International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Admissibility of Digital Forensic Evidence Under the Bharatiya Sakshya Adhiniyam, 2023: Legal and Investigative Challenges for Law Enforcement

Abida S Laskar[1], Dr. Kuntala Roychoudhury[2], Dr. Lairenjam Dhanamanjuri Devi[3]

[1]Research Scholar, Royal School of Law and Administration, The Assam Royal Global University
[2]Assistant Professor, Royal School of Law and Administration, The Assam Royal Global University
[3]Assistant Professor, B.R.M. Govt. Law College, Guwahati

Abstract
The rapid expansion of digital technologies has reshaped the landscape of criminal activity as well as criminal investigation, making digital forensic evidence increasingly central to the administration of justice. Recognising this transformation, India enacted the Bharatiya Sakshya Adhiniyam, 2023 (BSA), replacing the Indian Evidence Act, 1872, and introducing a modern framework that explicitly acknowledges the evidentiary value of electronic records. Against this backdrop, this paper explores the admissibility of digital forensic evidence under the BSA and examines the practical challenges faced by investigators, forensic experts, and courts in handling such evidence. The study adopts a doctrinal research approach, analysing statutory provisions, judicial pronouncements, and procedural safeguards governing electronic evidence. It focuses particularly on issues such as authenticity, integrity, chain of custody, certification requirements, and the complexities involved in accessing cross-border digital data. While the BSA represents a progressive step toward aligning India's evidentiary law with technological advancements, the paper argues that legislative reform alone is insufficient. Persistent gaps in infrastructure, technical expertise, and institutional coordination continue to hinder the effective use of digital forensic evidence in criminal proceedings. The paper concludes by recommending practical reforms aimed at strengthening investigative capacity, improving forensic infrastructure, and ensuring greater reliability in the use of digital evidence within India's evolving criminal justice system.

Keywords: Digital Forensic Evidence, Bharatiya Sakshya Adhiniyam 2023, Electronic Records, Chain of Custody, Admissibility, Cybercrime Investigation, Indian Evidence Law.

1. Introduction

A smartphone is a powerful witness in modern criminal trials. It does not have memory or emotion like a human. It silently remembers places, call logs, texts, photos, and web history, often creating a full timeline of events without knowing how important it is in court. For investigators and prosecutors, this makes digital proof strong and often indispensable.[1] At the same time, for defence lawyers, judges, and rights

groups, this use raises fundamental questions about how data is gathered, whether the data is genuine, and whether people's rights are protected in the process.[2]

India's criminal justice system has been slow to grapple with these questions at a systemic level. The Indian Evidence Act, 1872[3] — a statute drafted for a world of paper documents and oral testimony — was amended in 2000 with Sections 65A and 65B to accommodate computer-generated records.[4] The amendment was imperfect. Courts spent two decades arguing about what Section 65B required, who could certify what, and when the rule could be relaxed. The Supreme Court's rulings in *Anvar P.V. v. P.K. Basheer*[5] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[6] clarified some questions but opened others. Prosecutors lost cases on technicalities. Investigators grew confused about what procedures to follow.

Against this backdrop, the Bharatiya Sakshya Adhiniyam, 2023,[7] arrives as India's most significant reform of evidence law since Independence. It elevates electronic records to primary evidence status, broadens definitions to accommodate contemporary digital devices, and attempts to rationalise the certification requirements that plagued the earlier regime. Whether it genuinely solves the problem, or merely restates it in more modern language, is the central question this paper seeks to answer.

The argument advanced here is that the BSA is a necessary but insufficient step. Its real-world effectiveness depends on a chain of institutional capacities — forensic laboratories, trained investigators, judicial understanding of technical evidence, international data-sharing agreements — that remain seriously underdeveloped. Getting the statute right matters, but it is only the beginning of the work that needs to be done.

2. What we mean by Digital Forensic Evidence

Digital evidence is information stored or transmitted in an electronic form that may be used during investigations or judicial proceedings. This evidence can be extracted from computers and laptops, mobile phones and tablets, servers and databases, cloud storage systems, Internet of Things (IoT) devices, CCTV footage, social media platforms, emails, and instant messaging applications.[8] Unlike traditional forms of evidence, digital evidence is intangible and easily alterable; it often requires special tools and technical knowledge for recovery and analysis.

2.1 The Distinctive Character of Digital Data

Digital evidence is both more powerful and more fragile than it first appears. More powerful, because it is pervasive — virtually every interaction with a modern device generates data, and that data often persists long after the user believes it has been erased.[9] More fragile, because it can be altered without notice, copied unnoticed, moved across borders instantly, and destroyed simply by switching on a device without forensic precautions.

What makes digital evidence legally distinctive is not merely its technical complexity but the ease with which its integrity can be compromised. A document found at a crime scene can be examined for fingerprints, ink composition, and physical characteristics that establish authenticity. A digital file carries no such natural authentication marks. Metadata — the data about data, including file creation times, modification records, and access logs — can be altered by freely available tools, and courts without forensic guidance may have no means of detecting such manipulation.[10]

2.2 The Forensic Science Behind the Evidence

Digital forensics is the discipline that bridges the gap between raw data and courtroom-ready evidence. The discipline rests on a foundation of international standards — notably ISO/IEC 27037 on digital

evidence identification and collection,[11] and the frameworks developed by the Scientific Working Group on Digital Evidence (SWGDE)[12] — that specify how evidence should be identified, acquired, preserved, analysed, and reported. These standards exist because experience has demonstrated, repeatedly, that well-intentioned investigators acting without standardised procedures can inadvertently compromise the very evidence they are trying to preserve.

In India, compliance with these standards varies widely. Some state forensic laboratories follow rigorous procedures; others operate without formal protocols.[13] This inconsistency is not a minor administrative problem — it is a fundamental challenge to the reliability of digital evidence in Indian courts.

2.3 Why It Matters: The Breadth of Digital Crime

The significance of digital forensic evidence extends far beyond what is conventionally described as 'cybercrime.' Offences such as phishing, identity theft, ransomware, online fraud, and unauthorised computer access are inherently digital in character. But drug trafficking syndicates communicating over encrypted messaging applications, terror organisations recruiting through social media, human traffickers advertising on dark web forums, and financial criminals moving money through cryptocurrency exchanges are equally dependent on digital infrastructure that leaves evidence trails.[14] Digital evidence has become applicable across the entire range of serious criminal conduct — not a specialist matter but an everyday investigative reality.

3. From the Indian Evidence Act to the Bharatiya Sakshya Adhiniyam: A Story of Incremental Reform

The transition from the Indian Evidence Act of 1872 to the Bharatiya Sakshya Adhiniyam of 2023 reflects a trend of gradual reform rather than an entirely new approach to India's rules of evidence. The Bharatiya Sakshya Adhiniyam consolidates earlier incremental developments and places them within a single, coherent system that formally recognises electronic records, digital signatures, and forensic evidence as central components of modern criminal adjudication.

3.1 The Limitations of Sections 65A and 65B

When Parliament inserted Sections 65A and 65B into the Indian Evidence Act in 2000, it was attempting something genuinely innovative for the time: creating a statutory framework for computer-generated evidence that insisted on a degree of procedural accountability before such evidence could be admitted.[15] The requirement of a certificate under Section 65B(4), attesting to matters relating to the relevant computer's operation, the manner of data input, and the accuracy of the output, was designed to ensure that courts were not simply taking the authenticity of digital records on faith.

The problem was that the provision was drafted with more optimism than precision. It assumed that the party seeking to introduce electronic evidence would be in a position to obtain a certificate from the person responsible for the relevant computer — an assumption that frequently failed in criminal cases where the evidence had been extracted from a suspect's device, or where servers were controlled by third parties, or where the relevant records came from systems managed by foreign entities over which Indian law had no direct reach.

Courts responded to these difficulties with interpretive ingenuity, but the results were inconsistent. Some judges took a strict view of the certificate requirement and excluded electronic evidence when certificates were absent or imperfect. Others were more flexible, admitting evidence on the basis of oral testimony about its provenance. The result was a patchwork jurisprudence that left investigators and prosecutors uncertain about what was required of them.

3.2 The Supreme Court's Clarifications and Their Limits

The Supreme Court's ruling in *Anvar P.V. v. P.K. Basheer*[16] was meant to clear the fog around electronic evidence admissibility. A Constitution Bench held unequivocally that Section 65B is a complete code for proving electronic records and that a certificate under Section 65B(4) is a mandatory precondition for admissibility — not a procedural formality that courts could choose to ignore. The Court expressly overruled *State (NCT of Delhi) v. Navjot Sandhu*[17], which had allowed electronic evidence to be admitted through secondary evidence provisions, thereby bypassing the certificate requirement entirely.

Although doctrinally coherent, this ruling failed to account for the practical conditions of criminal investigation in India. These problems were most clearly seen in prosecutions before the Gauhati High Court, where insurgency-related offences, organised crime, and cross-border networks often depended on call detail records, intercepted communications, and mobile device data.[18] Trial courts in Assam similarly faced difficulties regarding the authenticity of WhatsApp chat screenshots and digital payment records — problems that matched what the Supreme Court noted in *Tomaso Bruno v. State of Uttar Pradesh*[19], where failure to produce available electronic evidence could lead to adverse inferences against the prosecution.

The Supreme Court revisited the issue in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[20], seeking to rebalance the equation. The Court clarified that a judge may compel production of the certificate under procedural powers, and that the requirement may be relaxed where the original device is produced before the court. It also, in effect, overruled the flexibility introduced in *Shafhi Mohammad v. State of Himachal Pradesh*[21]. Yet practical difficulties persist, especially in Assam, where devices seized in remote districts must be transported to the Assam Forensic Science Laboratory in Guwahati for analysis.[22] The jurisprudence continues to evolve as courts across the Northeast strive to reconcile procedural rigour with the practicalities of digital investigation.

4. The Bharatiya Sakshya Adhiniyam, 2023: Reform and its Residual Gaps

4.1 What the New Law Gets Right

The BSA represents a genuine improvement over what it replaces, and it would be unfair not to acknowledge this clearly. The elevation of electronic records to the status of primary evidence[23] is both symbolically and practically significant. It signals that digital data is no longer a special or suspect category of evidence requiring extraordinary procedural treatment, but a normal form of proof that courts should be as comfortable with as they are with paper documents.

The BSA's definition of 'electronic record'[24] is considerably broader than what the amended Indian Evidence Act contemplated, encompassing the full range of devices and storage environments that contemporary investigators encounter. Explicit provisions for electronic signatures[25] and electronic communications reduce the scope for definitional disputes that consumed considerable judicial energy under the earlier law. The treatment of audio-visual records — CCTV footage, call recordings, digital photographs — as documents within the broader framework of electronic records is a welcome and practical clarification.[26]

4.2 What the New Law Leaves Unaddressed

For all its improvements, the BSA does not resolve the most difficult practical challenges in digital evidence law. The certificate requirement persists in modified form,[27] and the conditions under which it can be waived remain subject to judicial interpretation. More fundamentally, the Act says nothing about how digital evidence should be collected, preserved, or analysed — it addresses admissibility in court but is silent about the forensic process that must precede the courtroom stage.

This is a significant omission. The admissibility of digital evidence depends not merely on a statutory certificate but on the integrity of the entire forensic chain — from the moment of seizure to the moment of presentation. A certificate is only as meaningful as the reliability of the process it certifies. If that process has been compromised by improper handling, inadequate preservation, or flawed analysis, the certificate becomes a formal gesture rather than a substantive guarantee.

The BSA also does not engage with the cross-border dimension of digital evidence — a dimension that has become increasingly central to serious criminal investigation as data storage has migrated to the cloud and communication has moved to platforms owned and operated by entities incorporated in foreign jurisdictions. The challenge of obtaining data from a Google server in California or a Meta server in Ireland is not a statutory problem that the BSA can solve, but its absence from the Act's framework means that investigators and courts are left without guidance on how to handle evidence obtained through international cooperation mechanisms.

5. The Forensic Process: What Admissibility Actually Requires

Understanding why digital forensic evidence so often becomes contested in court requires understanding what a sound forensic investigation actually involves. Each stage of the forensic workflow has legal implications, and failure at any stage can undermine the admissibility or weight of the evidence that emerges.[28]

Identification

The investigator must first identify all potential sources of relevant digital evidence — which may include not only obvious sources like a seized mobile phone or laptop, but also cloud accounts, backup services, data synchronised to other devices, and metadata held by service providers.[29] An investigator who seizes a smartphone but fails to issue a preservation request to the associated messaging platform may lose irreplaceable evidence within days, as data retention policies are applied automatically.

Acquisition

Acquisition is the most technically critical stage. Standard practice requires the creation of a bit-for-bit forensic image of the original storage medium using write-blocking hardware or software, ensuring that the original data is not altered by the imaging process itself.[30] Cryptographic hash values — typically MD5 or SHA-256 — are calculated for both the original and the image to create a mathematical fingerprint that enables verification of integrity at any subsequent point. Any deviation from these procedures creates a vulnerability that a skilled defence lawyer can and will exploit.

Preservation and Chain of Custody

Once acquired, evidence must be preserved in conditions that prevent accidental or deliberate alteration, and its movement and handling must be documented with precision. The chain of custody record — who had the evidence, when, in what circumstances, and what they did with it — is the mechanism by which a court can be satisfied that the evidence presented to it is the same evidence recovered from the source, unchanged.[31] Gaps or inconsistencies in the chain of custody record are among the most common grounds on which digital evidence is challenged in Indian proceedings.[32]

Analysis and Reporting

Forensic analysis involves the systematic examination of acquired evidence to extract relevant data, recover deleted files, reconstruct timelines, and identify digital artefacts of probative value. The methodology used must be documented, repeatable, and capable of independent verification. The findings

must then be reported in a form that is scientifically accurate and legally intelligible, and the examiner must be prepared to defend both methodology and conclusions under cross-examination.

6. The Challenges: Where Theory Meets Practice

Having described what a sound forensic process looks like in principle, it is necessary to confront the gap between that description and the reality that most Indian criminal courts actually encounter. The challenges are not merely technical — they are institutional, legal, and in some cases, constitutional. They interact with each other in ways that make simple solutions elusive.

6.1 The Problem of Authenticity: Can Courts Trust What They See?

The most fundamental question for a court when confronted with digital evidence is whether the data before it accurately represents what actually happened. Digital files carry no inherent authentication marks — a JPEG photograph does not announce whether it has been edited; a WhatsApp message does not reveal whether its timestamp has been altered; a spreadsheet does not disclose whether rows have been added or deleted after the fact. Metadata offers some authentication possibilities, but metadata can also be manipulated, and its manipulation is not always detectable.[33]

Courts that lack access to independent forensic expertise must largely take the presenting party's word for the authenticity of digital evidence. This is a structurally unsatisfactory position. The appointment of court-appointed forensic experts is rare in India,[34] and the judiciary's general technical literacy on digital matters, while improving, remains uneven. The result is that the reliability of digital evidence is sometimes evaluated by judges who are not in a position to ask, let alone answer, the right questions about how it was obtained and whether it has been compromised.[35]

6.2 Chain of Custody: The Weakest Link

In theory, maintaining a complete and documented chain of custody for digital evidence should be no more difficult than maintaining it for physical evidence. In practice, it proves considerably more problematic. Indian police forces do not uniformly follow standardised evidence handling procedures for digital materials. Seized devices may pass through multiple hands before reaching a forensic laboratory, with each transfer inadequately documented.

In Assam, devices seized in districts such as Karbi Anglong, Chirang, or Dhubri must be transported to the Assam Forensic Science Laboratory at Kahilipara, Guwahati — a journey that, without adequate procedural safeguards, creates multiple opportunities for chain of custody failure. Evidence may be stored without adequate protection against electromagnetic interference, physical damage, or unauthorised access. These failures have real consequences: courts have excluded digital evidence — and prosecutions have collapsed — because the chain of custody was too broken to sustain confidence in the evidence's integrity.

6.3 The Expertise Gap: What Happens When Investigators Do Not Know What They Are Doing

Perhaps the most pervasive challenge facing digital forensic evidence in Indian courts is the chronic shortage of adequately trained forensic investigators. This is not a criticism of individual officers — it is a structural observation about a system that has not invested proportionately in the specialist capacity that digital investigation requires.

The Assam Police's dedicated Cyber Crime Unit under the CID has improved capacity in Guwahati, but its reach remains concentrated in the state capital. Districts across the Northeast — particularly in remote and border areas — have minimal access to digital forensic support.[36] Investigators unfamiliar with forensic procedures may inadvertently alter evidence during seizure. Analysts working without validated

forensic tools may produce results that cannot be independently verified. Expert reports may overstate conclusions in ways that mislead rather than inform courts. When defence experts challenge such reports — as they increasingly do in high-stakes cases — prosecution forensic evidence can unravel.

The dependence on private forensic laboratories compounds the problem. Private labs vary enormously in competence, methodological rigour, and impartiality. Unlike government forensic laboratories, many private providers operate without formal accreditation, and courts have limited tools for evaluating the reliability of their procedures and conclusions.

6.4 The Missing Rulebook: No Uniform National Standards

Underlying many of these specific problems is a more fundamental structural gap: India has no nationally binding, legally enforceable set of standards governing the collection, preservation, and analysis of digital evidence by law enforcement. Guidance documents exist — the Ministry of Home Affairs has published manuals; CERT-In has issued advisories — but guidance is not law. Compliance is voluntary, and practice varies substantially across jurisdictions, agencies, and individual officers.[37]

This matters for admissibility in a particularly direct way. Courts assessing the reliability of digital forensic evidence need a reference point against which to evaluate the procedures followed by investigators. Without nationally recognised standards, courts must make these assessments on an ad hoc basis, relying on the expertise of whichever technical witnesses appear before them. This creates inconsistency, unpredictability, and — inevitably — injustice.

6.5 Cloud Data and Cross-Border Challenges: Evidence Beyond Reach

Consider a scenario that is far from hypothetical in Assam: a serious fraud conducted through emails hosted on a foreign server, cryptocurrency transfers recorded on a distributed blockchain, and coordination messages exchanged on an end-to-end encrypted platform headquartered abroad. Each of these evidence sources sits, in a meaningful legal sense, outside India's direct jurisdiction. Each requires a different set of legal tools to access.[38]

The cross-border dimension is particularly acute for Assam, given the state's international borders with Bangladesh and Bhutan, and its proximity to Myanmar. SIM card fraud networks operating across the Bangladesh border and investment scam syndicates traced to Myanmar-based operations have victimised residents across Assam, and the broader Northeast — yet the digital evidence needed to prosecute these cases frequently resides on servers in foreign jurisdictions.[39] The average MLAT request to the United States takes between six months and two years to process.[40] India has not yet acceded to the Budapest Convention on Cybercrime,[41] the primary multilateral framework for international cooperation in this area — leaving investigators without the expedited mechanisms that convention membership would provide.

6.6 Encryption: The Investigation that Hits a Wall

End-to-end encryption, increasingly deployed as a default feature of major communication platforms, creates a challenge that law enforcement agencies worldwide are struggling to address. When messages are encrypted end-to-end — as they are on WhatsApp, Signal, iMessage, and many other platforms — the service provider genuinely cannot read the content. An MLAT request for content data will be met with a legally accurate but operationally unhelpful response: the data exists, but it cannot be provided in readable form.[42]

Investigators then face a choice between technical solutions and legal arguments about whether suspects can be compelled to provide decryption keys or biometric access. The latter question is genuinely difficult under India's constitutional framework. The right against self-incrimination under Article 20(3) of the Constitution[43] creates uncertainty about the compellability of passwords and encryption keys. The

Supreme Court's landmark recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* adds further constitutional complexity. Any legislative solution to the encryption problem must be proportionate, subject to judicial oversight, and respectful of the privacy rights the Court has affirmed.

6.7 The Technology Moves Faster Than the Law

Courts and legislators everywhere are struggling to keep pace with technologies that generate new evidentiary challenges faster than legal frameworks can adapt. Three categories of evidence are increasingly relevant to Indian criminal investigations, but for which the existing legal framework provides no clear guidance.[44]

First, cryptocurrency transaction records: blockchain data is immutable in principle, but attributing a wallet address to a specific individual requires forensic techniques that differ substantially from conventional digital analysis. Second, AI-generated content: as machine learning tools become capable of generating convincingly realistic text, images, audio, and video, the risk of AI-assisted evidence fabrication grows correspondingly. Third, and most urgently in the Assam context, deepfake and morphed imagery: Assam has seen a significant number of registered cases involving morphed images of women circulated without consent, prosecuted under Section 66E of the Information Technology Act and Section 77 of the Bharatiya Nyaya Sanhita.[45] The evidentiary challenge of authenticating or disproving such imagery in court is directly relevant to this paper's concern with emerging technology challenges.[46]

6.8 Infrastructure: The Forensic Laboratory Crisis

Behind all these specific challenges lies a more basic material problem: India does not have enough digital forensic laboratories, and the ones it has are overwhelmed. The Assam Forensic Science Laboratory at Kahilipara, Guwahati, stands as a particularly clear illustration of this crisis — it is the sole accredited digital forensic facility serving the entire state of Assam, and also receives referrals from forensic units across several other Northeast Indian states.[47] The resulting backlog means that forensic examination reports may take months or years to arrive — delays that compromise both the efficiency of prosecution and the accused person's right to a speedy trial guaranteed under Article 21 of the Constitution.[48]

This is fundamentally a resource allocation problem, but also a priority problem. Investment in digital forensic infrastructure has not kept pace with the growth of digital crime.[49] The consequences are borne by victims who see offenders escape justice, and by accused persons who languish in custody while awaiting forensic reports that determine their guilt or innocence.[50]

7. What other jurisdictions can teach us?

7.1 The United States: Standards, Scrutiny, and the Daubert Gate

The United States has developed, over several decades, a sophisticated framework for evaluating the reliability of digital forensic evidence that Indian courts could learn from. At the heart of this framework is the *Daubert* standard for expert testimony,[51] which requires that expert evidence be grounded in reliable principles and methods, applied reliably to the facts of the case, and subject to meaningful scrutiny through cross-examination and opposing expert evidence.[52]

The National Institute of Standards and Technology (NIST) maintains a Computer Forensics Tool Testing programme that provides independent validation data for commonly used forensic software — data that courts can reference when evaluating whether a particular analysis was conducted reliably.[53] The United States also provides, through the CLOUD Act, a legal framework for cross-border data access that enables executive agreements between the US and partner nations to streamline the process of obtaining digital

evidence from American-based providers.[54] India has not yet concluded such an agreement, limiting its ability to access data from US-based platforms that are central to many serious criminal investigations.

7.2 The United Kingdom: Accreditation, Oversight, and the Regulator

The United Kingdom's approach is notable for its institutional architecture. The Forensic Science Regulator has developed Codes of Practice that specify the standards to which digital forensic providers — government and private alike — must adhere.[55] The College of Policing's Authorised Professional Practice guidance provides operational standards for digital evidence handling by police forces.[56] The combination of regulatory oversight of forensic providers and operational guidance for investigators creates a coherent quality assurance architecture that India currently lacks.

The UK's previous adherence to the Budapest Convention on Cybercrime[57] facilitated efficient cross-border digital evidence access — a model with considerable relevance for India's current position outside that convention framework.

7.3 The Implications for India

The comparative picture suggests that what India needs is not primarily a different statute — the BSA provides a reasonable legislative foundation — but a set of institutional structures that mature jurisdictions have developed: legally binding forensic standards with independent oversight; a framework for court-appointed technical experts; a credible mechanism for cross-border data access; and sustained investment in forensic science training and infrastructure.

8. A Path Forward: Recommendations for Reform

The reforms needed are interconnected, and piecemeal approaches will not suffice. What is required is a coordinated programme that addresses legislative gaps, institutional deficiencies, and capacity constraints simultaneously.

8.1 Enact Legally Binding Forensic Standards

The most urgent reform priority is the development and statutory enactment of national standards governing the collection, preservation, and analysis of digital evidence by law enforcement agencies. These standards should be aligned with internationally recognised frameworks such as ISO/IEC 27037 and should specify minimum requirements for forensic equipment, analytical methodology, chain of custody documentation, and examiner qualifications. Crucially, they should be legally enforceable — not merely advisory — and compliance with them should be treated by courts as a relevant factor in assessing the admissibility and weight of digital forensic evidence.

8.2 Invest Seriously in Forensic Capacity

The expansion and upgrading of India's digital forensic laboratory network must be treated as a criminal justice priority. This means dedicated funding for new laboratory facilities in underserved regions — with particular attention to the Northeast, where the Assam FSL at Kahilipara currently serves as the sole accredited facility for multiple states — regular renewal of forensic software and hardware, competitive remuneration for trained forensic personnel, and a national training programme for digital forensic investigators that is mandatory, standardised across police forces, and regularly updated to reflect evolving technology.

8.3 Build the Cross-Border Architecture

India should prioritise accession to the Budapest Convention on Cybercrime,[58] which would provide a multilateral framework for expedited cross-border digital evidence access. Separately, negotiations should be pursued with major data-holding jurisdictions toward bilateral data access agreements modelled on the

CLOUD Act framework.[59] This is particularly urgent for Assam and the Northeast, given the documented involvement of cross-border criminal networks in cybercrimes affecting the region.

8.4 Address Encryption Proportionately

Parliament should develop a clear, proportionate, and constitutionally compliant framework for compelling access to encrypted data in the context of serious criminal investigations, subject to prior judicial authorisation and independent oversight.[60] The framework should be explicitly designed in light of the Supreme Court's privacy jurisprudence in *Puttaswamy*[61] and should respect the constitutional protection against self-incrimination under Article 20(3).[62]

8.5 Build Judicial Capacity

The judiciary cannot fairly evaluate digital forensic evidence without a basic understanding of the technical processes that produce it. Structured training programmes on digital evidence should be made available through the National Judicial Academy and state judicial academies on a regular and systematic basis.[63] Courts handling significant digital evidence should have access to court-appointed technical experts who can assist in evaluating forensic methodology and interpreting technical findings.[64]

8.6 Legislate for Emerging Technologies

The BSA should be supplemented with specific frameworks for the admissibility and authentication of AI-generated content, deepfake media, blockchain records, and other categories of digital evidence that existing provisions are ill-equipped to address.[65] This is especially important in the context of morphed and deepfake image cases that have already been prosecuted in Assam courts,[66] where the absence of specific authentication standards places an unfair burden on both investigators and the judiciary.

9. Conclusion

In February 2021, Assam Police conducted a state-wide crackdown on cyber fraud networks, resulting in over 800 arrests.[67] That operation generated an enormous volume of seized digital devices. The subsequent prosecutorial challenge — converting those seizures into admissible, reliable evidence before courts — illustrated, in concentrated and local form, virtually every challenge this paper identifies.

There is a temptation to evaluate the Bharatiya Sakshya Adhiniyam, 2023,[68] against the Indian Evidence Act, 1872,[69] and conclude that things are considerably better — and, in formal terms, they are. The BSA is a more modern statute, better adapted to the evidentiary realities of the digital age, and it corrects genuine deficiencies in the framework it replaces. These are real achievements, and they matter.

But the more important evaluation is not the comparison with the past; it is the comparison with what effective digital criminal justice actually requires. Measured against that standard, the BSA is necessary but not sufficient. It provides a better statutory foundation, but the building that needs to be constructed on that foundation — in terms of forensic capacity, institutional standards, cross-border cooperation, judicial training, and constitutional balance — is largely still to be built.

The challenges documented in this paper are not simply technical problems waiting for technological solutions. They reflect choices about resource allocation, institutional design, and political priority. The decision to invest adequately in digital forensic laboratories, to train investigators rigorously, to accede to the Budapest Convention,[70] to develop a coherent encryption framework — these are choices that governments make or fail to make, with real consequences for the people who pass through the criminal justice system on both sides of the courtroom.

What gives these choices urgency is the trajectory of digital crime. The volume, sophistication, and transnational reach of offences that depend on digital evidence are growing faster than the institutional

capacity to investigate and prosecute them.[71] If that gap is not closed, the risk is not merely that prosecutions will fail. It is that the criminal justice system will simply cease to be credible in the domains where digital evidence is most relevant. That would be a failure not just of law enforcement or evidentiary procedure. It would be a failure of justice — and one that India's new evidentiary framework, however well drafted, cannot by itself prevent.[72]

REFERENCES

A. Statutes and Legislation

1. Bharatiya Sakshya Adhiniyam, No. 46 of 2023 (India).
2. Indian Evidence Act, No. 1 of 1872 (India).
3. Information Technology Act, No. 21 of 2000, §§ 65A–65B (India).
4. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77 (India).
5. Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023 (India).
6. India Const. arts. 20(3), 21.
7. Investigatory Powers Act 2016, c. 25 (U.K.).
8. Fed. R. Evid. 702 (U.S.).
9. Stored Communications Act, 18 U.S.C. §§ 2701–2713 (U.S.).
10. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523 (2018) (U.S.).

B. Cases

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
3. State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, (2005) 11 SCC 600 (India).
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
5. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178 (India).
6. Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570 (India).
7. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (India).
8. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993) (U.S.).

C. Books and Monographs

1. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3d ed. 2011).
2. Brian Carrier, File System Forensic Analysis (2005).
3. Bill Nelson, Amelia Phillips & Christopher Steuart, Guide to Computer Forensics and Investigations (6th ed. 2019).
4. Stephen Mason, Electronic Evidence (4th ed. 2017).
5. Kathryn Nance & Dennis Ryan, Legal Principles of Digital Forensics (2011).

D. Journal Articles

1. Simson L. Garfinkel, Digital Forensics Research: The Next 10 Years, 7 Digital Investigation S64 (2010).
2. Mark Reith, Clint Carr & Gregg Gunsch, An Examination of Digital Forensic Models, 1(3) Int'l J. Digital Evidence (2002).
3. Michael Losavio et al., The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy, and Security, 14 Security & Commc'n Networks (2018).

4. Vinod Barayumureeba & Florence Tushabe, The Enhanced Digital Investigation Process Model, 4(1) Int'l J. Digital Evidence (2004).

E. Official Reports, Treaties, and Standards

1. ISO/IEC 27037:2012, Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (Int'l Org. for Standardization 2012).
2. Scientific Working Group on Digital Evidence (SWGDE), Best Practices for Computer Forensics, Version 3.1 (2014).
3. Nat'l Inst. of Standards & Tech., Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1 (2014).
4. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, CETS No. 185.
5. Ministry of Home Affairs, Gov't of India, Cybercrime Investigation Manual (Bureau of Police Rsch. & Dev. 2022).
6. National Crime Records Bureau, Crime in India 2022 (Ministry of Home Affairs 2023).
7. Forensic Science Regulator, Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System, FSR-C-100 (3d ed. 2021) (U.K.).
8. College of Policing, Authorised Professional Practice: Digital Forensics (2020) (U.K.).
9. Law Commission of India, Report No. 269: Amendments to the Information Technology Act, 2000 (2017).

F. Regional Sources (Assam)

1. Assam Police, Crime in Assam: Annual Report 2021–22 (Crim. Investigation Dep't, Assam 2022).
2. Assam Police, Cyber Crime Unit, CID Assam: Organisational Overview and Case Statistics 2022.
3. Assam Police, Report on Cross-Border Cybercrime Operations 2020–22 (CID, Assam 2022).
4. Assam Forensic Science Laboratory, Annual Statistical Report 2021–22 (Kahilipara, Guwahati).
5. Assam Police, CID Annual Cybercrime Report 2022–23.

---

1. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet 3 (3d ed. 2011).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
3. Indian Evidence Act, No. 1 of 1872 (India).
4. Information Technology Act, No. 21 of 2000, §§ 65A–65B (India) (amending the Indian Evidence Act, 1872).
5. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
6. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
7. Bharatiya Sakshya Adhiniyam, No. 46 of 2023, § 1 (India).
8. Bill Nelson, Amelia Phillips & Christopher Steuart, Guide to Computer Forensics and Investigations 12–15 (6th ed. 2019).
9. Casey, supra note 6, at 47–52.
10. Mark Reith, Clint Carr & Gregg Gunsch, An Examination of Digital Forensic Models, 1(3) Int'l J. Digital Evidence (2002).
11. ISO/IEC 27037:2012, Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (Int'l Org. for Standardization 2012).
12. Scientific Working Group on Digital Evidence (SWGDE), Best Practices for Computer Forensics, Version 3.1 (2014).
13. Ministry of Home Affairs, Gov't of India, Cybercrime Investigation Manual 22–28 (Bureau of Police Rsch. & Dev. 2022).
14. National Crime Records Bureau, Crime in India 2022, at 214–218 (Ministry of Home Affairs 2023) (documenting rising cybercrime registrations with limited conviction rates attributable in part to forensic evidence deficiencies).
15. Indian Evidence Act, No. 1 of 1872, §§ 65A–65B (India) (as amended by Information Technology Act, 2000).
16. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, ¶¶ 24–28 (India).
17. State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, (2005) 11 SCC 600 (India).

18. Assam Police, Crime in Assam: Annual Report 2021–22, at 34–38 (Crim. Investigation Dep't, Assam 2022) (on file with authors).
19. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178 (India).
20. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, ¶¶ 60–65 (India).
21. Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (India).
22. Assam Forensic Science Laboratory, Annual Statistical Report 2021–22 (Kahilipara, Guwahati) (on file with authors) (reporting significant case backlog in digital forensic examination queue).
23. Id. §§ 57–63 (provisions governing electronic records as primary evidence).
24. Bharatiya Sakshya Adhiniyam, No. 46 of 1872, § 2(1)(t) (India).
25. Id. § 81 (electronic signatures).
26. Stephen Mason, Electronic Evidence ¶¶ 3.01–3.15 (4th ed. 2017).
27. Bharatiya Sakshya Adhiniyam, No. 46 of 2023, § 63 (India) (certificate requirements).
28. Brian Carrier, File System Forensic Analysis 17–22 (2005).
29. Nelson et al., supra note 9, at 45–60.
30. ISO/IEC 27037:2012, supra note 7, §§ 5.3–5.5.
31. Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570, ¶ 18 (India) (noting evidentiary risks arising from gaps in chain of custody documentation).
32. Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570 (India).
33. Anvar P.V., (2014) 10 SCC 473, ¶ 15 (India).
34. Ministry of Home Affairs, supra note 30, at 14–16.
35. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178, ¶ 22 (India).
36. Assam Police, Cyber Crime Unit, CID Assam: Organisational Overview and Case Statistics 2022, at 7 (on file with authors) (noting that dedicated digital forensic support is concentrated in Guwahati, with districts such as Karbi Anglong, Chirang, and Dhubri substantially underserved).
37. Ministry of Home Affairs, supra note 30, at 18.
38. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523 (2018).
39. Assam Police, Report on Cross-Border Cybercrime Operations 2020–22, at 5–8 (CID, Assam 2022) (on file with authors) (documenting SIM card fraud networks operating across the Bangladesh border and investment scam syndicates traced to Myanmar, victimising residents across Assam and the broader Northeast region).
40. Budapest Convention, supra note 40, arts. 29–35 (expedited preservation and disclosure procedures).
41. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, CETS No. 185 [hereinafter Budapest Convention].
42. Puttaswamy, (2017) 10 SCC 1, ¶¶ 180–200 (Chandrachud, J., concurring) (articulating a proportionality framework for limitations on the right to privacy).
43. India Const. art. 20, § 3 (protection against self-incrimination).
44. Simson L. Garfinkel, Digital Forensics Research: The Next 10 Years, 7 Digital Investigation S64, S66–S68 (2010).
45. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77 (India) (offences relating to publication of obscene or morphed images of women); Information Technology Act, No. 21 of 2000, § 66E (India) (punishment for violation of privacy).
46. Assam Police, CID Annual Cybercrime Report 2022–23, at 19–22 (on file with authors) (documenting registered cases involving morphed and AI-altered images, primarily targeting women, prosecuted under § 66E IT Act and relevant IPC provisions before Assam trial courts).
47. Assam Forensic Science Laboratory, supra note 32 (the FSL at Kahilipara, Guwahati is the sole accredited digital forensic facility serving Assam, and receives referrals from forensic units across Northeast India including Meghalaya, Nagaland, Mizoram, and Tripura).
48. National Crime Records Bureau, supra note 37, at 222 (noting that prolonged forensic examination delays contribute to trial delays and affect the right to speedy trial under Article 21 of the Constitution).
49. Assam Police, supra note 43, at 3 (noting that the 2021 Assam-wide crackdown on cyber fraud networks resulted in over 800 arrests, generating a correspondingly large volume of seized digital devices requiring forensic examination and ultimately presenting significant challenges for prosecution).
50. India Const. art. 21 (right to life and personal liberty, interpreted to include privacy and the right to a speedy trial).
51. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
52. Fed. R. Evid. 702.

53. Nat'l Inst. of Standards & Tech., Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1, at 2–4 (2014).
54. CLOUD Act, 18 U.S.C. § 2523 (2018).
55. Forensic Science Regulator, Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System, FSR-C-100 (3d ed. 2021) (U.K.).
56. College of Policing, Authorised Professional Practice: Digital Forensics § 3.2 (2020) (U.K.).
57. Budapest Convention, supra note 40, art. 1 (scope of cooperation obligations).
58. Budapest Convention, supra note 40, arts. 23–35.
59. CLOUD Act, 18 U.S.C. § 2523(b)(1) (framework for executive agreements with foreign partners).
60. Puttaswamy, (2017) 10 SCC 1, ¶¶ 310–315 (Kaul, J., concurring) (proportionality and necessity as limitations on state intrusion into privacy).