JUDICIAL ADMISSIBILITY OF DIGITAL EVIDENCE: LEGAL DEVELOPMENTS AND FORENSIC CONSTRAINTS

Ms. Muskan, Research Scholar, Amity Law School, Amity University, Haryana.

Dr. Vidushi Puri, Assistant Professor, Amity Law School, Amity University, Haryana

ABSTRACT

The fast process of digitization of the modern society has fundamentally altered the particulars of crime and served to alter the grounds of evidence on the bases of modern laws as well. This development has led to the emergence of the specialized field of digital forensics which has become essential in the adjudication of crimes that occur in the virtual world. Digital forensic labs have increasingly performed a thorough study of electronically stored data, which currently helps in identification, preservation, analysis, and presentation of digital proof in court. Physical artifacts are replaced with more complicated digital traces, including digital records, data on mobile devices, cloud-based records, and other categories of data that is generated electronically. Courts are now including the use of digital evidence as substantive and corroborative evidence, but its weight of evidence is commonly watered down by lack of uniform legal standards and standardized forensic practices. The alignment of forensic processes, detecting the presence of cross-national investigations via clouds, etc. only adds to issues in due-process. Submissions of expert and their credibility also stand at end point at times. Legally, developments are needed on crucial issues such as the reliability, authenticity, integrity and admissibility of digital evidence when it comes to making factual decisions. There is an utter need to induct more experts in the labs, train the existing ones and adopt the new laws with full force. The article in its complete essence addresses these issues with the solutions proposed, which if implemented may help in curbing the menace of cyber crime and issues in its admissibility.

Keywords: Court, Digital Forensics, Electronic Evidence, Experts & Law.

Introduction

The admissibility and assessment of digital evidence in India has been significantly changed substantively by factors such as technological spread like a wildfire, increasing levels of cybercrime, and the issue of the promulgation of the Bharatiya Sakshya Adhiniyam, 2023 (BSA). Since 1 July 2024, BSA replaced the Indian Evidence Act of 1872 which was used in colonial-era, and restated the status of electronic records as evidence. The digital evidence, such as emails, WhatsApp chats, social-media feeds, CCTV video recordings, call-data-records (CDRs), metadata, files on the clouds and logs on the devices have become the backbone of numerous criminal, civil, and even marital cases. This development is indicative of the booming Indian digital economy where there are now over 800 million smartphone users and even higher internet penetration due to which electronic records are now an essential part of proving factual assertions as in the case of cyber fraud or cyber-harassment or electoral disputes. Though now the courts have initiated to examine the issues more closely in regards to strict compliance with chain-of-custody measures, forensic integrity provisions, and protection of the procedures with procedural safeguards aimed at the maintenance of the evidential integrity, the provisions of standard protocols remain in absentia. This failure highlights the critical importance of standardization of forensic processes, integration of legal systems and a capacity building of institutions in the criminal justice system so that digital forensics has the capacity to make the digital bridge the gap between technology and law.

Traditionally, Section 65A and 65B of the Indian Evidence Act and the Information Technology Act, both of which did not provide either, categorized electronic evidence as secondary evidence, with a high degree of compliance with certification being required to make it authentic[1]. The judges ruled that a certification document, such as device information, hash values, and other tamper-evident signatures, were mandatory to secondary electronic outputs, but could be replaced in the event that the original device or record was used in court. This was a necessity that resonated with the concept of defect curability in exceptional situations and strengthened protection against fabrication. However, the dependence on certification and secondary status restricted the evidential effectiveness and procedural effectiveness of

[1] Aditya Mehta, Arjun Sreenivas & Swagata Ghosh, *Section 65B of the Indian Evidence Act, 1872: Requirements for Admissibility of Electronic Evidence Revisited by the Supreme Court*, India Corporate Law (July 27, 2020), https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/ (last visited Apr. 10, 2026).

electronic data.

Rise in Relevance Due to Cybercrime Growth and Digitalization in India

Digital information is volatile in nature and can easily be altered, deleted, encrypted or degraded without noticeable traces, thus making it hard to determine authenticity. Alterations can be made in a continuous manner via metadata manipulation, hashing or using advanced equipment like the deep-fake code and so on, undermining trust in evidence[2]. The involvement of digital gadgets in commission of a crime has been on rise, which leads to an act falling in the category of cyber crime. The criminals these days are advanced and are able to victimize the people. This is because of the main cause that the internet has made a space in every aspect of human life and now all the activities have an involvement of internet in some way or the other. For example, in our day-to-day life, when we move out to purchase a consumable item of mere ₹ 20, we prefer making the payment via the online method. This in turn shares our bank account information with the shopkeeper, which can be used to commit financial crimes. Such crimes are now considered normal in nature as there is lack of information in the public related to the use of internet and sharing of sensitive information to unknown elements of society. As per the report of the NCRB (National Crimes Records Bureau) in the year 2024 a total of 1, 01, 928 cases of cyber crime were registered against 86, 420 in the previous year[3].

Shift from traditional to digital-era evidence under modern laws

The involvement of technical gadgets, as a result were now forming an integral part of criminal activities. Courts, which were previously hesitant to consider the digital records to be included in the investigation and were reluctant to consider them as evidence, were now finding it difficult to cope up with the issue. Thus, as the usage grew along with the involvement, the cases at the door of the judiciary also mounted where electronic gadgets or the data was a part of crime commission. It was at this stage where the courts, gradually with the amount of expertise and police personnel we had, dived into the role of electronic evidence in the commission of an illegal act. As the judiciary and the staff, both were at the initial stage, issues

[2] Inha Kalancha, Valerii Bozhyk, Oleksii Muzychenko & Viktor Vatsiyk, *Digital Evidence in Comparative Criminal Procedure: International Experience and the Practice of Judicial Review*, 32 TPM: Testing, Psychometrics, Methodology in Applied Psychology S2, 34 (2025).
[3] The Hindu Bureau, *NCRB's Crime in India 2024 Report: A Comprehensive Coverage*, The Hindu (May 8, 2026), https://www.thehindu.com/news/national/ncrbs-crime-in-india-2024-report-a-comprehensive-coverage/article70954087.ece (last visited Apr. 12, 2026).

were bound to erupt. There were technical inadequacies along with the procedural and evidentiary glitches in existence. In cybercrime cases, the issue of defense against accusation often prevailed in the grounds of authenticity, which slowed justice or lead to acquittals, consequently undermining the effectiveness of prosecutors. Thus, reforms to put standardization in the first order: requiring certified laboratories, introducing forensic education to police and judges, using AI-aided technologies to test integrity, and internationalization, including the case of ISO guidelines on digital forensics standards were felt. In order to ensure prosecution effectiveness and satisfactory guarantees of fair-trial rights which require strong measures against fabrication and are obligatory to use the probative power of electronic evidence, there were two ways only – either amend the present laws or bring new laws into action. Thus, from the developmental phase including landmark cases ranging from Suhas Katti[4] case, where the court convicted a person for the first time under the category of cyber crime, to the recent case of Arjun Panditrao[5] where it affirmed the usage of certificate, the Indian legal picture has changed drastically and in a positive manner.

Digital/ Electronic Evidence in BSA, 2023

It was in 2023 that the new Act, Bharatiya Sakshya Adhiniyam was introduced and was enforced in July, 2024. By amending its Sections and other provisions in 2023, the BSA takes this structure more modern as further in Section 57, 61 and 63 electronic records have become primary evidence. Section 63 expressly understands the concept of Computer output, which refers to the information printed, stored, or copied by a computer or a device, as admissible documents in case integrity is proven using hash values, compatibility of metadata and certification. The certification regime, which is codified by Section 63(4), is stricter: it asserts signatory of both, the responsible person and the accredited expert, a prescribed format of schedule (Parts A and B), an authentication of Chain of Custody procedures using cryptographic tools. The rule is in line with the international best practices where digital records are equal to traditional documents as well as reducing the risk of tampering. Courts have imposed strict adherence through post-implementation of judicial trends; an example is in the case of the Kailash v. State of Maharashtra (2025) the Supreme Court stated that video evidence (e.g. stored on CDs) was fully admissible and did not require transcripts or auxiliary witnesses to provide a direct interpretation in court when the requirements of a BSA had been otherwise

[4] State of Tamil Nadu v. Suhas Katti, CC No. 4680 of 2004 (India)
[5] Arjun Panditrao v. Kaislash Gorantyal, AIR 2020 SC 4908 (India)

satisfied[6]. The Court reminded once again the scope of the provision of Section 63 of the Indian Contracts Act 1980 (amendment) to refer to an independent code of evidentiary expression that section could not be circumvented[7]. In more modern court practices, judicial bodies are becoming increasingly alert to the spread of deepfakes, AI-generated materials, and fabricated media, warning against the use of truncated or computerized references in a pleading, as in the 2025 a case of AI use in the operation of the law which cautioned of its actually influential place in the judiciary was identified[8].

Legal Framework Governing Admissibility in India

It is possible to say that the legal framework on admissibility of digital evidence in courts in India has matured considerably to cater to the demands of digital society. Until 2023, Section 65A and Section 65B of the Indian Evidence Act, 1872, which provided the basis of the electronic evidence, were included in the Information Technology Act, 2000. Section 65A effectively held that the content of electronic records was provable under Section 65B, which gave computer output (i.e. printed, stored or copied electronic data) secondary evidence status. To make such output admissible, the parties were required to meet exceptional qualifications among them being regular use of the device, successful functioning of the device, faithful reproduction of data and provision of a compulsory certificate as laid down under Section 65B(4). This certificate which identified the record, the device specifications and the conditions achieved had to be signed by a person in charge of the device. The IT Act definitions of the electronic records and the digital signatures were imposed upon the framework giving it reliability against tampering. However, judicial interpretations such as the necessary certification requirement arising as a result of the Anvar P.V v. P.K. Basheer[9] case often resulted in omission of evidence as a manifestation of procedural incompetence.

Electronic Data – From Secondary Evidence to Primary Electronic Records

In the Indian evidence law, primary evidence is the original document (according to the

[6]Swasti Chaturvedi, *Should Contents of Video be Reduced to Transcript in Words of Witness who Created It or Noticed in It: Supreme Court Answers*, Verdictum (Sept. 16, 2025), https://www.verdictum.in/court-updates/supreme-court/kailas-bajirao-pawar-v-the-state-of-maharashtra-2025-insc-1117-vide-contents-evidence-act-transcription-1591496 (last visited Apr. 12, 2026).
[7] Arjun, *supra* note 5.
[8] Akashvani, *Supreme Court Assures Judges Exercising "Utmost Caution" on Use of AI in Judicial Process*, Akashvani News (Dec. 6, 2025), https://www.newsonair.gov.in/supreme-court-assures-judges-exercisingutmost-caution-on-use-of-ai-in-judicial-process/ (last visited Apr. 12, 2026).
[9] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473 (India)

provisions of Section 62 of the old Act and its equivalent in the BSA), whereas secondary evidence is any copy or output that necessitate a foundational proof. Prior to the BSA, electronic records were originally classified as secondary under Section 65B (c) and had to be certified in order to be admissible except where the original device or record itself was created (e.g., showing a physical phone). Section 65B(1) created a deeming fiction that made the compliant computer outputs to be treated as documents admissible without originals to cover the gap in the law concerning intangible digital data. The BSA redefines this idea: Section 63(1) gives an even stronger operation of the deeming fiction by finding compliant computer outputs deeming documents wherein they do take a primary effect and so have an effect on evidence of contents or facts (not needing delivery by force or production), but retain conditions and integrity self-assessments of experts such as hash values[10]. The primary ones are the electronic originals (e.g., raw device data), but the deeming fiction enables practicability of admitting derivatives (printouts, exports) in large-volume electronic cases. This difference facilitates the pre-exclusion of all evidence without volatile digital environment having an original holder of information, but enforces a security against alteration. The history of compulsory secondary certification being shifted into a superior deemed documentary status thereby strikes a balance between accessibility and reliability hence mitigating against miscarriages and in line with international benchmarks of digital evidence.

Mandatory Requirements for Admissibility: The Certification Regime

On 1 July 2024, replacing the Indian Evidence Act, the Bharatiya Sakshya Adhiniyam (BSA) became effective, which changed the rule providing on electronic evidence in Section 63. This provision finds computer output as information obtained out of computers, communication devices, or optical or magnetic media, or semiconductor memory expressed in electronic form and considers them documents admissible without consequences of producing the original copy, provided the conditions are reflective of the prior regime but contain significant improvements: regular use to create, store, or process; ordinary input of information; reliability of devices; and the deriving or reproducing accuracy.

The certificate is presented on admission, with a predetermined schedule format, consisting of Parts A and B, where in part A, the details of production and the details of the devices are

[10] *The Bharatiya Sakshya Adhiniyam*, No. 47 of 2023, India Code (2023), https://www.indiacode.nic.in/bitstream/123456789/20063/1/aa202347.pdf (last visited Apr. 17, 2026)

recorded as the presenter offers them, and part B ensures this with expert verification, often using hash values and metadata that represents integrity. Section 56, which was previously 61 under the IEA (India Evidence Act, 1872) now, speaks about the admissibility of electronic evidence as included in the name of primary and secondary evidence. Section 2 (1) (d) under the new act includes electronic and digital records as a document, which now adds them to the list of evidences that are considerable in the present Indian courts. A notable section in the new act was 57, where primary evidence now covered electronic and digital records admissibility, which meant now they were admissible in the court in the first instance, without giving any loophole of it reliability. Under this section only, four new explanations were added which now govern the electronic records admissibility. These modifications solve the previous uncertainties, provide additional defense against compromise (e.g., through cryptographic validation) and pattern with the current digital realities in smartphones and cloud data, which helps reduce the exclusion in the procedure and enhances confidence in post-2024 scenarios[11].

The admissibility of digital evidence, in Indian courts, is essentially based on a certification regime which has developed out of the earlier system, the pre-2023 system, as the Bharatiya Sakshya Adhiniyam, 2023 (as of 1 July 2024) aspect of the domestic concept of certification. This regime is a pillar of protection since electronic records are required to meet high procedural and substantive standards before they can be used as evidence.

The forerunner Indian Evidence act, 1872, Section 65B (4), required the signing of a certificate by an individual occupying a position of responsibility over the computer or device in question. The certificate needed to recognize the electronic record, explain how it was created, give the details of the device that it was created on, and prove that it complied with integrity requirements that include normal use, appropriate functioning, and correct replication. This was used as a condition to the admissibility of secondary electronic evidence, a rule which came to be codified in landmark Supreme Court cases.

The necessity of the certificate was also clarified on the basis of the jurisprudence by the Supreme Court. The Court in Anvar P.V. v. P.K. Basheer[12] clearly reversed the soft-hearted decisions and stated that the certification was mandatory. The next case was Arjun Panditrao v. Khotkar. Kailash Kushanrao Gorantyal[13] which defined the certificate as a code that is

[11] The, *supra* note 10.
[12] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473 (India)
[13] Arjun, *supra* note 5.

complete and in exceptional situations, such as non-access by the producer it could still be curable, but only on timely alert about faults and could be produced at any stage before judgment.

BSA modernizes this framework by section 63 that provides the meaning of computer output as any electronic information printed, stored, recorded, or copied using computers, communication equipment, optical or magnetic media, or semiconductor memory. The terminology is admissible regardless of the requirement of its original production or any other evidence as long as the controlling person satisfies the requirement of the Sub-section 2 (a) namely, it was regularly used; (b) it was used in the ordinary course of data input; and (c) and it was allowed to operate properly or was not affected due to malfunction which means it remains identical; it must have been reproduced or derived faithfully. Sub-sections 3 treats networked or intermediary systems as one same system called computer to conserve evidence. The important change is in Sub-section (4) where it is mandatory to submit a certificate at the admission stage in all cases. This certificate should (a) state the record and how it is produced; (b) specify the devices involved; and (c) comment upon the conditions of Sub-section (2) which are signed by the person in control or the management and an expert.

The certificate is issued on a prescribed schedule format which consists of two sections. Part A, which is signed by the party or producer, includes device specifications like make, model, serial/IMEI number, cloud ID, the production method and a value computed with the SHA-256 digests or the MD5 hash or other hash number algorithm, and a report on the compiler of the hash computation is also included. Part B, which the expert signs, confirms the information presented in Part A, that the hash value has been correctly created, and that he is not violating the required conditions and signs with the relevant designation. The dual-signature (by the custodian or producer) and dual-signature (by an expert) is an enhanced aspect on reliability that adds cryptographic validation to identify any modification and enforcing technical validation by expert attestation. The examiners mentioned in IT Act Section 79A or forensic specialists notified to the experts provide technical credibility to the evidence[14].

The judicial tendencies since 2024 have served to abide strictly by the certification regime. The practical bottlenecks include shortages of forensic laboratories and experts gaps (such as the

[14] Admin, *A Legal Practitioner's Guide to Electronic Evidence Under the Bharatiya Sakshya Adhiniyam, 2023*, Law Web (Jan. 25, 2026), https://www.lawweb.in/2026/01/a-legal-practitioners-guide-to.html (last visited May 17, 2026).

Madras High Court of 2025) commanding central governments to list further experts per need to address shortages of mobile specialists[15].

Probative value is counterbalanced by safeguards of the regime as it is mandatory. It not only eliminates the easy admissibility of intangible cyber-data but also enables the pragmatic application of evidence in a big-data scenario, including smart phone-related cases or server logs. However, difficulties still remain. Limits on the supply of experts may result in delays or omissions, especially in jurisdictions with less density; hash verifying would require technical expertise; and third-party data matters e.g. social media export requires an expert to formalize the role of custodian and expert. BSA certification regime enhances the position of electronic evidence by requiring procedural soundness, in order to promote credibility in the digital justice environment in India.

Role of the Information Technology Act, 2000

Information Technology Act, 2000 (IT Act) provides the essential infrastructure to admissibility of digital evidence by defining some of the important terms, and allowing evidentiary accommodation. Section 2(t) defines an electronic record in general as data, a record, or a data image/audio in electronic form; Section 4 gives legal status to electronic records, and places them on par with paper records; and Section 5 accords legal status to contracts and records.[16] Successive amendments in 2008 perfected electronic signatures and authentication. All significant direct modifications to the evidence rules have raised have taken place until the BSA was enacted in 2023; the provisions of the IT Act, including the provisions of Section 79A of foreclosure (namely examiner designation) serve to endorse forensic elements. Recent IT Rules focus on the use of intermediaries and labeling of synthetic material (e.g. deepfakes), which indirectly strengthens evidence authenticity in cyber legal cases[17]. The cross-references in the IT Act have been critical in interpreting the terms in BSA like electronic form and scope of the device to provide continuity as the BSA deals with the fundamental

[15] *Madras High Court Directs MeitY to Expeditiously Notify Experts as per § 79A of the Information Technology Act for Authenticating Electronic Evidence*, Law Web (Nov. 1, 2024), https://www.lawweb.in/2024/11/madras-high-court-directs-meity-to.html (last visited Apr. 18, 2026)
[16] *Information Technology Act*, No. 21 of 2000, India Code (2000), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited Apr. 18, 2026)
[17] *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, Gazette of India, Extraordinary, pt. II, § 3, sub-sec. (i) (Feb. 25, 2021), https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf (last visited Apr. 18, 2026).

concerns in interpreting admissibility. Accordingly, the IT Act and the BSA are complementary to each other establishing a framework: the IT Act offers defining and facilitating framework of e-transactions and records during investigations, whilst the BSA regulates substantive rules of evidence.

Forensic Limitations and Technical Challenges

The vulnerability of digital evidence to manipulation, interference, destruction, or forgery is an inherent forensic drawback to the Indian judicial system. Unlike hardcopy evidence, which creates visible marks of presence, digital evidence can be processed quietly and effectively invisible by simply accessing a set of easily obtainable programs, software, or even specialized programs that can be used to alter the metadata of a specific file, or produce deep-faked content using more specialized tools[18]. Less extensive manipulations such as timestamp editing, file hash modification, or the use of steganography to hide information in seemingly irrelevant files, can be fabricated without leaving any obvious trace. In India, this has been the point of vulnerability in a string of cybercrime cases, where WhatsApp messages, email messages and CCTV footage have been testified as possibly being altered. The problem does not end here only, main contribution arrives from the uncodified rules of examining a forensic evidence that are present across states and whenever there is a matter on the cross-border front, there are clashes in the context of examination of evidence, which ultimately leads to miscarriage of justice. The distorted chain of custody contributes to the issues in a case leading to deviations in the forensic reports at times. Shortage of experts along with this at times creates a situation where a case is listed for years merely because of the fact that the electronic piece of evidence has not been examined as it is listed late for the same and there are other evidences in the pipeline.

- **Volatility and Fragility: Data degradation, encryption, hidden files**

Forensic analysts have difficulty with identifying any tampering, with even hash differences failing to provide conclusive result on whether the difference was deliberate or not. Evidence like the alleged forged digital records e.g. the precedents of the Gujarat High Court, fails to be accepted as valid evidence vary frequently, but to demonstrate the fabricated evidence, reverse engineering or comparing it is frequently a resource intense task. Confidence is further

[18] Carlton Jeffcoat, *The Importance of Volatile Data Capture in Digital Forensics*, Wetstone Technologies (July 27, 2023), https://www.wetstonelabs.com/importance-of-volatile-data-capture/ (last visited Apr. 18, 2026)

destroyed by the easy duplication and offline editing as it is possible to copy, edit information offline, and then reintroduce it without violation of a chain of custody unless the protocols are relaxed. This weakness in effect continues to invalidate fraud, harassment and election related prosecutions where defence questions integrity on a regular basis[19]. Although the 2023 BSA focuses on certification and hashing, the growth of easy-to-use tampering tools is outpacing the development of forensic countermeasures, and regardless, a system to curb risks in the changing digital evidentiary environment of India requires judicial review and new technologies, such as blockchain, immutable logging etc.

Chain of custody issues and lack of uniform preservation protocols

The very nature of digital data such as its instability and unsteadiness poses a great challenge to forensics, which means that evidence can deteriorate, disappear, or get unavailable in a matter of seconds. Volatile artifacts such as contents of random-access memory, temporary cache files, or dynamic system logs vanish when the device is shut down, power is lost or when normal job activity occurs, hence the timely preservation of volatile artifacts is urgent as well as often unavoidable where it involves a seizure. The effects of data degradation include bit rot in storage media, file-system corruption, or environmental effects and thus reduce the reliability of older evidence. Hidden files, deleted partitions or steganographic content are additional signs to hide it; cybercriminals use these vectors via anti-forensic means, which can be data wiping, sure deletion tools, or hidden channels[20].

Cloud-stored information sets up jurisdictional and access problems in Indian context, where it is even possible to wipe data remotely. Application architectures and heterogeneity of operating systems bring about forensic obstacles in which standard tools cannot read encrypted or fragmented remnants of different versions. The weakness of evidence is an invitation to failure of justice. Unstable data destruction damages the chronological integrity of device along with impenetrable encryption that enforces an obstacle on investigators[21]. The mitigation strategies require the live-acquisition procedures, special decryption initiatives, and advanced imaging and enhancement, though, the limitations faced by the resources limit the

[19] Geethapriya S. & Tvisha G., *Challenges of Electronic Evidence and Its Admissibility in Courts*, 10(11) International Journal for Research Trends & Innovation b1 (2025), https://www.ijrti.org/papers/IJRTI2511101.pdf

[20] *Malware Detection: Evasion Techniques*, CYFIRMA (Sept. 13, 2023), https://www.cyfirma.com/research/malware-detection-evasion-techniques/ (last visited Apr. 18, 2026).

[21] *Digital Forensics for Data Breach Investigations: Why It Matters*, Proaxis Solutions, https://www.proaxissolutions.com/blog/digital-forensics-data-breach-investigations (last visited Apr. 18, 2026)

effectiveness, turning the need to adopt proactive preservation policies and judicial recognition of this technical reality into a significant occasion for BSA practices.

Chain of Custody (CoC) violations and the lack of common preservation guidelines are the most adverse effects on digital evidence integrity in India. Digital evidence is to be carefully documented and all handling procedures from search and seizure till court presentation have to be recorded in such a way that it is clear that there had been no alteration; however, the intangible and volatile characteristics of data are hard to be reflected by traditional paper-based chain-of-custody records. Failure of continuity in police seizure, e.g. turning on devices without write-blockers, informal transfers or poor sealing, allows defense to highlight problems with authenticity.

There are inconsistent protocols in various states and agencies in India as there are currently no standardized guidelines on imaging, hashing, or logging in the country, leading to the disparities in how the evidence is treated. The absence of a unified code with regards to the CoC creates such hurdles and leads to delay in disposal of cases[22]. Cyber prosecutions due to the CoC breakdowns yield more acquittal or dismissal. Rural police stations at times have no Faraday bag to provide isolation of the signal or cover secure storage to prevent risks of remote access or degradation[23]. Court tends to stress on comprehensive registering, time stamps, and expert confirmation, but reality fails in operation due to lack of training.

Dependence on specialized tools, expertise and forensic labs

The digital forensics ecosystem in India is completely reliant on the use of specialized tools, qualified experts, and the forensic lab; however, due to severe capacity constraints, it is unfeasible to handle any digital forensic issue. Central Forensic Science Laboratories (CFSLs) and state FSLs face persistent preview lists even with extensions of new CFSLs with many thousands of cases on display (including in digital format), pending serving[24]. Scientific staff turnover rates are about 49 percent per, and in some states, the turnover rates are over 90

[22] Srishti Rajput, *Evidence Mishandling and Chain of Custody Failures in India*, 3 Innovation & Integrative Research Ctr. J. 786–791 (Apr. 2025), https://iircj.org/wp-content/uploads/81-Evidence-Mishandling-and-Chain-of-Custody-Failures-in-India.pdf

[23] Yuvraj Dilip Patil, *Challenges of Indian Police in Investigation of Crime*, 3 Bharati L. Rev. 41–46 (July–Sept. 2014).

[24] Government of India, *Forensic Labs*, Ministry of Home Affairs, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2085688&reg=3&lang=2 (last visited Apr. 19, 2026)

percent, and accreditation is crippling (6-8 percent in most facilities)[25].

Skills gaps lead to a shortage of examiners that have been notified in accordance with the provisions of Section 79A of the IT Act, which causes delays during certification and analysis. Backlogs result in evidence degradation (e.g. loss of information with time) or rushed examinations lead to errors in high-volume cyber-crime cases. The latest news reports highlight these issues which in turn violate the right to a speedy trial, as the accused has to wait till the reports are released and shared with the court[26]. Although the efforts that have been made through National Cyber Forensic Lab in Hyderabad and state modernizations (e.g., zero-pendency goals in Haryana) reflect improvement, there is still a national imbalance in quality of laboratories between urban and rural areas - metropolitan ones are better[27]. Reliance on the services of individual laboratories or foreign aid raises cost and jurisdiction issues, apart from the most important aspect where the integrity of the evidence is questioned if the same is examined at an external and non-authorized place. In general, these shortcomings severely hinder the high-quality standards provided by the BSA, which can readily result in unreliable outputs, omissions, and this highlights the urgency of investment in training, equipment renewal, staffing, and standardized capacity-building programs to streamline forensic infrastructure to match India demands in digital evidentiary equipment.

Delay in procurement of forensic tools

In terms of the electronic evidence examination, the major roadblock lie in the procurement of forensic tools, which are majorly outsourced only, at present, India has no forensic tools under the category of digital forensics which is made in India. All the tools are outsourced and the process for the same also stands lengthy. The problem not only ends here, the time consumption in terms of availing a forensic software or the tool is also high as the file has to undergo several level in order to clear and get the same sanctioned. Apart from the sanctioned aspect, maintenance of the same also incurs high cost. The tools which are available in the public domain often do not carry all the features that are required by the expert and this in turn again

[25] Kanishga I. & H.R. Bhargava, *Survey on the Underutilization of Forensic Expertise in India: Examining the Dominance of Law Enforcement in Evidence Collection and Investigations*, 9(1) Journal of Forensic Science and Research 67–86 (2025)
[26] Vidya, *Maharashtra Forensic Labs Backlogged Since 2020, Bombay High Court Seeks Report*, India Today (Apr. 18, 2026), https://www.indiatoday.in/india/story/maharashtra-forensic-labs-backlogged-since-2020-bombay-high-court-seeks-report-from-state-government-2898010-2026-04-18 (last visited Apr. 30, 2026)
[27] Government of India, *Forensic Labs and Forensic Infrastructure*, Ministry of Home Affairs, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2036389&reg=3&lang=2 (last visited Apr. 19, 2026)

hampers the examination process. This all combined leads to delays from the aspect of evidence expert[28].

Shortage of experts in India

The problem does not end at the aspect of softwares; it goes down to the shortage of experts as well. The forensic infrastructure in India has serious capacity constraints, Central Forensic Science Laboratories (CFSLs) and State labs have queues and much-needed special equipment to extract data on clouds or encrypted devices, and a shortage of trained professionals[29]. Apart from this, as these two categories of labs only have the most updated tools and softwares, the load on them is usually high, along with the fact that if a tool is absent at a lab then the expertise of the same also stands absent. This can be understood as if the expert examines evidence with a tool, over a period of time his expertise is polished over the tool and this in turn saves time when similar cases arrive. However, as not all labs are equipped with all the tools the expertise also remains on standby. There is a need to equip all the labs as per their need and then only the issue can be resolved.

Evidentiary and Procedural Challenges in Courts

The processing of digital evidence using the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has progressive characteristics, but lack of resources poses a problem. Such barriers exist because of the technical features of the medium and court process which can often lead to a delay in the processing and extinction of evidence or unequal application of jurisprudence to the proceedings.

The check of authenticity is a key difficulty, as digital evidence can be manipulated in metadata, can be misunderstood and even falsified. With the presence of metadata, which stores timestamps, geo-locations, and device identifiers and other relevant information, data of every nature can be altered in a covert manner that compromises its reliability. The lack of understanding of metadata can lead to misunderstandings when people misinterpret metadata, such as taking creation dates as the dates of modification and make incorrect assumptions.

[28] Deloitte, *Indian Digital Forensic Market Report 2025* (2025), https://www.deloitte.com/in/en/services/consulting/services/risk-regulatory-forensic/indian-digital-forensic-market-report.html (last visited Apr. 19, 2026)
[29] Directorate of Forensic Science Services, *DFSS Report 2018–2022* (Ministry of Home Affairs 2023), http://dfs.nic.in/pdfs/DFSS%20Report%202018-2022.pdf (last visited Apr. 12, 2026)

The increasing spread of deep fakes has led to calls to enhance the specificity of the forensic standards, but the issues in respect of alteration of data by any possible method has undermined the forensic capabilities which in turn becomes a favorable part for the offenders. Offenders are all too often found not guilty because of such grounds thus postponing the application of the law and serving acquittals in such cases. As a result, as much as the system of certification and hashing of BSA improves security, the increasingly sophisticated nature of manipulation methods requires continued comparative supervision by the judiciary, expert advice, and possibly amendments to the appropriate legislation in order to maintain evidentiary integrity in the field of the Indian online cell.

Volume overload and contextual analysis difficulties

The sheer amount of digital evidence overwhelms courts and investigators, thus, making contextual and trustworthy assessment more difficult. Cloud servers, social media, and smartphones generate large amount of data including thousands of messages, logs, images and metadata far greater than the traditional volumes of evidence. This is because when examining cyber criminal cases, extracting the relevant objects in bulk datasets is fraught with the risk of failing to depict the major context or showing biased pieces. A forensic backlog exonerates further to intensify this predicament- laboratories have a difficult time dealing with high volumes in a timely manner leading to impaired evidence or reports. Courts can find it hard to have a holistic interpretation; even isolated pieces (i.e. a single WhatsApp message) cannot have trace of the conversation chains, time, or intent, which encourages misinterpretation. Recent examinations emphasize the role that information overload plays in the existence of procedural delays and the decrease in the weight of evidence[30]. The judges have to go through large exhibits without proper summarizing or recognizing pattern tools, which increases their chances of making an error. The integrity focus of BSA is not necessarily about the volume, as common parties often present bulk information without proper duration, and in this manner, put a strain on courts. This overload impedes timelines of trials, exposes miscarriages of justice in cases where context is lost, and the need to have standardized processes of triage. Judicial training in the data handling quality and technological supports ensure that investigation covers comprehensive and efficient trials in high-stakes digital cases.

[30] Geethapriya, *supra* note, 19

Judicial technological literacy gaps and inconsistent rulings

Lack of judicial technological literacy is causing disparity in decisions on digital evidence to the marginalization of consistency in the provision of BSA. A significant number of judges and legal practitioners do not have substantial acquaintance with technical aspects including hashing, encryption, metadata, or forensic procedures resulting in inconsistent interpretation of authenticity, faithfulness, and compliance[31].

This inconsistency is due to the lack of training in spite of the e-Courts programs and AI applications like SUPACE to conduct research and transcription, as well as resource differences between cities and districts benches. Irrational use can be seen when it comes to video admissibility, or third-party data; some courts require an examination to be conducted, and others admit them through a prima facie report submitted by an expert. Such fluctuations destroy foresight, promotes entreaty and postpones justice. Reforms have proposed mandatory training on technology to the judiciary, standardized guidelines and expert panels, but there are no real changes. To make BSA a practical process, filling these gaps is vital to the successful implementation of the policies to safeguard the seamless, knowledgeable handling of adjudication that meets high standards of evidence with the swift technological change.

Conclusion and Path Forward

The exclusion of digital evidence on privacy grounds, proportionality standards, and lapses in the procedure often lead to the protection of the constitutional rights and the disadvantaging of prosecutions. Evidence obtained through non-unified methods adopted for seizures, unauthorized access or disproportionate harvesting are not admissible in court, such as the introduction of irrelevant personal information in matrimonial proceedings are regularly ruled out. The rejections are caused by procedural failures like the inability to secure a warrant, improper follow-up of CoC, inadequate certification or other similar issues with respect to Section 63 of BSA.

Lapses like use of devices without powering or mishandling of electronic record or information are inadmissible in the court of law. Although BSA reinforces integrity, it overlaps with the inadequacies of the CoC, which introduces exceptions in the case of their breach. Such tensions impedes efficiency in digitally-intensive cases, where guidance on collection within the law,

[31] *Id.* at 31

judicial balance in terms of proportionality as well as training is necessary to reduce procedure error while maintaining the fair-trial integrity.

BSA certification regime enhances the position of electronic evidence by requiring procedural soundness, in order to promote credibility in the digital justice environment in India. This could only be effectively implemented by increased training and certified labs as well as judicial uniformity to curb unwarranted evidentiary obstacles.