CCTV FOOTAGE AS ELECTRONIC EVIDENCE IN INDIAN COURTS: A CRITICAL ANALYSIS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Yogeshwaran B, B.Com. LL.B. (Hons.), SRM School of Law, SRM University.

V. Mahalingam, Assistant Professor, SRM School of Law, SRM University.

ABSTRACT

The accelerated growth of surveillance technology has made Closed Circuit Television (CCTV) footage one of the most frequently relied upon forms of electronic evidence in Indian criminal and civil proceedings. For decades, courts contended with an inadequate statutory framework, namely Sections 65A and 65B of the Indian Evidence Act, 1872 (IEA), that classified electronic records as mere secondary evidence, thereby burdening litigants with cumbersome certificate requirements. The enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on July 1, 2024, marks a typical shift by elevating electronic records to the status of primary evidence under Section 57 and by codifying a mandatory dual certification mechanism under Section 63 that now requires both a responsible person and an expert to jointly authenticate electronic records. This article critically examines the statutory framework governing the admissibility of CCTV footage under the BSA, traces the judicial evolution from Anvar P.V v. P.K Basheer (2014) through the landmark acquittal in Chandrabhan Sudam Sanap v. State of Maharashtra (2025), and evaluates the practical challenges that continue to best law enforcement and litigants in authenticating video surveillance evidence.

Keywords: Electronic Evidence, CCTV Footage, Bharatiya Sakshya Adhiniyam, Digital Evidence.

I. INTRODUCTION

The emergence of digital surveillance as an ubiquitous feature of modern urban life has irrevocably altered the evidentiary landscape of Indian Courts. Closed Circuit Television (CCTV) cameras have increased across railway stations, commercial establishments, banks, hospitals, and police station, generating enormous quantities of audio visual data that investigators and litigants routinely seek to produce as evidence. Yet for much of the last two decades, the law governing the admissibility of such footage was marked by confusion, conflicting judicial pronouncements, and procedural lacunae that, in certain cases, allowed perpetrators to escape conviction on technical grounds.

The Indian Evidence Act, 1872, a colonial era statute drafted long before the invention of digital technology, was amended in 2000 to accommodate electronic records, primarily through the insertion of Section 65A and 65B.[1] Section 65B stipulated that a printed copy or sorted version of an electronic record would be deemed a document only if accompanied by a certificate from a person occupying a responsible official position. However, courts were sharply divided on whether this certificate was a condition precedent to admissibility or a mere procedural requirement that could be waived. The resulting jurisprudential uncertainty culminated in a series of Supreme Court pronouncements, mostly notably Anvar P.V v. P.K Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), that attempted, with mixed success, to settle the law.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), passed by Parliament on December 25, 2023 and brought into effect on July 1, 2024, represents the first comprehensive rebuild of Indian evidence law in over 150 years.[2] The BSA not only replaces the IEA in its entirety but introduces several critical reforms to the treatment of electronic evidence, it reclassifies electronic records stored on semiconductor memory and communication devices , and codifies a new dual certificate requirement that mandates a hash value as part of the authentication certificate.[3] These changes have profound implications for how CCTV footage is tendered, authenticated and evaluated in Indian courts.

This article proceeds in six parts. After this introduction, Part II surveys the historical

[1] Indian Evidence Act, No of 1872, section 65B(India).
[2] Bhaaratiya Sakshya Adhiniyam, No. 47 of 2023.
[3] PRS Legislative Research, The Bharatiya Sakshya Bill, 2023 (2023), https://prsindha.org/billtrack/the-bharatiya-sakshya-bill-2023.

evolution of electronic evidence law in India. Part III examines the specific statutory provisions of the BSA governing CCTV footage, focusing on Sections 57, 61, 62, and 63. Part IV undertake a detailed analysis of the judicial treatment of CCTV evidence from 2005 to 2025. Part V evaluates the practical challenges under the new regime, including the dual certification requirement and chain of custody. Part VI offers conclusion and policy recommendations.

II. HISTORICAL EVOLUTION OF ELECTRONIC EVIDENCE LAW IN INDIA

The story of electronic evidence in India begins, somewhat inconsistent, with a statute drafted in 1872. The Indian Evidence Act, convinced by Sir James Fitzjames Stephen and modeled on English evidence law, defined document to include any matter expressed or described upon any substance by means of letters, figures or marks. This definition, while capacious in its time, made no provision for electronic stored information, a technology that lay nearly a century in the future.

The Information Technology Act, 2000, inserted Sections 65a and 65B into the IEA, providing the first statutory framework for electronic records. Under Section 65B, a computer output, defined as information printed on paper, stored, recorded or copied in optical or magnetic media, was deemed admissible as a document provided that four conditions were satisfied: (i) the computer was in regular use during the relevant period; (ii) information of the kind contained in the record was regularly fed into the computer; (iii) the computer was operating properly; and (iv) the record was a reproduction of the information fed into it. Additionally, Section 65B(4) required that a certificate be furnished by a person occupying a responsible official position, identifying the record and describing the manner of its production.

The first significant judicial test of Section 65B came in state (NCT of Delhi) v. Navjot Sandhu (2005), the parliament Attack case, where the Supreme Court held that electronic evidence could be admitted through oral testimony even without a Section 65B certificate.[4] This interpretation, which essentially read down the mandatory certification requirement, created a precedent that was widely followed by lower courts. However, the judgement was subsequently criticized for failing to give proper effect to the statutory language.

The matter came before a three judge bench of the Supreme Court in Anvar P.V v. P,K. Basheer & Ors. (2014), arising from an election petition where the appellant sought to rely on

[4] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600(India).

CDs containing campaign materials without furnishing the requisite Section 65B certificate.[5] The Court, in a judgement of considerable importance, held that 'any documentary evidence by way of an electronic record under the Evidence Act, in view of Section 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B' and expressly overruled Navjot Sandhu.[6] The Court further clarified that if the original device, a laptop, tablet or mobile phone, was produced directly in court, the certificate was unnecessary, since such production constituted primary evidence under Section 62 of the IEA.

Anvar P.V was followed by Shafhi Mohammad v. State of Himachal Pradesh (2028), where a division bench controversially held that the certificate requirement could be relaxed where the party producing the evidence was not in control of the device.[7] This created fresh uncertainty. The matter was finally put to rest by a three judge bench in Arjum Panditrao Khatkar v. Kailash Kushanrao Gorantyal (2020), which reaffirmed the correctness of Anvar P.V., overruled Shafhi Mohammad, and held that the section 65B(4) certificate was an absolute condition precedent to admissibility of secondary evidence by way of electronic records.[8] The Khotkar judgement also directed that appropriate riles for chain of custody, metadata preservation, and record retention be framed under the Information Technology Act, 2000.

III. THE STATUTORY FRAMEWORK UNDER THE BHARATIYA SAKSHYA ADHINIYAN, 2023.

A. The Definition Revolution: Electronic Records as Documents.

One of the most foundational changes introduced by the BSA is the redefinition of the word 'document' to expressly include electronic and digital records. Section 2(d) of the BSA, read with its Illustration (vi), provides that documents include electronic records on emails, sever logs, documents on computers, laptops or smartphones, messages, websites, voice mail messages stored on digital devices, and, crucially for present purposes, audio and video recordings stored on such devices. CCTV footage, which is inherently an audio, visual recording stored on a digital video recorder or a hard drive, thus falls squarely within the definition of document under the BSA.

[5] Anvar P.V v. P.K Basheer & Ors., (2014) 10 SCC 473 (India).
[6] Anvar P.V., supra note 3.
[7] Shafhi Mohammad v. State of Himachal Pradesh, (2028) 2 SCC 801 (India)
[8] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Or4s., (2020) 7 SCC 1 (India).

B. Primary Evidence Status Under Section 57.

Perhaps the single most significant change for CCTV evidence is the reclassification of electronic records as primary evidence under Section 57 of the BSA.[9] Under the IEA, electronic records were treated as secondary evidence, which meant the litigants were required to satisfy the Section 65B conditions on each occasion. The BSA departs from this approach by providing that electronic or digital records stored simultaneously or sequentially in multiple files are primary evidence, with each stored copy being equivalent to an original document, provided the record is produced from proper custody.

C. The Admissibility Conditions Under Section 63.

Section 63 of the BSA is the legislative heir of Section 65B of the IEA and governs the conditions under which computer output, including CCTV footage, may be admitted as evidence.[10] The section retains the four substantive conditions from Section 65B(2): (i) the device was in regular use during the relevant period; (ii) information of the relevant kind was regularly fed into it in the ordinary course of activity; (iii)the device was operating properly; and (iv) the record is a reproduction of the information so fed.

D. The Dual-Certification Requirement and Hash Values.

The most technically demanding innovation introduced by the BSA is the dual-certification requirement under Section 63(4) read with the Schedule. Under the old IEA, a single certificate from a person occupying a responsible official position sufficed. The BSA now requires two separate certificates: Part A, to be furnished by the person who generated or produced the electronic record (such as the CCTV operator or the facility manager), and Part B, to be furnished by an expert.[11] Critically, both Parts A and B of the certificate must state the hash value of the electronic record, along with specific cryptographic algorithm used, SHA1, SHA256, MD5, or another legally acceptable standard.

IV. JUDICIAL TREATMENT OF CCTV FOOTAGE: FROM NAVJOT SANDHU TO CHANDRABHAN SANAP.

A. The Pre-BSA Jurisprudence.

[9] BSA, supra note 1, § 57.
[10] BSA, supra note 1, § 63(1).
[11] BSA, supra note 1, § 63(4)(c) & Schedule.

The judicial treatment of CCTV footage in India has followed a unsettled path over the past two decades. As noted above, Navjot Sandhu (2005) allowed the admission of electronic records without a certificate, creating a permissive environment that was widely exploited.[12] Anvar P.V. (2014) corrected this by insisting on strict compliance with Section 65B, but courts continued to struggle with the primary-versus-secondary evidence distinction, particularly in CCTV cases.

The Madras High Court's decision in K. Ramajayam @ Appu v. Inspector of Police (2016) is particularly instructive. In that case, CCTV cameras installed in a jewellery shop captured the accused committing murder and rubbery. The footage was examined by a Scientific Officer of the Tamil Nadu Forensic Science Department, who analysed the DVR and provided a detailed report.[13] The Courts held that since the accused was clearly caught on camera during the commission of his offence, the CCTV footage constituted direct electronic evidence. The Court also affirmed that Memory Card, Hard Disks, CDs, and Pen Drives containing relevant data in electronic form are documents within the meaning of Section 3 if IEA, and upheld the conviction on the basis of footage, albeit commuting the death sentence to life imprisonment.

B. CCTV as a Tool Accountability: Paramvir Singh Saini v. Baljit Singh (2020)

While the cases discussed above concern CCTV footage as evidence against accused persons, the Supreme Court has also recognized the dual role of surveillance cameras as instruments of institutional accountability. In paramvir Singh Saini v. Baljit Singh (2020), a three-judge bench led by Justice R. F Nariman issued comprehensive directions mandating the installation of CCTV cameras al all police stations, lock-ups, corridors, inspector's rooms, and sub-inspector's rooms across the country.[14] This judgement was grounded in Article 21 and 22 of the Constitution and built upon the earlier directions in D.K. Basu v. State of West Bengal 2015).[15]

The Court specified that CCTV cameras must be equipped with night vision and must record audio as well as video. The footage recorded must be preserved for minimum period of six

[12] Anvar P.V., supra note 3 (The Court overruled State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600, finding that the earlier judgment had failed to properly appreciate Sections 59 and 65A of the Indian Evidence Act).
[13] K. Ramajayam @ Appu v. The Inspector of Police, (2016) Crl. A. 110 of 2015 (Madras High Court, India).
[14] Paramvir Singh Saini v. Baljit Singh & Ors., SLP (Crl.) No. 3543 of 2020 (Supreme Court of India, Dec. 2, 2020).
[15] D.K. Basu v. State of West Bengal, (2015) 8 SCC 744.

months. The Court further directed the Constitution of State-Level and District-Level Oversight Committees to review the footage and publish periodic reports on findings of human rights violations. The judgement is significant in the present context because it establishes CCTV footage not merely as a tool of prosecution, but as a constitutional safeguard against custodial abuse, a dual evidentiary function that raises novel questions about the chain of custody and certification of police-station footage that may later be used as evidence by either the state or the accused.

V. PRATICAL CHALLENGE AND CRITICAL ANALYSIS

A. The Chain of Custody Problem.

One if the most practical challenge in CCTV evidence is the establishment of an unbroken chain of custody from the moment of recording to the moment of production before the court.[16] In a typical case, CCTV footage passes through multiple hands: the facility manager or security officer who oversees the recording system, the first responder police officer who seizes the DVR or extracts the footage, the forensic examiner who analyses and certifies the footage, and ultimately the court official who marks it as an exhibit. Any gap or irregularity in this chain an opportunity for the defence to challenge the authenticity and integrity of the footage.

B. The Ambiguity of 'Expert' Under Part B of the Section 63 Certificate.

As noted above, the BSA's requirement of a Part B expert certificate introduces a layer of technical accountability that was absent from the IEA framework. However, the statute's failure to define who qualifies as an 'expert' for this purpose is a significant drafting lacuna.[17] The concern is not merely academic: if courts consistently require a notified forensic examiner under section 79A of the IT Act, 2000 to sign Part B, the practical burden on litigants, particularly in districts without forensic laboratories, could become prohibitive. Conversely, if any technically knowledgeable person is accepted as an 'expert', the certification requirement may be reduced to a formality that fails to provide the intended assurance of authenticity.

[16] Md. Imran Wahab, Judicial Examination of CCTV Footage as Evidence in Courts, Legal Service India (Sept. 1, 2025), https://www.legalserviceindia.com/Legal-Articles/judicial-examination-of-cctv-footage-as-evidence-in-courts/.
[17] Naavi, Section 63 of Bharatiya Sakshya Adhiniyam, Naavi.org (June 27, 2024), https://www.naavi.org/wp/section-63-of-bharatiya-sakshya-adhiniyam/.

C. Metadata, Timestamps, and the Integrity of Digital Forensics.

Modern CCTV systems embed a wealth of metadata within each recording, including timestamps, camera identification numbers, GPS coordinates (where applicable), and recording parameters. This metadata is of considerable evidentiary significance: it can establish when and where a recording was made, and can detect signs of tampering or editing.[18] Courts have increasingly recognized the importance of metadata analysis, and the Khotkar judgement specifically directed that rules be framed for the preservation of the meta data to avoid corruption.

However, India's forensic infrastructure remains underdeveloped relative to the scale of demand. Many police forensic laboratories lack the specialised software and trained personnel requirement for sophisticated metadata analysis. This creates an asymmetry between the legal standard, which increasingly demands technical rigour, and the institutional capacity available to meet it. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) takes a step in the right direction by mandating forensic evidence collection at crime scenes for offenses punishable with seven or more years of imprisonment under Section 176(3).[19] Section 105 of the BNSS further requires mandatory audio-visual recording of search and seizure operations,[20] which, if implemented faithfully, would generate a contemporaneous audio-visual record of the seizure of CCTV footage.

VI. CONCLUSION AND POLICY RECOMMENDATIONS

The Bharatiya Sakshya Adhiniyam, 2023, constitutes a significant and largely welcome modernisation of Indian evidence law as applied to electronic records, including CCTV footage. By reclassifying electronic records as primary evidence, expanding the definitional scope to cover semiconductor memory and communication devices, and codifying a hash-value-based dual-certification mechanism, the BSA provides a more principled and technologically complex framework than the IEA ever did. At the same time, the statute's ambiguities, particularly regarding the qualification of expert under Part B, and the persistent challenges of chain of custody management and forensic infrastructure pose substantial risks

[18] Wahab, supra note 15 (Discussing how courts increasingly examine hidden metadata, timestamps, and camera ID numbers embedded in CCTV footage).
[19] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 176(3) (India) [hereinafter BNSS]
[20] BNSS, supra note 41, § 105.

to the effective implementation of these reforms.

On the basis of the foregoing analysis, this article puts forward the following policy recommendations. First, the Supreme Court should issue practice directions classifying the minimum qualifications required of an 'expert' for purposes of Part B of the Section 63(4) certificate, distinguishing between cases involving simple CCTV extraction and those requiring complex forensic analysis. Second, the Ministry of Home Affairs should expedite the farming of comprehensive rules under Section 67C of the IT Act, 2000 governing the chain of custody for electronic evidence, building upon the BPRD SOP and directions in Arjun Panditrao Khotkar.[21] Third, India's forensic laboratories must be substantially upgraded in personnel and equipment to handle the growing volume of CCTV and other digital evidence, a process that the BNSS's mandatory forensic evidence collection provisions make all the more urgent.

Fourth, high courts should consider framing rules of procedure that require the certification of CCTV footage as a mandatory step in the investigation protocol, enforceable at the stage of charge-farming if not earlier. The lesson of Chandrabhan Sanap is unambiguous: where a prosecution is built on CCTV footage, the failure to certify that footage is not a curable procedural omission but a fundamental evidentiary defect that can, and in a capital case, did lead to acquittal. Fifth and finally, the legislature should consider where the current dual-certification framework should be supplemented by a presumption of authenticity for CCTV footage extracted by a police officer from a public surveillance system, where no specific allegation of tampering is made, in order to reduce the evidentiary burden without compromising the integrity of the fact-finding process.[22]

The integration of CCTV footage into the Indian evidentiary framework is an ongoing and evolving project. The BSA has laid a far stronger foundation that existed before, but statutory reform alone cannot substitute for institutional capacity, prosecutorial diligence, and judicial sensitivity to the dual imperatives of truth-finding and fair trial. The coming years of litigation under the new regime will determine whether the promise of Section 63 is fully realized or once again frustrated by the gap between law on paper and law in practice.

[21] Nikhil Pahwa, Revolutionising Digital Forensics: India's New Legal Frontiers, Bar and Bench (July 27, 2024), https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontiers.
[22] Nikhil Pahwa, Revolutionising Digital Forensics: India's New Legal Frontiers, Bar and Bench (July 27, 2024), https://www.barandbench.com/columns/revolutionizing-digital-forensics-indias-new-legal-frontie