropriate balance between technological innovation, procedural safeguards, and constitutional rights, the Act has the potential to significantly strengthen India's response to cybercrime and reinforce public confidence in the justice delivery system.