DIGITAL EVIDENCE IN CORRUPTION INVESTIGATIONS IN INDIA: LEGAL CHALLENGES OF ADMISSIBILITY, AUTHENTICATION AND CHAIN OF CUSTODY UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Ms. Sarumathi G R, Research Scholar, St. Joseph University, Chennai

ABSTRACT

Investigating and proving corruption cases in India depends on electronic records. Digital records help show connections and transactions that cannot be testified by witnesses. However, electronic records can be altered. The aim of this article is to analyze the recently enacted Bharatiya Sakshya Adhiniyam (BSA) 2023, and assess the risks of admissibility and authentication of records in corruption cases. This article will also consider prejudicial cases before the BSA, as well as legislations, rules, case laws and forensic literature between the years 2020 to 2025. This article seeks to ensure that remedial and protective measures prescribed in the BSA are not "evidential" and "prejudicial" in nature. This article also supports the preservation of corruption records, and mandates the prevention of theft and alteration of records. Since record custodianship is a contentious issue, this article advocates for orders preventing the destruction of records and assuring the availability of records. Forensic custody of records should be ensured. Prevention of destruction and assuring continued availability of records should be combined with protection of evidence. Verification and evaluation of records should be ensured. In this article, the author argues that effective measures should be enacted to ensure accountability of public functionaries without compromising the rights of citizens.

Keywords: Digital evidence; corruption investigations; Bharatiya Sakshya Adhiniyam; authentication; chain of custody; digital forensics.

1. Introduction

Investigations into corruption focus on digital first. Traces of financial transactions are commonly identified and analyzed later in an investigation. Records related to tenders may contain information regarding irregular bids. Unauthorized access to a secure message may contain information concerning a demand for a bribe. Bank records may help identify a front. CCTV footage may help place individuals of interest. Information from various sources, including records and surveillance, may contain information pertinent to a corruption investigation.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), comes into effect on July 1, 2024 and replaces the Indian Evidence Act, 1872. The BSA outlines procedures related to digital documents and evidence and addresses the validation of digital records. Like its predecessor, the BSA allows for latitude in terms of adjusting to changing circumstances. As a result, the BSA outlines processes and procedures applicable to ongoing proceedings, and provides transitional provisions applicable to all proceedings, including investigations, initiated under the Indian Evidence Act, 1872.[1]

It is important to determine the transitional provisions applicable to a given proceeding in order to assess the likelihood and prospect of the BSA facilitating the introduction of evidence relevant to a corruption proceeding. It is expected that evidence subjected to legal validation will undergo further processes including forensic analysis.

2. Methodology and Scope

The study analyzes statutes, decisions, and guidelines. It conducts research and integrates forensic science. It analyzes and evaluates case law relating to former section 65B certificates. It accesses and assesses integrity and security of forensic methods. It offers proposals for improvement. It does not include results of experiments or case datasets. It does not include interviews. Illustrative examples are included to explain principles; they should not be construed to represent any findings or conclusions concerning any specific individuals or situations.

[1] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 170(2) (India); Ministry of Home Affairs, Notification S.O. 849(E) (Feb. 23, 2024) (commencement July 1, 2024).

3. Legal Framework for Evidence in Electronic Form

The Evidence Act states that an electronic record shall not be excluded merely because it is in electronic form (section 61). How a Court may admit electronic records is provided in section 62. The Act defines 'primary evidence' (section 57) to include any electronic record which is created, generated or recorded by a computer, or electronic device. A primary record does not assist in explaining how it was collected, how its ownership is disputed or how section 63 applies.[2]

Section 63 deals with computer records. It gives definitions relating to ordinary course of use, input of data and other computer interactions. Section 63(3) provides for a certification of an electronic record which is produced by a computer. The definition and the certificate permit conclusions to be drawn on the record and its contents. Section 63(4) requires a requesting court to issue a direction for production of the record. The Schedule to the Act contains instructions relating to the request and certification.[3]

Section 39(2) acknowledges opinions of designated Examiners of Electronic Evidence under Section 79A of the Information Technology Act, 2000. Explanation of extraction methods, analysis of metadata and identification of anomalies by an expert may help the Court to understand the methods adopted by the Prosecution for digital evidence extraction without shifting the Court's judgment on the digital evidence to an expert. The Information required to constitute offences under the Prevention of Corruption Act, 1988, is contained in that Act, and evidence to prove such information is contained in the Bharat Sarbhaga Samadhan, 2023 (BSS, 2023). Evidentiary proof to such Information as contained in the BSS, 2023, may also be required to be audio-video recorded and sealed along with a list prepared in the presence of a witness.[4]

4. Admissibility and the 'Certificate' Problem

Electronic records may be altered easily, and courts may face challenges while attempting to determine the admissibility of such records. In several cases, the Court may accept a printout of the electronic record without any proof of its integrity or authenticity. However, Section 63

[2] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 57, 61–63 (India).
[3] Id. § 63(2)–(4) & sched. (certificate, pts. A–B).
[4] Id. § 39(2); Information Technology Act, No. 21 of 2000, § 79A (India); Prevention of Corruption Act, No. 49 of 1988, § 7 (India); Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 105 (India).

of the BSS, 2023 requires the Court to consider such matters before accepting a printout as an electronic record.

The special procedure under the now repealed Evidence Act, 2002, for admissibility of electronic records (Section 65B) have been explained in detail in several cases including Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. Section 65B of the now repealed Evidence Act, 2002 (along with other provisions) was incorporated in the Bharat Sarbhagaa Samadhan, 2023. Until Court rules and orders are translated to Practice, principles enunciated in the above mentioned cases may be relied upon.[5]

Admissibility and weight are distinct concepts. A misaligned time stamp on a CCTV export may raise a reasonable doubt as to its integrity and probative value, regardless of certification. Conversely, a gap in a record should be appropriately documented and proven. Such a gap does not render an export automatically inadmissible. In the context of a foreign import, the same principles should apply.[6]

There are circumstances in which crucial information is temporally or logically divided, retained or stored overseas. Requests should clearly articulate the time period and identify audit trails. The requested information should also identify accounts and be preserved. If a record is divided, other service providers may corroborate the information through independent accounts. The information may also be documented through logs. If the information is stored electronically, it is imperative that the service provider export the record to the requesting entity. In doing so, the service provider must act within the parameters of the law.[7]

5. Authentication and Forensic Reliability

The aim of authentication is to provide reasonable assurance that an evidence item is what the proponent claims it to be. It may be necessary to identify the subscriber of an electronic communication or message. It may also be necessary to identify the user of the communication or message. Forensic science provides various means to prove the authenticity of evidence,

[5] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India); *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).
[6] Vaibhav Chadha & Janani Sivaraman, Critical Analysis of the Law on Admissibility of Electronic Evidence in India, 15 Jindal Glob. L. Rev. 119, 119–32 (2024), https://doi.org/10.1007/s41020-024-00219-1.
[7] Sci. Working Grp. on Digit. Evidence, Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers, SWGDE 23-F-004-1.1 (Jan. 13, 2025), https://www.swgde.org/23-f-004/.

including artifacts and metadata. Other corroborating evidence may include bank records and timestamps.

Hash values of digital files may be captured and compared to prior values. Changes may occur between the two values. Hash values do not prove the evidence was not fraudulently altered. It is appropriate for forensic practitioners to work from the originals of digital files. However, if copies are used, the practitioners should verify that the files were in fact a true and accurate reflection of the original. To prove the time and date of a digital file, it may be necessary to consider various timestamps.

Forensic methods must be standardized and consistent. Nordvik and others describe shortcomings of informal tool comparisons, and Neale points out shortages of adequate techniques for authentication of digital evidence. As a result, we can not accept forensic software outputs without questioning and analyzing them critically.[8]

AI-generated audio and video, and selective-sed transcription tend to fabricate and alter evidence. Real evidence may be altered to appear false and fictitious evidence may be fabricated to appear real. The evaluation of evidence should be performed by experts who consider all possible ways in which evidence may have been fabricated and/or altered, and provide their opinions on the integrity of the evidence and the possible alternative hypotheses that may explain the evidence. Courts should rely on the opinions of experts and consider the limitations of data and the methods used to evaluate evidence.[9]

6. Chain of Custody and Seizure Integrity

A chain of custody documents how an item of evidence was handled from the time it was found until it was presented in court. This includes describing the telephone or device from which the evidence was seized. It includes the condition of the device at the time it was seized, the name of the person seizing the evidence and witnesses to the seizure. It also includes the manner and purpose for which the evidence was transferred. When evidence is copied,

[8] Rune Nordvik et al., Reliability Validation for File System Interpretation, 37 Forensic Sci. Int'l: Digit. Investigation 301174 (2021); Christopher Neale, Fool Me Once: A Systematic Review of Techniques to Authenticate Digital Artefacts, 45 Forensic Sci. Int'l: Digit. Investigation 301516 (2023).
[9] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 39 (India); Pranav Verma, Unmasking the Rhetoric of Reform—The Bharatiya Sakshya Adhiniyam 2023 in Context, 36 Nat'l L. Sch. India Rev., no. 1, art. 2 (2025), https://doi.org/10.55496/YRTF3099.

acquisition and verification hashes are recorded to link the evidence copy with the original.

Section 105 of the BNSS specifies the process for capturing the forensic history of searches and seizures. While this may include an audio-video recording, other records may also be required to fully capture the history. A recording may show how a device was discovered; however, it may not show what happened to the contents of the device. The case records should be connected by a series of documents, including the recording, evidence seizure inventory, chain log, digital extraction report and a Section 63 Certificate.[10]

Precautions and procedures outlined in the published guide should be taken to secure and protect evidence, and to log all changes made to the evidence. Storage service providers may be required to allow law enforcement to access evidence by changing the permissions and/or settings associated with the storage. Cloud data, in particular, may require special consideration, as records accessed and downloaded at a later date may be different from the data originally accessed and stored.[11]

An unaccounted gap in custody should not be interpreted as an exclusion under the statute. Factors such as the potential for modification of the record, availability of corroborating evidence, impact of the record on the overall case evidence, etc. need to be evaluated in this regard. In the absence of the original record or in case of mismatch in hash values, which is unexplained, or in case of transfer of record without court order, etc. prosecution case suffers. Introduction of new technology in custodial record systems should be planned and executed in a proper manner. While advancements in technology should not be viewed with skepticism, auditable records in combination with proper systems and controls should be implemented.[12]

7. Judicial Assessment and Institutional Reform

There is a general apprehension regarding digital evidence. In Neeraj Dutta vs. State (Govt. of NCT of Delhi), the Apex Court indicated that in the absence of direct evidence to indicate

[10] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 105 (India); Bureau of Police Rsch. & Dev., Standard Operating Procedures on New Criminal Laws, at 24–27 (2024), https://bprd.nic.in/uploads/pdf/Standard_Operating_Procedures.pdf.
[11] Sci. Working Grp. on Digit. Evidence, supra note 7, §§ 9–12.
[12] Tommaso D'Anna et al., The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data, 11 Healthcare 634 (2023), https://doi.org/10.3390/healthcare11050634; Harsh Patil et al., Potential Applicability of Blockchain Technology in the Maintenance of Chain of Custody in Forensic Casework, 14 Egypt. J. Forensic Sci. 12 (2024), https://doi.org/10.1186/s41935-023-00383-w.

illegal gratification, suspicion in digital records may be relied upon to establish the demand. Digital records should not be relied upon to prove the presence of illegal gratification, where such records demonstrate the digital contact of the public official and the person who is alleged to have made the illegal demand.[13]

In evaluating digital evidence, courts should determine, (i) is the evidence relevant? (ii) Is the evidence produced in compliance with legislative requirements? (iii) Does the evidence retain its integrity? (iv) Does the evidence support the conclusion drawn by the party producing the evidence? Technical details should not obfuscate answers to these questions.

Five changes are suggested. First, anti-corruption agencies should routinely preserve evidence and export source-system data. Second, the documentation of seizure and hash reports should be incorporated with signatures of custody and relevant particulars. Third, forensic service providers should disclose the limitations of the methods and software. Fourth, certificates and court records should be inspected for defects and irregularities, which should be corrected prior to filing and/or hearing. Fifth, defendants should be allowed to review relevant data, logs and reports of expert opinions.

These suggestions should be considered only to the extent that they are authorized by law and necessary to achieve the above objectives. The right to privacy should be protected in accordance with established laws and practices. The honorable judge, K.S. Puttaswamy (Retd.), recognized right to privacy in the Constitution of India. Therefore, state agencies should not collect and retain personal information in an unregulated and unfettered manner.[14]

8. Conclusion

While the Act merely assists in situating digital information in a corruption case and does not mandate its inclusion, it offers a way to certify digital information. Sections 57, 61-63 and 39, along with the scheduled certification formats, are helpful in this regard. Locating and admitting digital information in corruption cases would require substantial incremental technology and expert acquisition. In the meantime, we must maintain that the truth and authenticity of digital information certified under the BSA would be dependent on the integrity

[13] *Neeraj Dutta v. State (Gov't of N.C.T. of Delhi)*, (2023) 4 S.C.C. 731 (India) (Constitution Bench decision delivered Dec. 15, 2022).
[14] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

of the chain of custody and control of the information. Courts must continue to make a distinction between the admissibility of information, the weight of evidence and proof of the commission of the offense. In order to enhance the admissibility of information and the weight of evidence in digital corruption cases, the state may reasonably implement some of the safeguards available.

REFERENCES

Legislation

Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).

Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023 (India).

Information Technology Act, No. 21 of 2000 (India).

Prevention of Corruption Act, No. 49 of 1988 (India).

Indian Evidence Act, No. 1 of 1872 (India) (repealed, subject to savings).

Judicial Decisions

Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).

Neeraj Dutta v. State (Gov't of N.C.T. of Delhi), (2023) 4 S.C.C. 731 (India).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Secondary Sources and Guidance

Chadha & Sivaraman, 15 Jindal Glob. L. Rev. 119 (2024), doi:10.1007/s41020-024-00219-1.

Verma, 36 Nat'l L. Sch. India Rev., no. 1, art. 2 (2025), doi:10.55496/YRTF3099.

Nordvik et al., 37 Forensic Sci. Int'l: Digit. Investigation 301174 (2021), doi:10.1016/j.fsidi.2021.301174.

Neale, 45 Forensic Sci. Int'l: Digit. Investigation 301516 (2023), doi:10.1016/j.fsidi.2023.301516.

D'Anna et al., 11 Healthcare 634 (2023), doi:10.3390/healthcare11050634.

Patil et al., 14 Egypt. J. Forensic Sci. 12 (2024), doi:10.1186/s41935-023-00383-w.

SWGDE, Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers (2025).

Bureau of Police Research & Development, Standard Operating Procedures on New Criminal Laws (2024).