BRIDGING LEGAL RIGOUR AND TECHNOLOGICAL CONSTRAINTS: ANALYSING DEFICIENCIES IN DIGITAL EVIDENCE HANDLING UNDER THE BHARTIYA SAKSHYA ADHINIYAM 2023

Parth Attry, Chandigarh University

ABSTRACT

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), marks a significant reform in Indian legal history, acting as a comprehensive update to the Indian Evidence Act of 1872. This legislation clearly recognizes and incorporates electronic evidence, reflecting the urgent need to align India's evidentiary framework with current technological realities and digital communication methods. By adding 170 sections, the BSA systematically replaces outdated colonial-era language with definitions and provisions that are specifically designed to meet modern judicial challenges related to digital evidence. Its core reforms include the broad acceptance of electronic records as legally valid evidence, equivalent to traditional documents. This legal recognition explicitly expands the scope of "documents" to include digital formats such as emails, electronic signatures, and other electronically stored information, thereby reducing ambiguity and ensuring consistency in court procedures.

Additionally, specific provisions within the Act, notably Sections 61 and 63, play crucial roles in ensuring electronic evidence is accepted rather than dismissed because of its format. Section 61 prevents courts from denying evidence solely because it is electronic, while Section 63 introduces a standard expert certification process to verify such evidence, enhancing judicial confidence and procedural efficiency. Moreover, the BSA extends its authority to include military courts, representing a comprehensive nationwide reform.

Despite these pioneering legislative actions, challenges in implementation remain, mainly due to infrastructural deficiencies, limited forensic technologies, and a lack of skilled personnel trained in cyber forensics. The Act's goals to streamline digital evidence management are further complicated by cybersecurity risks, privacy issues, and transnational jurisdictional complexities caused by cloud computing and dispersed data environments. These factors highlight the need to upgrade government infrastructure and establish clear protocols to preserve evidential integrity.

Furthermore, the BSA is part of a broader legal transformation alongside the Bharatiya Nyaya Sanhita and the Bharatiya Nagarik Suraksha Sanhita, which collectively aim to effectively address cybercrime and strengthen judicial capacity in the digital age. Technological advancements such as blockchain, artificial intelligence, and proactive digital forensic techniques promise to support these reforms, but also require updates in legal education and court procedures to fill existing competency gaps.

In conclusion, the Bharatiya Sakshya Adhiniyam, 2023, creates a vital foundation for a progressive, technology-ready legal system in India. To realize its full potential, ongoing investments in forensic infrastructure, judicial training, interdisciplinary collaboration, and policy improvements are essential. These measures will help ensure fair, transparent, and efficient justice, balancing the strict demands of the law with the challenges of digital innovation.

INTRODUCTION

Background on Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), marks a significant legislative milestone in modernizing the Indian legal framework and serves as an important update to the Indian Evidence Act of 1872. Originally enacted during colonial rule, the older Indian Evidence Act contained outdated terminology and definitions that no longer reflect current realities, particularly concerning technological developments. The BSA provides a necessary overhaul by replacing colonial terms with language that is modern and reflective of contemporary legal and technological practices. A key feature of the BSA is its focus on electronic evidence, acknowledging the growing importance of digital data in legal proceedings today. Unlike older statutes, which often viewed electronic records as secondary or peripheral evidence, the BSA actively broadens the admissibility scope to include digital records seamlessly within formal evidentiary processes. This includes redefining concepts like "documents" and "evidence" to explicitly cover various digital formats, eliminating ambiguities, and ensuring consistent understanding across courts. The enactment of the BSA is also notable for expanding jurisdictional scope to include military courts, representing a comprehensive reform that impacts India’s entire judicial system. With 170 sections, the BSA aims to harmonize legal standards with technological advances, fundamentally reshaping evidence law to meet the

evolving needs of modern Indian jurisprudence. [1],[2].

Significance of Digital Evidence in Modern Legal Systems

In the current era, digital communication, record keeping, and transactions have permeated nearly every aspect of societal functioning and governance. This transformation highlights the importance of updating legal systems to effectively handle and evaluate digital evidence. The digital realm introduces complexities such as authenticity, immutability, and chain of custody that challenge traditional evidentiary principles. Courts worldwide increasingly encounter cases where crucial proof is stored in electronic records like emails, instant messages, system logs, videos, and metadata. Therefore, legal frameworks must evolve to ensure that this evidence is reliably admissible and can be thoroughly evaluated in judicial processes. In India, the digitization of evidence is particularly urgent given the acceleration of the internet in the era of digital governance efforts. Despite legal advances, exemplified by the BSA, significant challenges remain in ensuring digital evidence is handled in a way that maintains its reliability and meets judicial standards. These challenges include verifying the authenticity and origin of digital records, keeping pace with rapidly advancing technology, and navigating jurisdictional issues due to the global nature of digital networks. These complexities make developing strong, transparent, and technologically competent legal frameworks essential. [3], [4].

Objective and Scope of the Analysis

This article aims to critically analyse the deficiencies and challenges that persist in handling digital evidence under the provisions of the Bharatiya Sakshya Adhiniyam, 2023, despite its forward-looking legislative reforms. While the BSA represents a significant step towards integrating digital modalities into the legal evidentiary system, the practical and technological constraints that plague full implementation demand a comprehensive evaluation. The objective is to pinpoint and elaborate on gaps where legal rigor must be balanced against the realities of

[1] M.I. Wahab, Bharatiya Sakshya Adhiniyam, 2023: An Overview of Key Amendments, INT'L J. MULTIDISCIPLINARY RES., 2024, https://doi.org/10.36948/ijfmr.2024.v06i06.30136.
2.V. Singh et al., Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, METALLURGICAL & MATERIALS ENGINEERING, 2025, https://doi.org/10.63278/1383.
[3] N.K. Bharti & N. Gupta, Admissibility of Electronic Evidence in India: Legal Framework, Judicial Trends, and the Impact of the Bharatiya Sakshya Sanhita, 2023, INT'L J. MULTIDISCIPLINARY RES. (2025), https://doi.org/10.36948/ijfmr.2025.v07i04.54750.
[4] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627.

technical infrastructure, forensic capacities, and judicial expertise. Moreover, this analysis aims to highlight the deficiencies in processes such as evidence collection, certification, preservation, and courtroom admissibility of electronic records, and how these may hinder the judicial system's effectiveness. The study emphasizes the importance of a coordinated approach that involves legal professionals, technologists, and policymakers to bridge these gaps. Additionally, it stresses the necessity of continuous professional training and policy reform to enhance judicial technology literacy and procedural standards. Thus, the scope of this research encompasses legal provisions, infrastructural capabilities, technological innovations, privacy and ethical dilemmas, and policy-level implementation barriers, offering a holistic view of digital evidence handling under the BSA[5].

LEGAL FRAMEWORK OF THE BHARTIYA SAKSHYA ADINIYAM 2023

Structural Revisions and Terminology Modernization

The Bharatiya Sakshya Adhiniyam, 2023, undertakes a vast revision of the Indian Evidence Act, focusing on updating obsolete language and adapting legal concepts relevant to the digital era. This structural modernization addresses the linguistic and conceptual traditions inherent in colonial legal texts by incorporating definitions that explicitly accommodate electronic evidence and digital documentation. Key concepts such as "documents" now include digital signatures, emails, electronic records, and other forms of digitally created or stored data. This clarity is crucial in standardizing evidentiary procedures and avoiding interpretive discrepancies in courts across jurisdictions. The BSA codifies the admissibility criteria for electronic records with distinct provisions, reflecting an understanding of the complexities of digital data. The Act's detailed sections articulate strict conditions for the preservation and presentation of digital evidence, emphasizing integrity and authenticity, while simultaneously allowing for procedural flexibility to keep pace with technological evolution. These legislative revisions represent a conscious departure from the colonial-era statutes' limited scope to a framework that is responsive and adaptive to contemporary needs, underpinning a modern, technology-aligned justice system. [6]

[5] J.F.M. Cruz, C.P.M. Davila, H.A.G. Laguna & E.J.G. Malaga, Innovative Management in the Legal World: Keys to Making the Right Decisions, PETITA JURNAL KAJIAN ILMU HUKUM DAN SYARIAH (2025), https://doi.org/10.22373/petita.v10i2.834.

[6] M.I. Wahab, Bharatiya Sakshya Adhiniyam, 2023: An Overview of Key Amendments, INT'L J. MULTIDISCIPLINARY RES. (2024), https://doi.org/10.36948/ijfmr.2024.v06i06.30136.

Key Provisions for Electronic Evidence

Among the BSA's most consequential reforms are Sections 61 and 63, which directly confront long-standing challenges in the treatment of electronic evidence. Section 61 is particularly groundbreaking as it undoubtedly prohibits the denial of admissibility solely on the basis that the evidence is electronic in nature. This removes a major barrier that historically relegated digital records to secondary evidentiary status and establishes parity between electronic and conventional documentary evidence. Complementing this, Section 63 introduces a uniform certification process that mandates expert authentication of electronic records, reinforcing mechanisms to verify digital evidence's authenticity and reliability. This process assists courts in adjudicating the validity of e-records while streamlining adjudicative procedures. Together, these provisions not only expedite judicial handling of cases involving electronic evidence but also reduce procedural challenges that arise due to technological ambiguities. By embedding such legal clarity, the BSA aims to build judicial confidence in handling electronic evidence and minimize cases of wrongful exclusion based on format scepticism. [7].

Integration with Other Recent Legal Reforms

The BSA does not operate in isolation but forms a key component of a broader framework of legal reforms introduced in 2023, including the Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Nagarik Suraksha Sanhita (BNSS). These statutes collectively mark a paradigm shift by replacing outdated colonial provisions with Indian-centric, modern laws tailored to the realities of digital society. Together, they overhaul investigative, prosecutorial, and adjudicatory procedures, particularly in the context of cybercrimes and digital evidence. The BSA's integration with these complementary reforms enables a cohesive approach to evidence handling that supports efficient cybercrime prosecution, protection of citizen rights, and enhancement of due process. Such alignment ensures consistency across the criminal justice system, fostering judicial efficiency and legal certainty. Moreover, with cyber offenses increasingly pervasive and complex, the synchronicity among these laws is essential in empowering law enforcement agencies and the judiciary with holistic tools for digital evidence

[7] V. Singh et al., Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, METALLURGICAL & MATERIALS ENG'G (2025), https://doi.org/10.63278/1383.

management. [8]

TECHNOLOGICAL CONSTRAINTS IN DIGITAL EVIDENCE HANDLING

Infrastructure Deficiencies

A critical obstacle to the effective implementation of the BSA's provisions is the glaring deficiency in forensic infrastructure across India. Despite legislative advances, many regions, especially rural and resource-poor jurisdictions, suffer from a lack of adequately equipped forensic laboratories and trained personnel. This infrastructure gap directly affects the collection, preservation, and analysis of digital evidence. Forensic labs essential for data extraction, verification, and the maintenance of the chain of custody are either under-resourced or non-existent in numerous districts. Such deficiencies introduce risks of evidence degradation, loss, or contamination, ultimately undermining the integrity and admissibility of electronic evidence. Furthermore, inadequate technical support systems compound these problems, resulting in delayed investigations and compromised prosecutions. Therefore, while the BSA sets standards for electronic evidence, infrastructural realities impose severe constraints on fulfilling those standards uniformly across the country. [9].

Cybersecurity and Data Integrity Challenges

The digital nature of evidence presents inherent vulnerabilities to tampering, cyber-attacks, and unauthorized modifications, necessitating robust cybersecurity protocols to protect data integrity throughout its lifecycle. In the practical application of the BSA, risks of manipulation during the collection, storage, or transmission of electronic records threaten evidentiary reliability. The challenge lies not only in developing technical safeguards but also in institutionalizing secure procedures that guard against such threats. For instance, authentication mechanisms under Section 63 require the utilization of cryptographic and forensic tools that are sometimes difficult to deploy in heterogeneous technological environments. Additionally, cybercriminals may employ sophisticated techniques to alter or fabricate digital evidence, raising the need for advanced forensic analytic capabilities to detect such forgeries. The failure

[8] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627.
[9] V. Singh et al., Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, METALLURGICAL & MATERIALS ENG'G (2025), https://doi.org/10.63278/1383.

to adequately address cybersecurity and data integrity jeopardizes judicial outcomes and diminishes public trust in the legal system's capacity to handle digital evidence impartially and accurately[10].

Privacy and Jurisdictional Issues

Handling digital evidence raises complex issues regarding privacy rights and jurisdiction, often complicating evidence acquisition and admissibility. In India, as in many jurisdictions, the collection of electronic data must carefully balance investigative imperatives against individual privacy protections. The absence of explicit legal clarity on surveillance limits, data retention standards, and usage conditions can lead to infringements on civil liberties and potential misuse of sensitive information during criminal investigations. Moreover, jurisdictional challenges arise particularly in cases where data is stored or processed across geographical and political boundaries, a common scenario in cloud-based and distributed ledger systems. These cross-border data flows often encounter conflicting national laws, hindering smooth judicial cooperation and creating procedural uncertainties. The evolving nature of digital evidence calls for updated legal provisions to harmonize privacy rights with effective law enforcement, ensuring that constitutional and international standards are respected while facilitating evidence admissibility. [11], [12].

DEFICIENCIES IN LEGAL PROCEDURES REGARDING DIGITAL EVIDENCE

Evidence Collection and Preservation Difficulties

The identification, collection, and preservation of electronic evidence present unique procedural complexities that challenge conventional forensic methods. Digital evidence often resides in heterogeneous formats covering multiple device types, operating systems, and cloud environments, which complicates standardization of collection protocols. The dynamic and fleeting nature of some digital data, such as transient memory or volatile logs, necessitates

[10] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627.
[11]S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627.
[12] N.K. Bharti & N. Gupta, Admissibility of Electronic Evidence in India: Legal Framework, Judicial Trends, and the Impact of the Bharatiya Sakshya Sanhita, 2023, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i04.54750.

prompt acquisition techniques often difficult to reconcile with slower judicial processes. Moreover, real-time or live evidence acquisition faces limitations in terms of both technical admissibility and legal authorization. The absence of clear procedural guidelines for handling such evidence in the BSA, or its integration with operational frameworks, hampers investigators' ability to execute timely and comprehensive data collection, risking evidence loss or contamination. These difficulties underscore the need for updated procedural manuals and technological resources, as well as specialized training for law enforcement and forensic experts. [13].

Chain of Custody and Authenticity Concerns

The integrity of digital evidence hinges on rigorous maintenance of the chain of custody and assured authenticity, yet these aspects remain problematic under current procedural frameworks. Establishing an unbroken chain of custody for electronic records demands meticulous documentation and secure handling at every stage, from acquisition, transfer, storage, to presentation in court. Discrepancies or gaps in this chain cast doubt on the evidentiary reliability and may result in the exclusion of crucial digital proof. Additionally, expert certification as prescribed by Section 63 of the BSA is subject to variability due to the absence of uniform procedural clarity and differences in certification standards across regions and jurisdictions. This generates inconsistencies in how digital evidence is authenticated before courts, occasionally leading to judicial scepticism or rejection. Addressing these concerns requires the development of uniform procedural protocols, widely recognized certification standards, and enhanced monitoring mechanisms to safeguard evidentiary authenticity. [14].

Courtroom Admissibility and Judicial Capacity

A further bottleneck in the effective handling of digital evidence is the limited technological literacy among judicial officers and legal practitioners. Many judges and lawyers possess an inadequate understanding of the technical nuances underlying electronic evidence, often undermining their ability to assess, interpret, and weigh such evidence appropriately in trials. This gap compromises judicial capacity to engage with forensic experts, evaluate certification credibility, and articulate reasoned judgments on digital data admissibility. The increasing

[13] V. Machaka & T. Balan, Investigating Proactive Digital Forensics Leveraging Adversary Emulation, APPLIED SCI. (2022), https://doi.org/10.3390/app12189077.
[14] V. Singh et al., Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, METALLURGICAL & MATERIALS ENG'G (2025), https://doi.org/10.63278/1383.

complexity of digital forensics demands specialized judicial training programs and continuous capacity building to enhance legal professionals' competence in technological domains. Without such empowerment, courts risk inconsistent rulings and may struggle with evidentiary challenges unique to digital proof. Hence, investing in educational initiatives and fostering collaborations between technologists and legal actors is fundamental to ensuring judicial effectiveness in the digital era. [15], [16].

GAPS IN FORENSIC INFRASTRUCTURE AND EXPERTISE

Inadequate Forensic Laboratories and Equipment

Despite India's progress in legislative reform, the forensic infrastructure remains grossly insufficient to meet the demands imposed by modern digital investigations. Many forensic laboratories lack advanced digital forensic tools and updated equipment necessary for the extraction, preservation, and analysis of complex electronic evidence. This insufficiency particularly affects regions outside metropolitan centres, creating regional disparities in forensic capability and thereby impacting the uniformity of justice delivery. The lag in infrastructure upgrading is reflective not only of limited funding but also of the slow pace of technological adoption in government agencies. Consequently, forensic investigations relying heavily on digital evidence face delays, compromised quality, and diminished effectiveness. Addressing this gap requires targeted investment in state-of-the-art forensic labs equipped with cutting-edge technologies that can handle diversified digital evidence efficiently. [17].

Lack of Specialized Cyber Forensic Training

Complementing physical infrastructure, the human capital dimension presents a significant challenge. There is an acute shortage of trained personnel possessing expertise in cyber forensics, digital evidence law, and technological investigation methods. This shortage impairs the quality of forensic processes and weakens the prosecution of cases reliant on digital evidence. Continuous capacity building through dedicated certification programs, workshops,

[15] J.F.M. Cruz, C.P.M. Davila, H.A.G. Laguna & E.J.G. Malaga, Innovative Management in the Legal World: Keys to Making the Right Decisions,https://doi.org/10.22373/petita.v10i2.834.
[16] V. Singh et al., Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, METALLURGICAL & MATERIALS ENG'G (2025), https://doi.org/10.63278/1383.
[17] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627.

and advanced training modules tailored for forensic scientists, law enforcement officers, and legal professionals is crucial. Upskilling efforts must keep pace with evolving technological landscapes to ensure personnel remain proficient in emerging tools and evidence types. Ultimately, increasing the availability of cyber forensic specialists strengthens the entire investigative ecosystem and bolsters confidence in digital adjudication. [18].

CHALLENGES IN CERTIFICATION AND AUTHENTICATION OF ELECTRONIC RECORD

Uniform Certification Processes Under BSA

Section 63 of the BSA establishes a framework for the expert certification of electronic records, yet practical challenges persist in achieving uniformity and consistency in certification processes. Variability in expert qualifications, divergent authentication practices across jurisdictions, and inconsistencies in procedural implementation undermine the credibility and acceptance of certified digital evidence. These disparities result in uneven courtroom experiences and may cause admissibility disputes. Moreover, the evolving nature of electronic evidence types demands adaptive certification protocols that can accommodate diverse record formats and origins without compromising legal standards. Thus, the uniform application and enforcement of Section 63 provisions remain a critical area necessitating further policy enhancement and operational guidance to support judicial reliability. [19].

Judicial Interpretation and Case Law Trends

Judicial interpretations of electronic evidence under analogous provisions to Sections 65A and 65B, which relate closely to the BSA's approach, have significantly influenced the evidentiary landscape in India. Courts have grappled with setting evidentiary thresholds, balancing technical authenticity with procedural fairness. While some rulings have adopted progressive stances recognizing the validity of electronic records with expert certification, others have exhibited caution, emphasizing stringent standards to preclude tampering and unreliable data. This inconsistency underscores the ongoing evolution of case law, wherein judicial actors

[18] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES.
(2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627
[19] V. Singh et al., "Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023," Metallurgical & Materials Engineering, 2025. https://doi.org/10.63278/1383

continuously adapt to the complexities of digital evidence. The dynamic jurisprudence highlights the critical role of judicial education and consistent legal frameworks to harmonize interpretations and foster predictability in electronic evidence admissibility. [20].

PRIVACY AND ETHICAL CONSIDERATIONS

Digital investigations often entail intrusions into highly sensitive personal information, raising profound concerns about privacy and civil liberties. The collection and examination of electronic evidence must navigate the tension between effective law enforcement and the right to privacy guaranteed by constitutional and human rights principles. The BSA and related statutes currently lack sufficiently explicit provisions to safeguard privacy during digital evidence acquisition, potentially leading to excessive surveillance or infringement on personal data rights. Transparent and well-defined protocols are necessary to ensure that investigation strategies respect privacy norms, limit data collection to relevant information, and prevent misuse. Such safeguards help maintain public trust in legal institutions and ensure that the deployment of digital forensic powers does not undermine democratic freedoms.[21]

Cybercrime Investigations and Ethical Constraints

The rise of cybercrime has situationally challenged ethical boundaries in investigative techniques. The use of AI and automated tools in evidence collection, while enhancing efficiency, introduces dilemmas related to bias, consent, and the extent of surveillance. Ethical frameworks must guide how such technologies are deployed to prevent overreach, unjust profiling, or the erosion of procedural fairness. Investigators and forensic specialists require clear ethical guidelines that align with human rights considerations, ensuring that the pursuit of cyber justice does not compromise foundational legal principles. Moreover, transparency in investigative methods and accountability mechanisms remains essential to uphold the legitimacy of cybercrime prosecutions reliant on complex digital evidence. [22].

[20] N.K. Bharti & N. Gupta, Admissibility of Electronic Evidence in India: Legal Framework, Judicial Trends, and the Impact of the Bharatiya Sakshya Sanhita, 2023, INT'L J. MULTIDISCIPLINARY RES. (2025), https://doi.org/10.36948/ijfmr.2025.v07i04.54750.
[21] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES. (2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627
[22] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES. (2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627

TECHNOLOGICAL INNOVATION AND ITS LEGAL IMPLICATIONS

Technological innovations such as blockchain, artificial intelligence (AI), and big data analytics offer promising avenues to enhance the accuracy, reliability, and efficiency of digital evidence management. Blockchain's distributed ledger technology can provide tamper-evident audit trails that strengthen evidence authenticity. AI-powered predictive models assist judicial decision-making by analysing patterns, assessing risks, and forecasting case outcomes, thereby supporting judicial efficiency and transparency. Big data analytics facilitates the synthesis of complex datasets, enabling more comprehensive investigations and evidentiary insights. Additionally, collaborative digital platforms streamline communication and workflow among legal stakeholders, expediting case processing. The integration of these technologies aligns with the BSA's modernization goals and amplifies its potential impact when coupled with appropriate legal safeguards. [23].

POLICY AND IMPLEMENTATION CHALLENGES

Infrastructure and Resource Allocation Deficits

One of the most pressing challenges hindering the comprehensive implementation of the BSA provisions is the shortfall in adequate funding and resources dedicated to forensic laboratories and digital tools. This deficit sharply contrasts between urban centres, which often have access to modern facilities, and rural or marginalized regions that struggle with minimal infrastructure. Such disparities not only impede the uniform application of digital evidence standards but also risk creating systemic inequities in access to justice. Addressing these imbalances demands dedicated policy focus and increased budgetary allocations to build and maintain forensic facilities, invest in digital investigative tools, and upgrade technological infrastructure countrywide. [24], [25].

Coordination Across Legal and Technological Stakeholders

Effective digital evidence handling under the BSA requires seamless coordination and

[23] J.F.M. Cruz, C.P.M. Davila, H.A.G. Laguna & E.J.G. Malaga, Innovative Management in the Legal World: Keys to Making the Right Decisions, PETITA JURNAL KAJIAN ILMU HUKUM DAN SYARIAH (2025), https://doi.org/10.22373/petita.v10i2.834

[24] V. Singh et al., Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, METALLURGICAL & MATERIALS ENG'G (2025), https://doi.org/10.63278/1383.

[25] S. Singh & S. Pandey, The Evolving Cybercrime Landscape in India: Legal Challenges, Digital Evidence, and New Criminal Laws, INT'L J. MULTIDISCIPLINARY RES. (2025), https://doi.org/10.36948/ijfmr.2025.v07i02.41627.

collaboration between multiple stakeholders, including legal professionals, forensic experts, technologists, law enforcement agencies, and policymakers. Challenges persist in fostering interdisciplinary dialogue, aligning priorities, and integrating disparate expertise within investigative and judicial processes. The complexity of cyber investigations often necessitates multi-agency cooperation that may be hampered by bureaucratic silos, inconsistent protocols, and communication gaps. Establishing institutional frameworks that promote cross-sector collaboration, information sharing, and joint training initiatives is vital for the successful integration of technological tools into legal workflows. These collaborative models facilitate a holistic and informed approach to digital evidence management. [26].

CONCLUSION

This analysis reveals several critical deficiencies in the handling of digital evidence under the Bharatiya Sakshya Adhiniyam, 2023. Infrastructural gaps, including insufficient forensic laboratories and limited regional capabilities, constrain the practical application of the Act's provisions. Procedural challenges persist in evidence collection, preservation, chain of custody, and certification due to a lack of uniform standards and judicial expertise. Privacy concerns and jurisdictional uncertainties add layers of complexity in evidence acquisition and admissibility. While the BSA establishes a modern legal foundation, practical and technological constraints impede the realization of its full potential, underscoring systemic weaknesses requiring urgent attention

To overcome these challenges, strategic investments are essential in developing forensic infrastructure and cyber forensic capacity nationwide. Judicial training programs must be designed and implemented to enhance the technology literacy among people related to the judicial environment. Additionally, adoption of advanced technological tools such as blockchain, AI, and PDFI should be pursued alongside the establishment of clear legal and procedural safeguards. These targeted measures collectively can bridge the existing divide, fostering an efficient, transparent, and technologically competent judicial system.

[26] J.F.M. Cruz, C.P.M. Davila, H.A.G. Laguna & E.J.G. Malaga, Innovative Management in the Legal World: Keys to Making the Right Decisions, PETITA JURNAL KAJIAN ILMU HUKUM DAN SYARIAH (2025), https://doi.org/10.22373/petita.v10i2.834.