CHHATTISGARH STATE JUDICIAL ACADEMY, BILASPUR (C.G.)

Divisional Judicial Seminar of Durg Division Held On 11.04.2026

Topic

An Overview of eSakshya with reference to newly statutory mandates. Admissibility mandates of eSakshya under Section 63 BSA

Prepared under guidance of

Respected **Shri K. Vinod Kujur** Principal District & Sessions Judge, Durg

Presented By:-

Shri Awadh Kishore, District & Additional Sessions Judge (FTC), Durg
Ravi Kumar Mahobia, I Ad. Judge to the Court of I C J Senior Division Durg
Aishwarya Diwan, XVII Civil Judge Junior Division, Durg

Acknowledgement

It is with profound gratitude and a deep sense of privilege that we present this paper on "An Overview of eSakshya with Reference to Newly Statutory Mandates. Admissibility Mandates of eSakshya Under Section 63 BSA." The journey from conceptualisation to completion of this work has been shaped and enriched by the generous guidance and support of several esteemed individuals, to whom we owe our sincerest acknowledgements.

At the outset, we express our heartfelt gratitude to the **Hon'ble High Court of Chhattisgarh** and the **Chhattisgarh State Judicial Academy** for organising this Divisional Judicial Seminar and for extending to us the distinguished opportunity to deliberate upon a subject of such contemporary legal significance. The Academy's continued commitment to judicial education and professional excellence has provided an invaluable forum for the exchange of ideas on evolving legal frameworks.

We place on record our deepest reverence and most respectful regards for **Respected Shri K. Vinod Kujur, Principal District and Sessions Judge, Durg, Chhattisgarh,** whose scholarly acumen, unwavering encouragement, and constructive supervision have been the guiding light throughout the preparation of this paper. His Honour's invaluable insights and consistent mentorship have not only elevated the quality of this work but have also broadened our understanding of the nuanced interplay between emerging technology and the law of evidence.

We acknowledge, with humility, that any merit this paper possesses is a reflection of the guidance we have been so fortunate to receive, while any shortcomings remain entirely our own.

Awadh Kishore, D & A S J (FTC), Durg
Ravi Kumar Mahobia, C J Senior Division Durg
Aishwarya Diwan, C J Junior Division, Durg

Abstract

This paper examines the admissibility framework for electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), with particular reference to Section 63 and the eSakshya portal. It traces the historical evolution of electronic evidence law in India from the Indian Evidence Act, 1872, through the Information Technology Act, 2000, to the comprehensive overhaul effected by the BSA. The paper analyses the key statutory conditions prescribed under Section 63(2), the mandatory certification requirement under Section 63(4), and the judicial flow of admissibility as a four-stage analytical model. It surveys landmark judicial pronouncements including Anvar P.V. v. P.K. Basheer, Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, and Sonu @ Amar v. State of Haryana, identifying doctrinal principles applicable to trial court adjudication. The paper further addresses emerging challenges posed by social media evidence, deepfake technology, cloud computing, and artificial intelligence. It concludes with a structured set of best practices for judges and advocates, emphasising that a coherent judicial approach requires the simultaneous exercise of legal rigour, practical wisdom, and technological awareness.

Table of Contents

Introduction & Historical Evolution

"E-Sakshya" (Electronic Evidence) refers to information stored or transmitted in digital form that is used as evidence in judicial proceedings. With the rapid digitisation of society, electronic evidence has become central to both civil and criminal adjudication.

India has recently undergone a major transformation in evidence law with the enactment of Bharatiya Sakshya Adhiniyam, 2023 replacing the colonial-era Indian Evidence Act, 1872

The new framework reflects a shift towards digital justice and technological integration.

Introduction:
Why Electronic Evidence Now Stands at the Centre of Adjudication.

The law of evidence has always moved with the dominant modes by which human beings create, preserve and communicate information. In an earlier era, facts were remembered orally, then recorded in writing, later typed into documents, and today they are generated, stored, transmitted and retrieved in electronic and digital form. The modern courtroom therefore cannot remain confined to the evidentiary assumptions of a paper dominated world. Emails, mobile messages, CCTV footage, call detail records, GPS data, social media posts, audio recordings, cloud backups, digital photographs, server logs and metadata now routinely arise in both civil and criminal adjudication.

The evolution of the law of evidence in India reflects, in many ways, the evolution of society itself. For over a century, evidentiary principles were designed to address disputes arising in a largely physical world—documents were tangible, communications were traceable, and authenticity could be visually or orally verified. However, the digital transformation of human interaction has fundamentally altered the nature of information, its creation, storage, transmission, and manipulation. In this context, the emergence of electronic evidence is not merely an incremental development but a paradigmatic shift that challenges the very foundations of traditional evidentiary law.

The Bharatiya Sakshya Adhiniyam, 2023 represents a conscious legislative response to this transformation. While it retains the structural continuity of earlier evidentiary principles, it introduces critical modifications that seek to integrate electronic evidence into the mainstream evidentiary framework. One of the most significant developments in this regard is the explicit inclusion of electronic and digital records within the definition of "document" This seemingly simple change carries profound implications, as it eliminates the earlier conceptual ambiguity regarding whether electronic records could be treated as documents at all.

Under the earlier framework, courts were often compelled to engage in interpretive exercises to accommodate electronic records within the existing definition of documents. The definition under the Indian Evidence Act, No. 1 of 1872, Section 3 was confined to matter expressed upon a substance through letters, figures, or marks.2 While this could be stretched to include certain forms of electronic output, it did not naturally encompass digital data in its native form. Consequently, electronic

evidence was often treated as an extension of documentary evidence rather than as a category deserving independent recognition.

The new statutory framework removes this ambiguity by unequivocally recognising electronic and digital records as documents in their own right. This recognition is not merely definitional; it alters the manner in which courts approach the admissibility, evaluation, and probative value of such evidence. By placing electronic records within the core definition of documents, the law acknowledges that the digital medium is no longer exceptional—it is the norm.

The new framework is intended to modernise the criminal justice process and to integrate evidence collection, storage and presentation through digital systems, including the eSakshya application and linked platforms such as CCTNS and ICJS. It also emphasizes that evidence now includes electronic and digital records and that judges are expected to work within a technologically integrated evidentiary environment.

This development also has a constitutional dimension. A criminal justice system does not serve its purpose merely by convicting the guilty and acquitting the innocent; it must do so through a fair, reliable and reasonably swift process. The move toward electronic evidence management and electronic hearings is therefore also a move toward procedural efficiency, transparency and integrity.

Historical Milestones

Year / Statute	Development
Indian Evidence Act, 1872	Documentary proof was essentially physical proof; no recognition of electronic records.
Information Technology Act, 2000	First major legislative milestone — granted legal recognition to electronic records (Section 2(1)(t)) and introduced Sections 65A and 65B into IEA.
Indian Evidence Act Amendment, 2000	Section 3 IEA widened the definition of documentary evidence by adding electronic records; Sections 65A, 65B, 67A, 73A, 81A, 85A-C, 88A inserted.
Bharatiya Sakshya Adhiniyam, 2023	Replaces IEA; expressly includes electronic/digital records in the definition of 'document' (S.2(1)(d)); Section 63 replaces Section 65B with enhanced provisions.
Bharatiya Nagarik Suraksha Sanhita, 2023	Replaces CrPC; mandates audio-video recording of search/seizure (S.105); integrates eSakshya portal, CCTNS and ICJS into the criminal justice system.

The Historical Evolution of Electronic Evidence in India

The Indian Evidence Act, 1872 was drafted in an age when documentary proof was essentially physical proof. With rapidly developing technological environment, whereby technological gadgets like cell phones, tablets, laptops, etc. have become necessities and this has resulted in the way communications and transactions are made and stored.With the growth of computing and digital communication, the Information Technology Act, 2000 became the first major legislative milestone by granting legal recognition to electronic records. After that, certain amendments were incorporated in criminal laws. Section 65 A and Section 65 B were added in the Indian Evidence Act,1872 to govern the admissibility of electronic records.. Sec 3 IEA 1872 widened the definition of documentary evidence by adding electronic records in it and certain other words like electronic signature, electronic form, electronic records, information, secure digital signature, etc were also added by mentioning that they will have the same meaning which is assigned to them in IT Act ,2000.

The earlier law, however, generated substantial litigation because courts and lawyers struggled with several recurring questions: What is the "original" of a digital record? Is a printout primary or secondary evidence? When is a certificate mandatory? What happens if the party producing the record does not possess the original device? What is the status of copied footage, chats, compact discs and call records?

The Centrality of Electronic Evidence in Contemporary Adjudication One of the reasons electronic evidence became a difficult

subject is that digital material does not behave like a conventional paper document. A digital file may exist on a hard disk, a server, a cloud backup, a phone, a mirror image, a pen drive, or a printed copy. It may be created by a chain of systems rather than by a single machine. It may also be altered invisibly. The old paperbased distinction between original and copy therefore needed conceptual modification.

It also necessitates a re-examination of the classical distinction between primary and secondary evidence. Traditionally, primary evidence referred to the original document itself, while secondary evidence was admissible only under specific circumstances, such as loss or unavailability of the original. This distinction was premised on the assumption that an original document possesses inherent reliability, while copies are susceptible to inaccuracies.

This is why the law gradually developed a special rule for electronic records rather than forcing them into ordinary categories of documentary evidence.

In the digital context, this assumption becomes problematic. Electronic records do not exist in a singular, immutable form. A digital file may exist simultaneously in multiple identical copies, each indistinguishable from the other. A document stored on a server may be accessed, copied, and transmitted without any degradation in quality. In such circumstances, the very notion of an “original” becomes conceptually unstable.

This shift from form to process is perhaps the most significant conceptual development in the law of electronic evidence. In traditional evidence law, authenticity could often be inferred from the document itself or from the testimony of witnesses. In contrast, the authenticity of

electronic evidence depends largely on the integrity of the system that produced it. The reliability of the evidence is therefore linked not to the document alone but to the entire technological ecosystem in which it was created.

This necessitates a deeper judicial engagement with the conditions under which electronic records are generated. Courts must now consider factors such as:

- Whether the system was functioning properly.
- Whether the data was recorded in the ordinary course of activities.
- Whether the record has been preserved without alteration.
- Whether the process of extraction or reproduction is reliable.

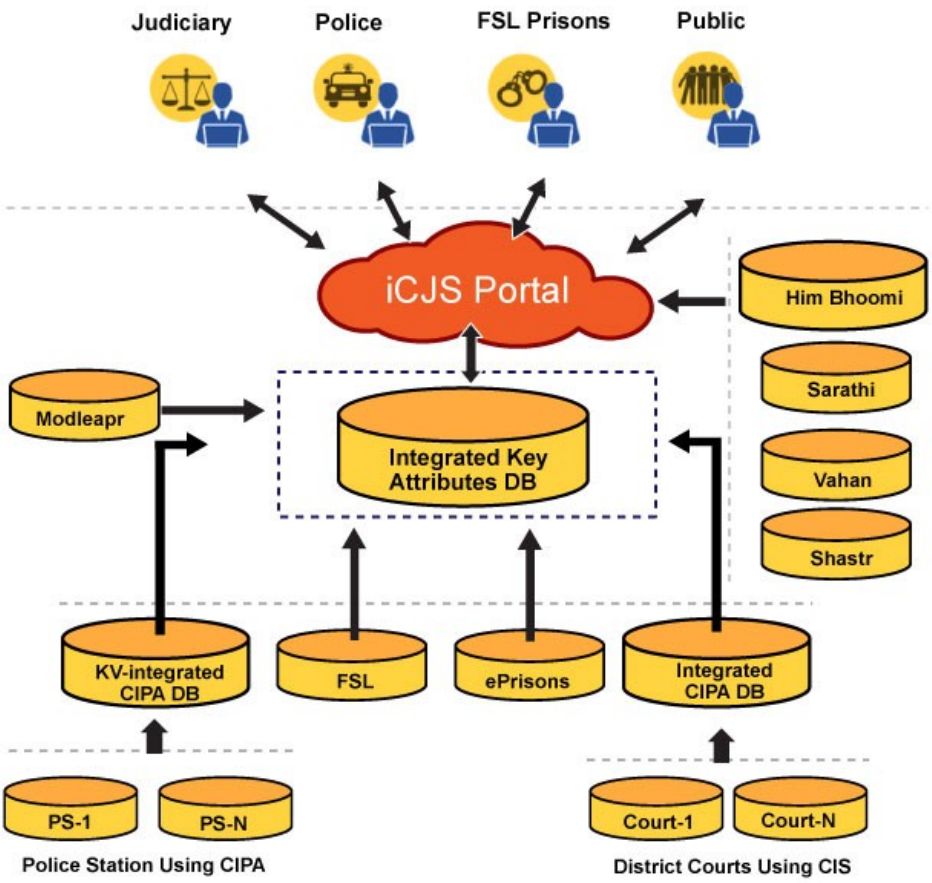
These considerations underscore the fact that electronic evidence cannot be assessed in isolation. It must be evaluated in the context of its technological environment.

The Paradigmatic Shift - From Paper to Digital

The digital transformation of human interaction has fundamentally altered the nature of information—its creation, storage, transmission, and manipulation. The emergence of electronic evidence is not merely an incremental development but a paradigmatic shift that challenges the very foundations of traditional evidentiary law.

A digital file may exist on a hard disk, a server, a cloud backup, a phone, a mirror image, a pen drive, or a printed copy. It may be created by a chain of systems rather than a single machine. It may also be altered invisibly. The old paper-based distinction between original and copy

therefore needed conceptual modification. The shift is from form to process — the authenticity of electronic evidence depends on the integrity of the entire technological ecosystem in which it was created.



Statutory Framework

The Information Technology Act, 2000

The Information Technology Act, 2000 amended the definition of "evidence" under the Indian Evidence Act, 1872 to include electronic records. **Section 2(1)(t) of the IT Act 2000** defines **"electronic record"** which reads as thus: **"electronic record"** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche;" In other words an electronic record is a digital representation of information that can be created, modified, stored or shared by a computer system. Electronic records can include text, graphics, audio, data, and more.

Sec 3 IEA 1872 widened the definition of documentary evidence by adding electronic records in it and certain other words like electronic signature, electronic form, electronic records, information, secure digital signature, etc were also added by mentioning that they will have the same meaning which is assigned to them in IT Act, 2000.

Specific provisions were included

Section 22A IEA 1872 -

When oral admission as to contents of electronic records are relevant.

Section 45A IEA 1872 -

Opinion of Examiner of Electronic Evidence.

Section 47A IEA 1872 -

Opinon as to electronic signature, when relevant.

Section 65A IEA 1872 -

Special provisions relating to electronic records.

Section 65B IEA 1872 -

Admissibility of electronic records.

Section 67A IEA 1872 -

Proof as to electronic signatures.

Section 73A IEA 1872 -

Prood as to verification of digital signature.

Section 81A, 85A to 85C IEA 1872 -

Presumptions relating to electronic records.

Section 88A IEA 1872 -

Presumption regarding electronic messages.

Additionally, the law recognises that oral evidence cannot ordinarily be used to prove the contents of electronic records, thereby reinforcing the importance of documentary proof.

Under The Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 introduces a more comprehensive framework for electronic evidence. It expands the definition of "document" to explicitly include electronic and digital records.

Definition of 'Document' — Section 2(1)(d) BSA

Section 2(1)(d) BSA defines **'document'** as any matter expressed, recorded or described on a substance using letters, figures, marks or other means — expressly including electronic and digital records such as emails, server logs, documents on computers, messages, websites and voice mail messages.

This eliminates the ambiguity under Section 3 IEA, 1872, where the definition was confined to 'matter expressed upon a substance through letters, figures, or marks' — which did not naturally encompass digital data in its native form.

Definition of 'Evidence' — Section 2(e) BSA

The definition of evidence under BSA expressly includes:

- Oral Evidence — all statements, including those given electronically, which the Court permits or requires to be made before it.
- Documentary Evidence — all documents, including electronic or digital records, produced for the inspection of the Court.

The definition of evidence has also been broadened to include

statements made electronically.

This represents a significant shift, as such statements are now treated as oral evidence within the statutory framework.

Electronic records such as emails, server logs, messages, location data and voice recordings are expressly recognised as documents, thereby eliminating earlier ambiguities.

Primary and Secondary Evidence — Sections 57 & 58 BSA

Primary Evidence - Section 57 BSA	Secondary Evidence - Section 58 BSA
Explanation 4: Each file stored simultaneously or sequentially across multiple files is primary evidence. **Explanation 5:** Electronic records produced from proper custody are primary evidence unless disputed. **Explanation 6:** Video simultaneously stored and broadcast — each stored recording is primary evidence. **Explanation 7:** Every automated storage, including temporary files, in a computer resource is primary evidence.	Encompasses certified copies, copies made by mechanical processes, oral and written admissions, oral accounts of document contents. Relevant when the original document cannot be produced for Court inspection. **Section 63 BSA is the complete code for admitting secondary electronic evidence.**

Relevancy vs Admissibility — A Critical Distinction

Relevancy vs Admissibility:

Relevancy pertains to whether a fact is logically connected to the issue in dispute.

Admissibility relates to whether such evidence can legally be received by the Court.

An electronic record may be relevant but inadmissible if it fails to meet the statutory requirements of Section 63. Provisions governing admissibility do not determine relevancy.

A clear distinction must be drawn between relevancy and admissibility of evidence. Relevancy pertains to whether a fact is logically connected to the issue in dispute. Admissibility relates to whether such evidence can legally be received by the court. In the context of electronic evidence, relevancy must first be established. Thereafter, admissibility is determined in accordance with statutory provisions. It is important to note that provisions governing admissibility do not determine relevancy. An electronic record may be relevant but inadmissible if it fails to meet statutory requirements.

Under the Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) replaces the Code of Criminal Procedure, 1973 (CrPC). It introduces several new statutory mandates relating to eSakshya — embedding digital evidence collection and management as a mandatory component of the criminal justice process.

Section 105 BNSS — Mandatory Audio-Visual Recording of Search & Seizure

Section 105 BNSS, 2023 provides:

The process of conducting search of a place or taking possession of any property, article or thing, including the list of all things seized in the course of such search and seizure and signing of such list by witnesses, shall be recorded through any audio-video electronic means preferably by cell phone, and the police officer shall without delay forward such recording to the District Magistrate, Sub-Divisional Magistrate or Judicial Magistrate of the First Class.

Compare with Section 100 CrPC: The old provision merely permitted panchnama; Section 105 BNSS makes audio-video recording mandatory.

Section 176 BNSS — Procedure for investigation

Section 176(1) .....

Provided further that in relation to an offence of rape, the recording of state-ment of the victim shall be conducted at the residence of the victim or in the place of her choice and as far as practicable by a woman police officer in the presence of her parents or guardian or near relatives or social worker of the locality and such statement may also be recorded through any audio-video electronic means including mobile phone.

Section 176(3) On receipt of every information relating to the commission of an offence which is made punishable for seven years or more, the officer in charge of a police station shall, from such date, as may be notified within a period of five years by the State Government in this regard, cause the forensic expert to visit the crime scene to collect forensic evidence in the offence and also cause videography of the pro-cess on mobile phone or any other electronic device:

Provided that where forensic facility is not available in respect of any such offence, the State Government shall, until the facility in respect of that matter is developed or made in the State, notify the utilisation of such facil-ity of any other State.

Section 183 BNSS — Recording of confessions and statements

Section 183 BNSS provides that:

Any confession or statement made under this sub-section may also be recorded by audio-video electronic means in the presence of the advocate of the person accused of an offence.

Provided also that if the person making the statement is temporarily or perma-nently, mentally or physically disabled, the statement made by the person. with the assistance of an interpreter or a special educator, shall be re-corded through audio-video electronic means preferably by mobile phone;

Section 193 BNSS — Report of police officer on completion of investigation

Section 193(3)(ii) the police officer shall, within a period of ninety days, inform the progress of the investigation by any means including through electronic commu-nication to the informant or the victim;

193(8) .....

Provided that supply of report and other documents by electronic communication shall be considered as duly served.

Section 230 BNSS — Supply to accused of copy of police report and other document

Provided further that if the Magistrate is satisfied that any such document is voluminous, he shall, instead of furnishing the accused and the victim (if represented by an advocate) with a copy thereof, may furnish the copies through electronic means or direct that he will only be allowed to inspect it either personally or through an advocate in Court:

Provided also that supply of documents in electronic form shall be considered as duly furnished.

Integration with eSakshya Portal — CCTNS & ICJS

Platform	Role in eSakshya Framework
eSakshya App	Secure upload, storage and Hash Value generation for audio-visual recordings under Section 105 BNSS.
CCTNS	Crime and Criminal Tracking Network & Systems — links FIR data with electronic evidence repositories.
ICJS	Interoperable Criminal Justice System — enables courts, police, prisons and forensic labs to access electronic evidence seamlessly.

Under the CG eSakshya Management Rules, 2025

The Governor of Chhattisgarh is pleased to make the following rules under the Bharatiya Nagarik Suraksha Sanhita, 2023 after consultatin with the High Court of Chhattisgarh, namely:-

Rules

Short title and commencement -

(1) These rules may be called the **Chhattisgarh eSakshya Management Rules, 2025.**

(2) They shall come into force from the date of their publication in the Official Gazette.

Definitions -

(1) In these rules, unless the context otherwise requires, -

(a) **"CCTNS"** means Crime and Criminal Tracking Network and Systems, a system software used by the Police for the collection of data and execution of instructions;

(b) **"CIS"** means Case Information System, a system software used by the District Judiciary and High Courts for the collection of data and execution of instructions;

(c) **"eSign"** means authentication of any electronic record by a subscriber or court, by means of the electronic technique specified in the Second Schedule of the Information Technology Act, 2000 (No. 21 of 2000) and includes digital signature. Also, when a process or report generated in

electronic form is authenticated by means of electronic signature, it shall be deemed to be authenticated by signature of the person who affixed the electronic signature;

(d) **"High Court"** means the High Court of Chhattisgarh;

(e) **"ICJS"** shall mean Inter-operable Criminal Justice System, a software presently in operation for transfer of information among various pillars of criminal justice system, which includes Investigating agencies, courts, correctional homes, forensic laboratories, prosecution; and any other stakeholder as notified by the Central Government;

(f) **"Investigating Officer"** means any police officer or any other person authorized by a competent authority or empowered to undertake investigation for any offence;

(g) **"Sakshya"** means any evidence collected/recorded as a document through eSakshya Mobile Application. Sakshya consists of video recording(s), photograph(s), photograph(s) of witness(s) and photograph of the investigating/recording officer. All evidence recorded through eSakshya Mobile Application shall generate a secure packet of the event (hereinafter referred to as "eSakshya Packet") with a unique ID called SID, a unique 16 digit ID (SID) with opening, closing time stamp and geo-location. Each SID and its contents will have unique hash value to ensure integrity. Sakshya will be stored in immutable storage;

(h) **"Sanhita"** means the. Bharatiya Nagarik Suraksha Sanhita,

2023 (No. 46 of 2023).

(2) Words and expressions used, but not defined in these rules shall have the same meaning as assigned to them in the Bharatiya Nagarik Suraksha Sanhita, 2023 (No. 46 of 2023); the Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023); the. Bharatiya Sakshya Adhiniyam, 2023, (No. 47 of 2023) and the Information Technology Act, 2000 (No. 21 of 2000).

3. Every Investigating Officer shall record all video and photo evidence as required under Section 105, 173, 176, 180, 185, and 497 of the Sanhita through the eSakshya Mobile Application.

4. Investigating Officer shall generate a certificate contained in Section 63(4) (c) of Part A of Schedule of the Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023) through the eSakshya Mobile Application. All Certificates will be eSigned.

5. Investigating Officer shall link SID with the concerned FIR number/GD number generated through CCTNS.

6. The Sakshya uploaded to immutable storage shall be construed to be forwarded to Magistrate as required under Section 105 and 185 of the Sanhita.

7. The courts can view and manage all Sakshya concerning to their jurisdiction in the CIS application/Sakshya portal on ICJS.

8. The courr may permit sharing of Sakshya with accused and the victim (if represented by an advocate) as per the provisions under

Section 230 of the Sanhita.

9. eSakshya packet will be archived after completion of trial and will be moved to Archival mode.

10. Nothing in these rules shall be deemed to limit the power of the Courts to view the Sakshya by the Court.

11. These rules shall be in addition to, not in derogation of any other law or rules for time being in force for accepting and managing Sakshya by the Court in terms of the provisions of Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023).

Changes Brought Through Judicial Pronouncements

In one line of reasoning, the courts adopted a flexible approach, allowing electronic evidence to be admitted even in the absence of strict compliance with procedural requirements. This approach was driven by the concern that rigid adherence to technical requirements could impede the administration of justice **State (NCT of Delhi) Vs. Navjot Sandhu, (2005) 11 SCC 600** However, this flexibility also raised concerns about the reliability of electronic evidence and the potential for misuse.

A more stringent approach was subsequently adopted, emphasising the mandatory nature of statutory requirements governing

electronic evidence. In **Anvar P.V. Vs. P.K. Basheer & Others (2014) 10 SCC 473** the Hon'ble Supreme Court held that compliance with the prescribed conditions is essential for the admissibility of electronic evidence and that these provisions constitute a complete code.[1] This position was reaffirmed in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1**, where the Court underscored the necessity of certification and rejected the dilution of statutory safeguards.

These decisions reflect a judicial preference for reliability over flexibility. The Court recognised that while electronic evidence is indispensable in modern litigation, it must be subjected to rigorous standards to prevent misuse. The insistence on compliance with statutory conditions is therefore not a mere technicality but a substantive requirement aimed at preserving the integrity of the judicial process.

1

Conceptual Foundations of e-Sakshya

The Emergence of e-Sakshya : A Systemic Approach to Digital Evidence

Meaning and Scope of e-Sakshya

e-Sakshya represents a structured approach to handling electronic evidence within the criminal justice system. It is not limited to a single application or tool; rather, it encompasses the entire lifecycle of electronic evidence from collection at the scene of occurrence to presentation before the court.

The system is designed to ensure that evidence is captured accurately, preserved securely, and transmitted in a manner that maintains its integrity. By standardising procedures, it reduces the risk of human error and minimises the possibility of tampering.

Collection of Evidence Through Digital Means

One of the most critical stages in the evidentiary process is the collection of material at the scene of occurrence. e-Sakshya systems enable investigating officers to record the scene through photographs and videography in a systematic manner. The process typically involves capturing multiple angles, documenting relevant objects, and recording environmental details.

The use of digital tools ensures that evidence is captured contemporaneously, reducing the likelihood of subsequent fabrication or alteration. Features such as geotagging and timestamping further enhance the reliability of the recorded material.

Preservation and Chain of Custody

Preservation of electronic evidence requires careful handling because digital data can be easily altered or corrupted. e-Sakshya systems address this issue by providing secure storage mechanisms and maintaining a clear chain of custody.

The concept of chain of custody refers to the documented history of the evidence from the moment it is collected until it is presented in court. Maintaining an unbroken chain of custody is essential to establish that the evidence has not been tampered with.

Integration with Judicial Systems

Modern evidence management systems are integrated with digital platforms used by investigative agencies and courts. This integration enables seamless transmission of evidence, reduces delays and enhances transparency. Courts are able to access and examine electronic records directly through digital interfaces, thereby improving efficiency in trial proceedings.

Statutory Recognition of e-Sakshya under the BSA

BSA makes two significant changes.

• The definition of "document" under Section 2(1)(d) now expressly includes "electronic and digital records."

• Second, the law relating to electronic evidence is correspondingly reframed. Section 63 works through a legal fiction: if the statutory conditions are satisfied, the electronic output is "deemed" to be a document and becomes admissible without further proof or production of the original source device.

That is a major doctrinal move because it places properly proven electronic material on the footing of documentary proof without insisting on production of the originating hardware. Digital evidence now holds stronger, more central legal salience under the new framework. Although the full page could not be fetched in this environment, the retrievable result reinforces the same broader point: the BSA is not treating digital material as a peripheral anomaly, but as a core evidentiary category requiring coherent doctrine.

The recognition of electronic records as primary evidence in specific circumstances represents an attempt to address situations where strict compliance with procedural requirements may not be feasible. These provisions suggest a movement towards a more balanced approach that seeks to harmonise reliability with accessibility. Another significant development is the expansion of the scope of expert evidence. The law now recognises the relevance of expert opinion in "any other field," thereby accommodating the growing importance of technological expertise in judicial proceedings. By expert it means, the person has to have experience

in the the field. This is particularly important in the context of electronic evidence, where technical complexities often require specialised knowledge.

Expansion of the Definition of "Document"

The Bharatiya Sakshya Adhiniyam expands the definition of "document" to include electronic and digital records. This is a fundamental change because it removes any ambiguity regarding the status of electronic material as documentary evidence.

Inclusion within the Definition of "Evidence"

The definition of evidence under the BSA expressly includes statements made in electronic form and documents in the form of electronic or digital records. This ensures that electronic evidence is treated on par with traditional forms of evidence.

Legal Effect of Electronic Records

The law recognises that electronic records have the same legal effect, validity and enforceability as other documents, subject to compliance with statutory conditions. This recognition reflects an acknowledgment of the central role of digital data in modern transactions and interactions.

The Core Provision on Admissibility S 63 BSA : Detailed Analysis

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 constitutes the principal provision governing the admissibility of electronic records. It provides a structured framework that addresses both the conceptual and practical challenges associated with digital evidence.

Mirroring Section 65B IEA with significant enhancements address modern technological realities.

Section 63(1) BSA, 2023 — The Deeming Fiction

Section 63(1) — The Core Provision:

Any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory, produced by a computer or any communication device, shall be deemed to be a document, if the conditions mentioned in this section are satisfied, and shall be admissible in any proceedings without further proof or production of the original.

Key Innovation: 'Communication Device' is expressly included — covering mobile phones, smartphones, tablets — an addition absent in Section 65B IEA.

The term 'deemed' creates a legal fiction: electronic output, otherwise secondary evidence, is elevated to the status of primary documentary proof conditional and not automatic.

Section 63(2) — Four Conditions Ensuring Reliability

The following four conditions must be fulfilled:

(a)	Regular Use of the Device: The computer output was produced during the period over which the device was used regularly to create, store or process information for the purposes of any activity regularly carried on by the person having lawful control over its use.
(b)	Ordinary Course of Activity: The information was regularly fed into the device in the ordinary course of the said activities — ensuring it is part of routine operations and not artificially introduced for purposes of litigation.
(c)	Proper Functioning: The device was operating properly during the material part of the said period; or if not, the malfunction did not affect the accuracy of the electronic record.
(d)	Integrity of Output: The information in the electronic record reproduces or is derived from such information fed into the computer or communication device in the ordinary course of the said activities.

Section 63(3) — Recognition of Modern Technological Systems

Where during any period the function of creating, storing or processing information was regularly performed by means of one or more computers or communication devices — whether in standalone mode, on a computer system or network, on a computer resource, or through an intermediary — all such computers or communication devices shall be treated as constituting a single entity.

New Addition in BSA (vis-à-vis Section 65B IEA):

Section 65B(3) IEA covered only storage and processing operations. Section 63(3) BSA additionally covers the creation operation and expressly includes intermediaries — bringing social media platforms, cloud services and third-party apps within the fold of electronic evidence jurisprudence. This is particularly important in cases involving cloud storage, server-based systems and networked databases.

Section 63(4) — The Mandatory Certificate

Section 63(4) mandates production of a Certificate whenever electronic evidence is submitted for admission. This is mandatory and not merely directory.

The Certificate must:

(a) Identify the electronic record containing the statement and describe the manner in which it was produced.

(b) Give particulars of the device involved, showing it was produced by a computer or communication device within Section 63(3).

(c) Deal with the conditions in Section 63(2) signed by a person in charge of the device or management of the relevant activities and an Expert.

Two-Factor Authentication - The Landmark Change:

Part A - To be filled by the party / police officer who has produced the electronic record.

Part B - To be filled by an Expert (Examiner of Electronic Evidence under Section 79A, IT Act, 2000).

The Certificate itself becomes evidence of the matters stated in it. This two-factor system removes the ambiguity of 'who, when and what' that plagued the Section 65B IEA regime.

Section 63(5) BSA —

For the purposes of this section, -

(a) information shall be taken to be supplied to a computer or communication device if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) a computer output shall be taken to have been produced by a computer or communication device whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment or by other electronic means as

referred to in clauses (a) to (e) of sub-section (3).

Certificate Requirement — Part A & Part B

Part - A (To be filled by the Party)	Part - B (To be filled by the Expert)
• Type of device (Computer/DVR/ Mobile/Flash Drive etc.).	• Type of device and digital record source
• Make, Model, Serial Number, IMEI/UIN/MAC/Cloud ID. • Hash Value of the electronic record (MD5/SHA-1/SHA-256).	• Make, Model, Serial Number, IMEI/UIN/MAC/Cloud ID • Hash Value of the digital record with algorithm used.
• Confirmation of lawful control and proper operation of device.	• Expert's designation and signature.
• Hash Report to be enclosed with the Certificate.	• Hash Report to be enclosed with the Certificate.

Judicial Principles on Certificate

- Certificate is mandatory (sine qua non) — Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- Absence of certificate renders electronic evidence inadmissible — State of Karnataka v. M.R. Hiremath, (2019) 7 SCC 515.

- Certificate can be produced at any stage of trial before the hearing is over — Arjun Panditrao; State of Karnataka v. T. Naseer, 2023 LiveLaw (SC) 965.
- Oral evidence cannot substitute the written certificate — Ravinder Singh v. State of Punjab, (2022) 7 SCC 581.
- Objection to mode of proof must be raised at trial stage and not at appellate stage — Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570.
- Call Detail Records Not Admissible Without S.65 Evidence Act Certificate - Pooranmal Vs. State of Rajasthan & Another 2026 LiveLaw (SC) 227

Hash Value — Significance and Procedure

A Hash Value is the 'digital fingerprint' of an electronic file. It is a unique alphanumeric string generated by applying a cryptographic hash algorithm to an electronic record. Even a minor change in the data — even a single bit — results in a completely different hash value, making tampering immediately detectable.

Legal Significance

- Proves data integrity: If the Hash Value of the original source data matches the copy produced before Court, the copy is authentic.
- Ram Kishan Fauji v. State of Haryana, (2016) SCC OnLine P&H 14198: If a CD cannot pass the hash value comparison test with the source, the transcript of its audio footage carries no evidentiary value.
- Mandatory inclusion in Part A and Part B of the Certificate under Section 63(4) BSA.
- By comparing hash values at different stages, courts can determine whether the data has been altered at any point in the chain of custody.

Hash Algorithms Recognised

Algorithm	Output Size	Status / Use
MD5	128-bit	Widely used; general purposes
SHA-1	160-bit	More secure than MD5
SHA-256	256-bit	Most recommended; highest security
Other (Legally Accepted Standard)	Varies	As approved by Court

How to Calculate Hash Value — Step-by-Step

1. Download and install WinMD5Free v1.20 from www.winmd5.com.
2. Open the WinMD5Free application.
3. Drag and drop the electronic file (video/audio/document) onto the application window, OR click 'Browse' and select the file.
4. The MD5 Hash Value will appear automatically in the 'Current file MD5 checksum value' field.
5. For SHA-256/SHA-1: Use HashCalc (same drag-and-drop procedure).
6. Record this Hash Value in the Certificate (Part A / Part B) and enclose the Hash Report.
7. To verify: paste the original source Hash Value in the 'verify' box and click 'Verify' — 'Match' confirms integrity.

Judicial Flow of Admissibility — A Functional Approach

For practical purposes, the judicial handling of electronic evidence may be conceptualised through a structured five-stage flow:

Stage	Inquiry
Stage 1 Identification	Determine whether the material qualifies as an electronic record. Printouts, screenshots and transcriptions must be recognised as deriving from underlying electronic systems — they must satisfy Section 63.
Stage 2 Admissibility	Examine whether Section 63 conditions are fulfilled — verify presence and adequacy of Certificate (Part A & Part B) and Hash Report.
Stage 3 Authentication & Integrity	Even where statutory conditions are met — assess whether the record is genuine and free from tampering; examine chain of custody and hash value match.
Stage 4 Probative Value	Determine weight of the evidence in context of the entire case — corroboration, consistency and contextual relevance.

This staged approach ensures that the Court does not conflate admissibility with reliability or probative value. Each stage serves a distinct function, and the integrity of the adjudicatory process depends on maintaining these distinctions.

For practical purposes, the judicial handling of electronic evidence may be conceptualised through a structured flow. While not codified in

statutory language, such a model assists in ensuring consistency and completeness in adjudication.

The first stage involves **identification**. The Court must determine whether the material sought to be introduced qualifies as an electronic record. This step is critical because parties often attempt to present electronic evidence in disguised forms, such as printouts or transcriptions, without acknowledging their digital origin. The Court must recognise that such materials derive their evidentiary value from underlying electronic systems and must therefore satisfy the requirements of Section 63.

Once identified, the Court proceeds to the second stage, namely **admissibility under statutory conditions**. At this stage, the Court examines whether the requirements of Section 63 have been fulfilled. This includes verifying the presence and adequacy of the certificate, as well as ensuring that the conditions relating to system integrity and data reliability are satisfied.

The third stage involves **authentication and integrity verification.** Even where the statutory conditions are met, the Court must assess whether the record is genuine and free from tampering. This requires an examination of the source of the record, the chain of custody, and any indications of alteration.

Authentication — Source and Attribution

The first and most fundamental inquiry is the question of authorship and origin. Authentication requires the Court to be satisfied that the record emanates from the source it purports to represent. Electronic

communications may be transmitted through devices that are shared, compromised, or impersonated. Email accounts may be accessed by multiple users; messaging platforms may be subject to spoofing; digital identities may be fabricated.

Courts must look for corroborative indicators:

- Metadata associated with the record
- IP address logs
- Device identification details (IMEI, MAC Address)
- Consistency with other evidence on record

Integrity of Data — Possibility of Tampering

Digital data can be modified without leaving visible traces, unlike physical documents. The law addresses this through Section 63(2)(c) — the device must have been functioning properly. However, courts must additionally examine the chain of custody.

Chain of Custody — Key Questions for the Court:

- Who handled the device at each stage from seizure to production before Court?
- Whether the transfer process was documented (Chain of Custody Proforma)?
- Whether safeguards (Hash Value generation) were in place to prevent alteration?

- Whether the Hash Value of the original source data matches the copy produced in Court?

  The absence of a clear chain of custody does not automatically render evidence inadmissible, but it significantly affects its weight.

Cross-Examination as a Tool

Cross-examination assumes a particularly critical role in cases involving electronic evidence. Effective cross-examination may reveal:

- Lack of personal knowledge of the certifying person regarding the system
- Inadequate understanding of the technical process
- Inconsistencies in the description of the record in the Certificate
- Failure to follow proper procedures — for instance, certificate asserts proper functioning but certifier had no knowledge of system's operational history
- Discrepancies in timestamps, inconsistencies in data entries, or irregularities in the process of extraction

Expert Testimony — Section 39 BSA

Section 39(1) BSA expands the scope of expert evidence by recognising expertise in 'any other field', thereby accommodating digital forensics and information technology. Experts may assist the Court in:

- Analysing metadata to determine authenticity
- Detecting signs of tampering or editing

- Explaining system logs and data structures
- Verifying reliability of extraction processes
- Providing opinion on hash value comparison and data integrity

Caution: Expert opinions are not conclusive — they are advisory. The judge must evaluate the reasoning underlying the expert's conclusions and assess whether it is consistent with other evidence on record. In cases of conflicting expert opinions, the Court must weigh credibility, qualifications, and methodology.

The final stage is **evaluation of probative value**. At this stage, the Court determines the weight to be accorded to the electronic evidence in light of the entire evidentiary record. This involves considering corroboration, consistency, and contextual relevance.

This staged approach ensures that the Court does not conflate admissibility with reliability or probative value. Each stage serves a distinct function, and the integrity of the adjudicatory process depends on maintaining these distinctions.

Electronic Evidence — Social Media, Deepfakes & Cloud Computing

Social Media and Digital Communications

The proliferation of social media and instant messaging platforms has introduced new complexities. Messages, images, and videos shared through WhatsApp, Instagram, Facebook, and similar platforms are increasingly relied upon in civil and criminal proceedings. These forms of evidence present unique challenges:

- The ease of creating fake accounts and impersonation
- Lack of centralised control over data and metadata
- Difficulty in establishing authorship beyond the account level
- Messages can be deleted, edited, or fabricated prior to screenshot

The mere production of a screenshot or printout is insufficient to establish authenticity. The Court must require:

- Verification of account ownership and device linkage
- Examination of device-specific data and metadata
- Section 63(4) Certificate with Hash Report
- Corroboration with other independent evidence

Dell International Services Pvt. Ltd. v. Adeel Feroze & Ors. — 2024 SCC OnLine Del 4576

Held :	Screenshots of WhatsApp conversations cannot be admitted as evidence unless accompanied by an electronic evidence certificate under Section 65B IEA (now Section 63 BSA, 2023).

Integrity of Data and Possibility of Tampering

Closely linked to authentication is the question of integrity. Even if the source of an electronic record is established, the Court must still be satisfied that the record has not been altered or tampered with. Digital data can be modified without leaving visible traces. Unlike physical documents, which may show signs of erasure or alteration, electronic records may be edited seamlessly. This creates a significant evidentiary risk. The law addresses this concern indirectly through the conditions prescribed under Section 63, which require that the system producing the record must have been functioning properly and that the data must have been recorded in the ordinary course of activities. However, these conditions alone may not be sufficient to dispel all doubts regarding integrity.

In practice, courts must examine the **chain of custody** of the electronic record. This involves tracing the movement of the record from its origin to its production before the court. Any unexplained gaps in this chain may raise doubts about the possibility of tampering. For example, if a video recording is extracted from a device and subsequently transferred across multiple storage media before being produced in court, the Court must examine:

- Who handled the device at each stage

- Whether the transfer process was documented
- Whether safeguards were in place to prevent alteration

The absence of a clear chain of custody does not automatically render the evidence inadmissible, but it significantly affects its weight.

Deepfakes and Manipulated Digital Content

Deepfake technologies enable the creation of highly realistic but entirely fabricated videos and audio recordings. These pose serious risks to the integrity of the judicial process. Traditional methods of assessing authenticity may be inadequate in detecting sophisticated manipulations.

While the statutory framework does not explicitly address deepfakes, Section 63 provides the foundation for judicial response — the emphasis on system integrity, proper functioning, certification and hash value can be extended to require forensic expert analysis for suspected deepfake evidence.

Cloud Computing and Distributed Storage

Data stored in cloud environments raises distinct questions:

- Who is the custodian of the data? — For Certificate purposes under Section 63(4), the service provider or the user?
- How can certification be obtained when data is distributed across multiple servers in different jurisdictions?
- Section 63(3) BSA addresses this by treating multiple

computers/systems as a single entity — but establishing reliability still requires certification by expert.

Artificial Intelligence — Evidentiary Uncertainty

AI-generated outputs — whether predictive analytics, automated decisions, or AI-drafted documents — raise fundamental questions: Can machine-generated outputs be treated as reliable evidence? How can courts assess algorithm accuracy? The principles of Section 63 — system integrity, reliability, and certification — provide the starting framework for addressing AI-generated evidence.

Judicial Evaluation, Evidentiary Testing, and Courtroom Application of Electronic Evidence

The admissibility of electronic evidence under Section 63 marks only the threshold of judicial inquiry. The more demanding and nuanced task begins thereafter—namely, the evaluation of authenticity, the testing of reliability, and the determination of probative value. In the digital context, these stages assume heightened importance because the inherent characteristics of electronic data render it both powerful and precarious as a source of proof.

Unlike traditional documents, electronic records are not static artefacts; they are dynamic outputs generated through complex technological processes. A digital record is the culmination of interactions between hardware, software, and human input. Consequently, the reliability of such evidence cannot be assessed solely by examining its visible form. It must be evaluated in light of the processes that produced it, the systems that stored it, and the manner in which it was retrieved.

This necessitates a shift in judicial methodology. The judge must move beyond passive reception of evidence and adopt an active, analytical role in interrogating the technological underpinnings of electronic records. The process of evaluation can be conceptualised as comprising three interrelated stages: **authentication, integrity verification, and evidentiary appreciation**.

Civil & Commercial Disputes: Digital Transactions & Contracts

In civil litigation, electronic evidence often arises in the context of contracts, financial transactions, and corporate records. Emails, digital agreements, and transaction logs are frequently relied upon to establish rights and obligations.

In such cases, the Court must focus on:

- The authenticity of the communication
- The authority of the parties involved
- The consistency of the record with other evidence

The increasing use of automated systems and digital platforms introduces additional complexities. Courts must consider whether the system itself is reliable and whether the records generated reflect actual transactions.

Authentication and Integrity: Beyond Formal Compliance- Authentication of Source and Attribution

The first and most fundamental inquiry in relation to any electronic record is the question of authorship and origin. Authentication requires the Court to be satisfied that the record emanates from the source it purports to represent. In the digital realm, this is often far from straightforward.

Electronic communications, for instance, may be transmitted through devices that are shared, compromised, or impersonated. Email accounts may be accessed by multiple users; messaging platforms may be subject to spoofing; digital identities may be fabricated. In such circumstances, the mere production of a record—whether in the form of a printout or electronic file—does not establish its authenticity.

Courts must therefore look for corroborative indicators that link the record to a specific individual or system. These may include:

- Metadata associated with the record
- IP address logs
- Device identification details
- Consistency with other evidence

Judicial precedents have underscored the importance of such corroboration. In *Anvar P.V. v. P.K. Basheer*, the Supreme Court emphasised that electronic evidence must satisfy statutory conditions precisely because of the ease with which it can be manipulated. The Court recognised that authenticity cannot be presumed; it must be demonstrated.

Judicial Appreciation of Electronic Evidence: From Admissibility to Probative Value

The final stage in the judicial handling of electronic evidence is the assessment of its probative value. Admissibility under Section 63 does not automatically translate into evidentiary weight. The Court must evaluate the significance of the evidence in the context of the entire case.

This involves considering:

- The consistency of the electronic record with other evidence
- The credibility of the source
- The presence of corroboration
- The possibility of alternative interpretations

For example, a video recording may establish the presence of an individual at a particular location but may not, by itself, establish intent or culpability. Similarly, an electronic communication may suggest involvement but may require corroboration to establish authorship or context.

The Court must therefore integrate electronic evidence into the broader evidentiary matrix rather than treating it as determinative in isolation.

Best Practices and Common Errors in Trial Court Adjudication

The increasing prevalence of electronic evidence has revealed certain recurring patterns of error in trial court adjudication. Identifying and addressing these errors is essential for ensuring consistency, reliability, and fairness in the judicial process.

Common Error	Corrective Judicial Approach
Mechanical admission on production of certificate without examining its adequacy or the reliability of the underlying system.	Engage actively with the contents of the certificate; verify all four conditions under Section 63(2) are specifically addressed.
Rejection of evidence on hyper-technical grounds where minor defects in certification are treated as fatal.	Adopt a calibrated approach — permit rectification of curable defects; reserve exclusion for absence of certification altogether.
Failure to examine chain of custody, increasing risk of relying on tampered evidence.	Trace the complete movement of electronic record from origin to court; scrutinise gaps in custody.
Insufficient engagement with expert evidence — either deference without analysis or disregard without reasoning.	Evaluate the methodology and reasoning of expert opinion; integrate it into the broader evidentiary matrix rather than adopting it wholesale.

1. Regarding certficate In practice, courts frequently encounter certificates that are incomplete, vague, or technically deficient. The judicial response to such defects must be guided by a balance between procedural compliance and substantive justice.

Where the defect is curable for instance, where the certificate lacks certain details but the underlying record appears reliable the Court may permit the party to rectify the deficiency. However, where the defect goes to the root of admissibility such as the absence of certification altogether the Court must exercise caution.

The Hon'ble Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* clarified that the requirement of certification is mandatory and cannot be dispensed with merely on grounds of convenience.[2] At the same time, the Court recognised that parties may seek appropriate directions to obtain the certificate where it is not readily available. Thus, the judicial approach must be neither rigid nor permissive but calibrated to the circumstances of each case.

2. One common error is the **mechanical admission of electronic evidence** upon production of a certificate. Courts often fail to examine whether the certificate actually satisfies the statutory requirements or whether the underlying system is reliable. This reduces the certification process to a mere formality.

3. Another frequent issue is the **rejection of evidence on hypertechnical grounds**, particularly where minor defects in certification are treated as fatal. Such an approach may result in the exclusion of otherwise reliable evidence and undermine the objective of justice.

4. A third area of concern is the **failure to examine the chain of custody**. Courts sometimes admit electronic records without considering how they were handled, transferred, or stored. This oversight increases the risk of relying on tampered or manipulated evidence.

5. Additionally, there is often insufficient engagement with **expert evidence**. Courts may either defer entirely to expert opinion without independent evaluation or disregard it without adequate reasoning.

The corrective approach requires judges to:

- Engage actively with the contents of the certificate
- Evaluate the reliability of the system and process
- Consider the possibility of tampering

Integrate expert testimony into the broader evidentiary framework.

Judicial Checklist for Electronic Evidence

The following checklist is recommended for courts when confronted with electronic evidence:

Judicial Checklist: Electronic Evidence under Section 63 BSA

☐ **STAGE 1 — IDENTIFICATION:**
Is this material an electronic record within the meaning of Section 2(1)(d) BSA? Does it derive its evidentiary value from a digital system?

☐ **STAGE 2 — CERTIFICATE:**
Has a certificate under Section 63(4) been produced? Does it specifically address each of the four conditions under Section 63(2)?

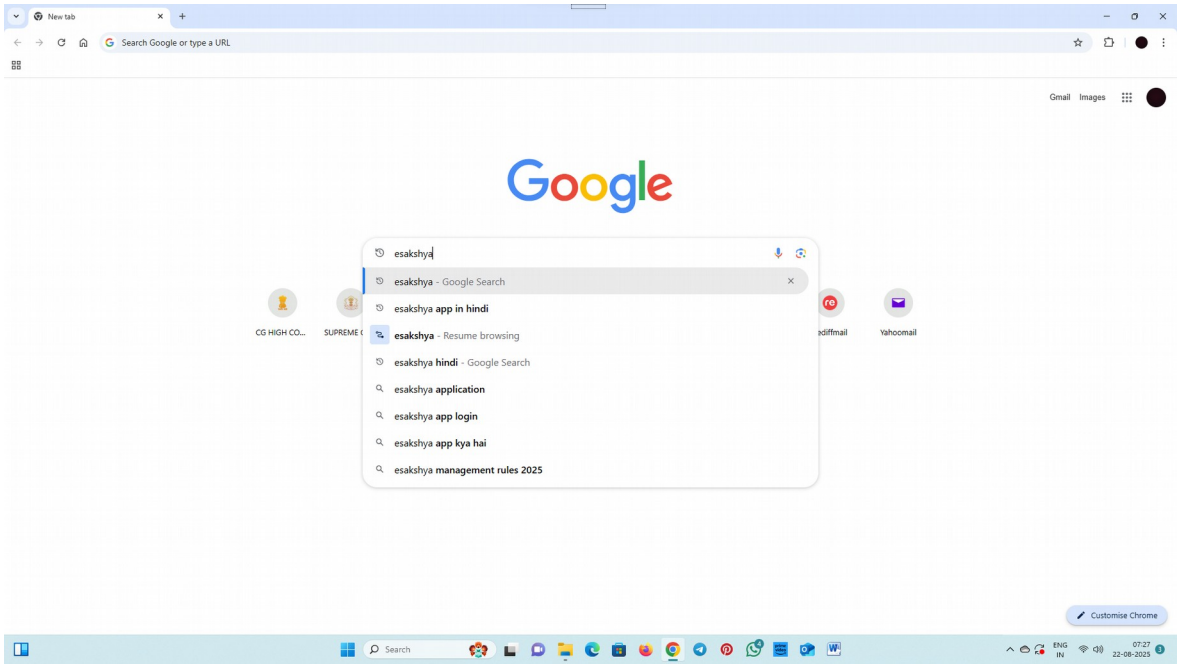
☐ **STAGE 3 — SYSTEM INTEGRITY:**
Was the device in regular use? Was data recorded in ordinary course of activity? Was the device functioning properly? Is the output an accurate reproduction?

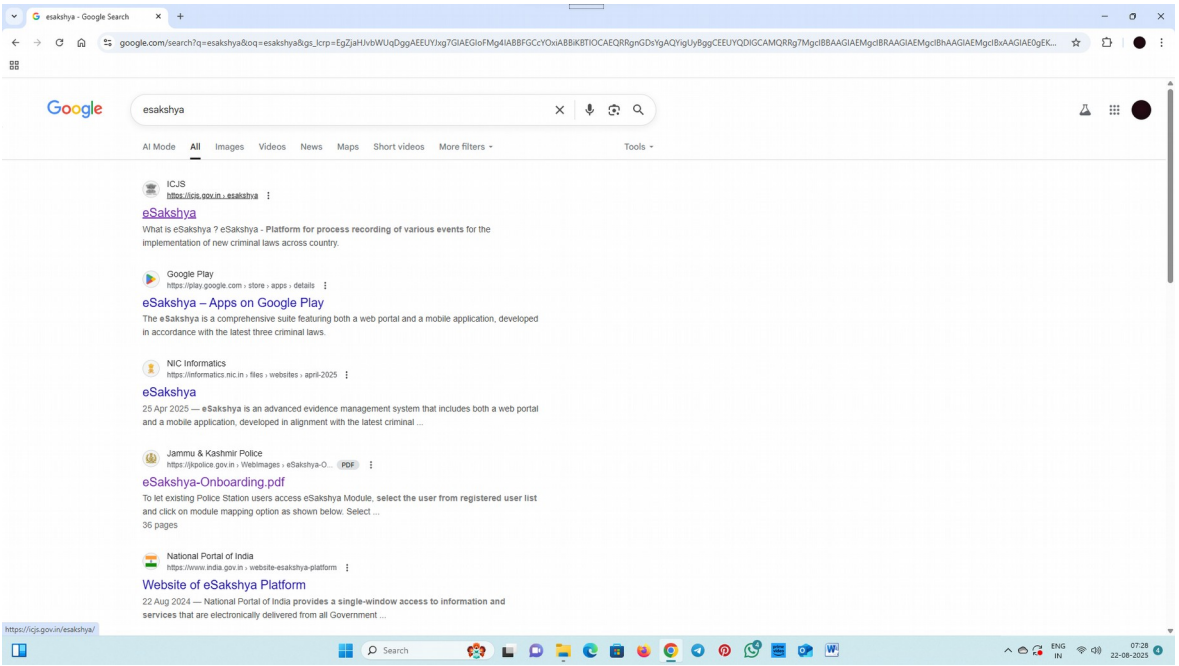
☐ **STAGE 4 — CHAIN OF CUSTODY:**
Is the chain of custody documented and unbroken from collection to court? Are gaps explained?

☐ **STAGE 5 — AUTHENTICATION:**
Is there evidence of tampering? Is the hash value recorded and verified? Is the source of the record established?

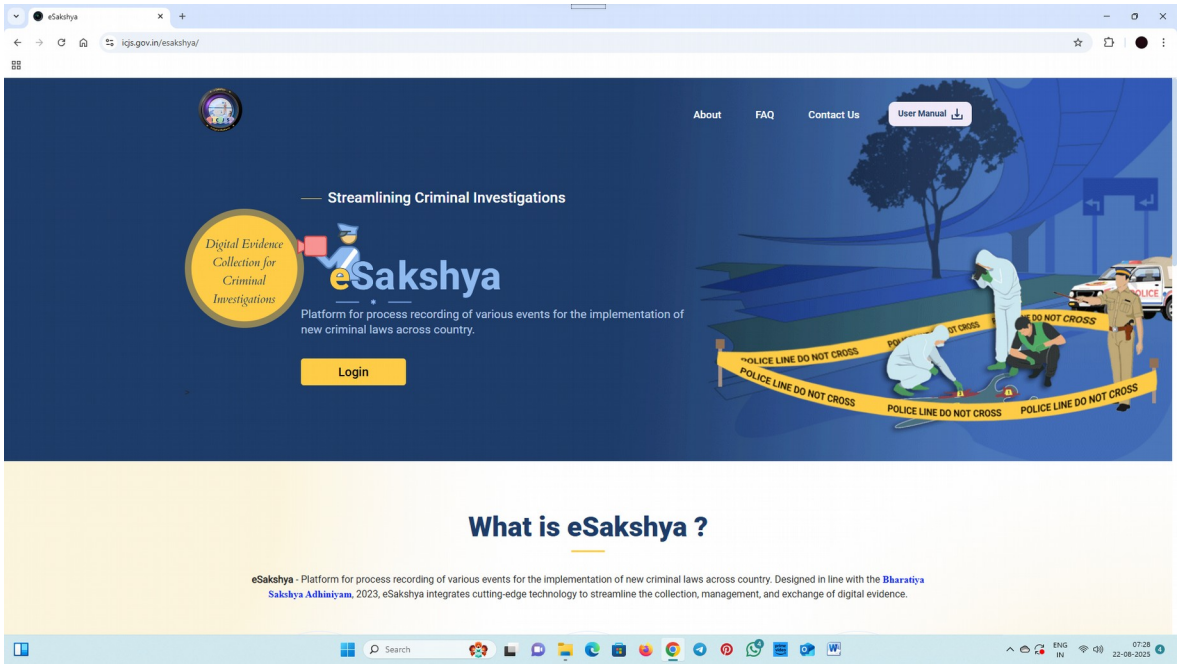
☐ **STAGE 6 — PROBATIVE VALUE:**
Is the electronic record corroborated by other evidence? Does it withstand cross-examination? What weight should be accorded in the overall evidentiary matrix?

Login steps on eSakshya web portal

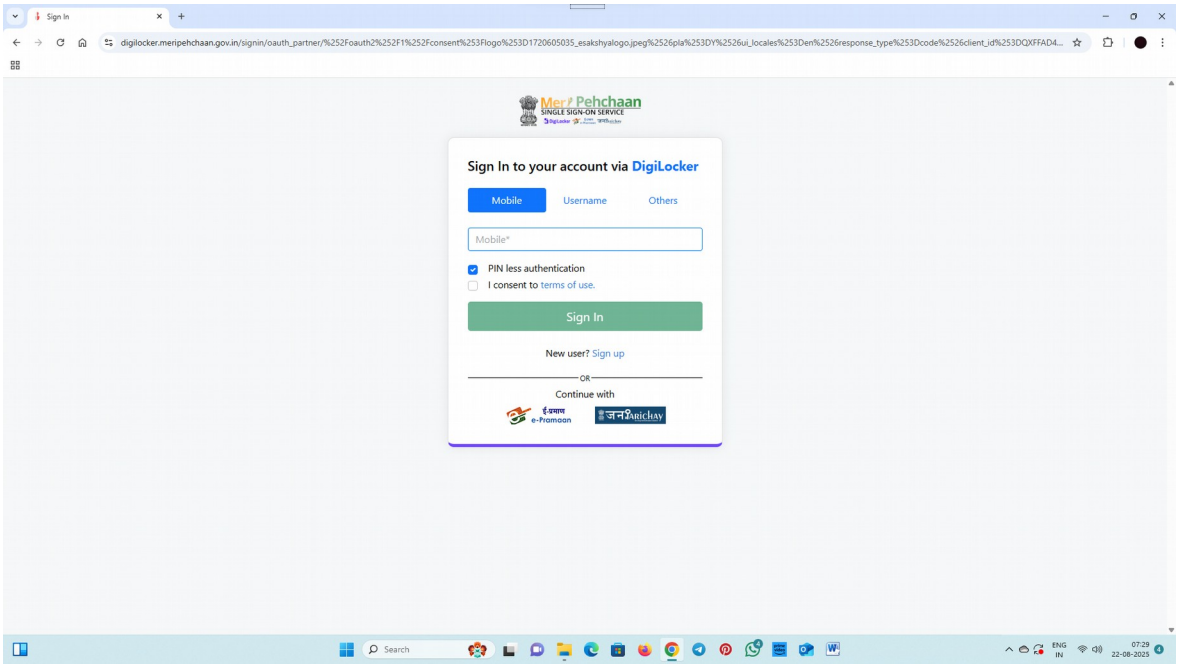




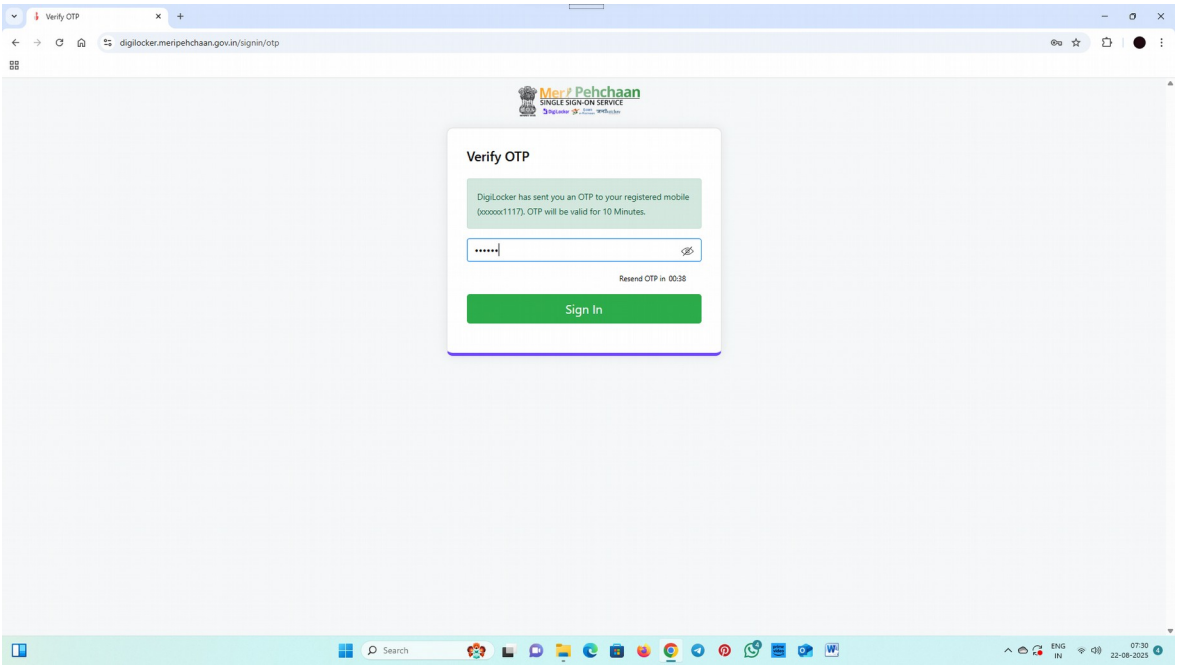
Open URL (https://icjs.gov.in/esakshya/) to access eSakshya web portal and click on Login button.



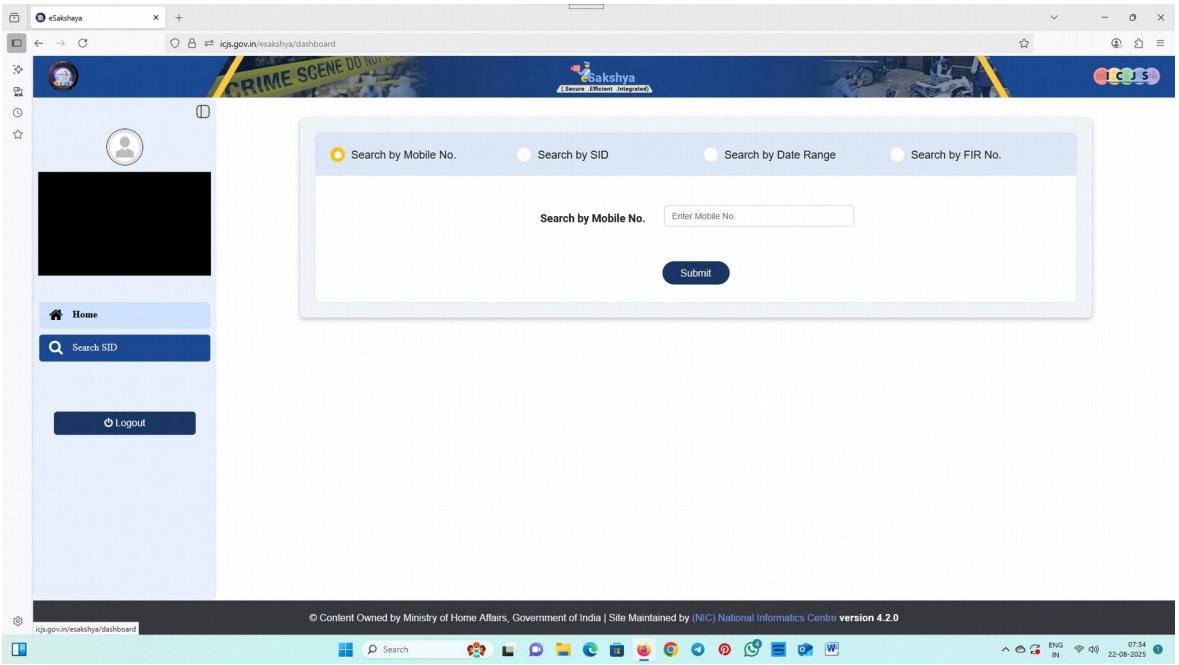
Login MeriPehchaan NSSO using registered mobile number, select “PIN less authentication” and “I consent to terms of use” checkboxes and click on Sign In button.



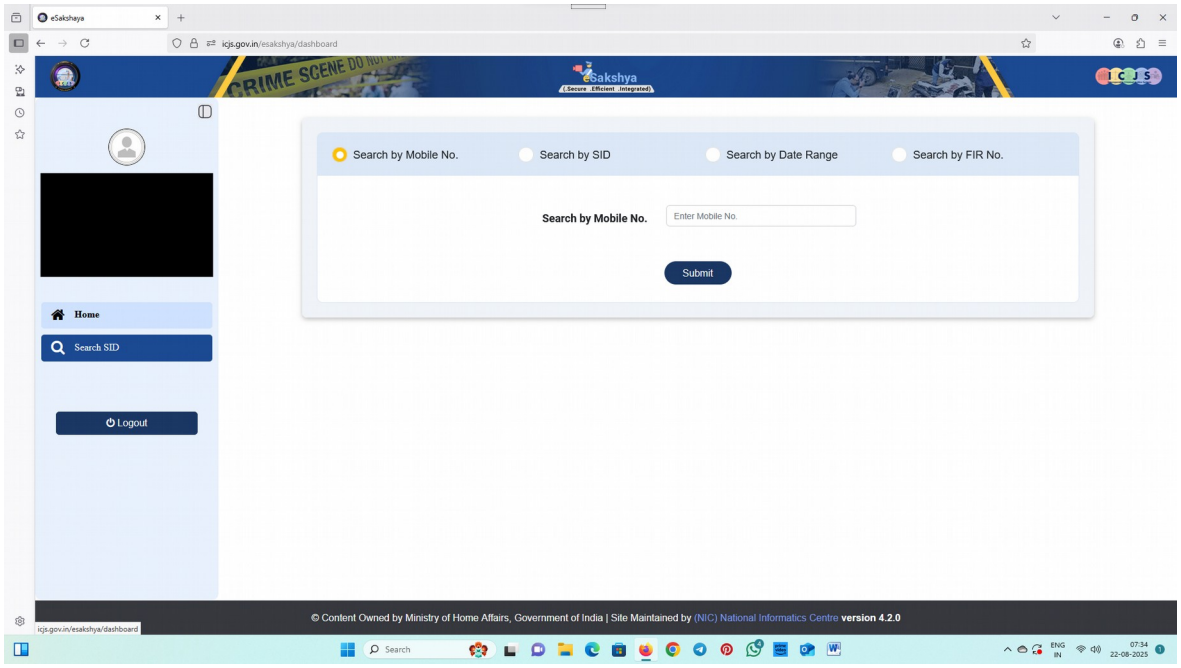
Enter 6 digit OTP as received on registered mobile number and click on Sign In button.

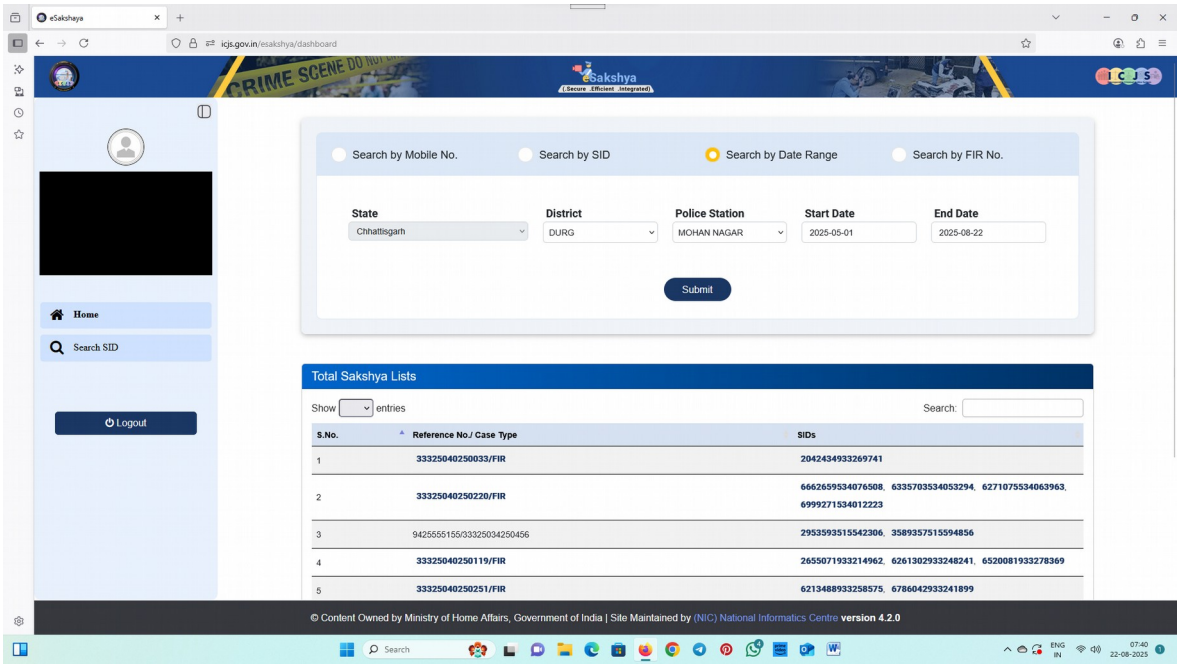


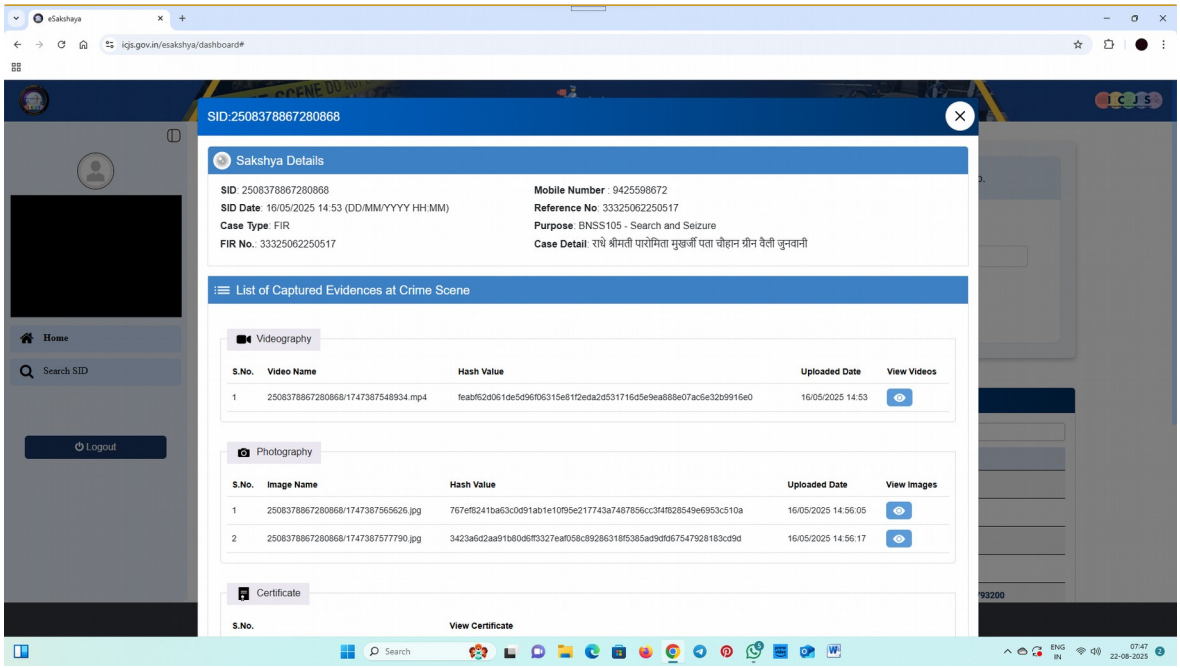
You will be redirected to eSakshya Home page after successful login.



After login on eSakshya web portal, click on ‘Search by SID’ option to view recorded Sakshya.






eSakshya
icjs.gov.in/esakshya/dashboard#
SID:2508378867280868
Sakshya Details
SID: 2508378867280868
SID Date: 16/05/2025 14:53 (DD/MM/YYYY HH:MM)
Case Type: FIR
FIR No.: 33325062250517
Mobile Number : 9425598672
Reference No: 33325062250517
Purpose: BNSS105 - Search and Seizure
Case Detail: राधे श्रीमती पारोमिता मुखर्जी पता चौहान ग्रीन वैली जुनवानी
List of Captured Evidences at Crime Scene
Videography
S.No. Video Name Hash Value Uploaded Date View Videos
1 2508378867280868/1747387548934.mp4 feabf62d061de5d96f06315e81f2eda2d531716d5e9ea888e07ac6e32b9916e0 16/05/2025 14:53
Photography
S.No. Image Name Hash Value Uploaded Date View Images
1 2508378867280868/1747387565626.jpg 767ef8241ba63c0d91ab1e10f95e217743a7487656cc3f4f828549e6953c510a 16/05/2025 14:56:05
2 2508378867280868/1747387577790.jpg 3423a6d2aa91b80d6ff3327eaf058c89286318f5385ad9dfd6754792818 3cd9d 16/05/2025 14:56:17
Certificate
S.No. View Certificate
Home
Search SID
Logout

State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru — (2005) 11 SCC 600 (Parliament Attack Case)	
Facts :	On 13 th December , 2001 , five heavily armed persons practically stormed the Parliament House complex and inflicted heavy casualties on the security men on duty. In the gun battle that lasted for 30 minutes , these five terrorist who tried to gain entry into the Parliament when it was in session were killed..
Relevancy of electronic evidence :	The links between the slain terrorists and the masterminds of the attack were established only through phone call transcripts obtained from the mobile service providers. One of the major issue raised from the side of the accused was the inadmissibility of the electronic records (mobile phone call records) because there was no certificate produced by the prosecution which is necessary for admitting any electronic record .
Held :	The Apex Court concluded that the cross- examination of competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records. Irrespective of the compliance of the requirements of Section 65B which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely Sections 63 & 65

Anvar P.V. v. P.K. Basheer & Others — (2014) 10 SCC 473	
Facts :	In the present case , appellant had filed election petition to set aside the election of first respondent on ground that alleged songs, announcements , and speeches made as part of election propaganda of first respondent , amounted to corrupt practices.
Relevancy of Electronic Evidence :	alleged songs, announcements , and speeches were recorded using some instrument and by feeding them into computer, CDs were made which were produced in the court. However, certificate in terms of section 65-B was not produced in respect of such CDs.
Held :	A three-Judge Bench of the Hon'ble Supreme held that CDs concerned, not being the original CDs themselves, cannot be admitted in evidence since the mandatory requirements of section 65-B of Evidence Act are not satisfied. Hon'ble Court further held that the Computer Output is not admissible without compliance of Section 65B. It overruled the judgment in State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru [(2005) 11 SCC 600] by the two judge Bench of the Supreme Court. The court observed that "the Judgment of Navjot Sandhu, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled. Hon'ble Apex Court in Anvar P.V vs. P.K.Basheer held that under Section 65B(4) of the Evidence Act, if it is desired to give a statement in any proceedings pertaining to an electronic record, it is permissible provided the following conditions are satisfied:

	(a) There must be a certificate which identifies the electronic record containing the statement; (b) The certificate must describe the manner in which the electronic record was produced; (c) The certificate must furnish the particulars of the device involved in the production of that record; (d) The certificate must deal with the applicable conditions mentioned under Section 65B(2) of the Evidence Act; and (e) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device. The objective behind aforesaid step-by-step processes is to identify whether the computer in question was properly processed, stored and reproduced whatever information it received.

Tomaso Bruno & Another Vs. State of UP — (2015) 7 SCC 178	
Facts :	Appellants were foreigners , who were tourist in India , charged with having murdered their companion in a hotel. The prosecution case was based on circumstantial evidence that it were appellants alone who could do this because all the three were lodged in10 a single room . Per contra, the version of the appellants was that they were out of hotel for a couple of hours while the deceased stayed back because he was not well and when the appellants returned , they found deceased in serious condition.
Relevancy of electronic evidence :	Appellants location at material time was crucial to unravel the truth and this could be determined with the help of CCTV recordings in the hotel and movement of mobile phones

Held :	The Hon'ble Court set aside the conviction of the appellants under section 302/34 of IPC on the ground that CCTV footage and call records was not produced by the prosecution. Further, without referring to the judgment passed in Anwar PV case, the Hon'ble Court held that secondary evidence of the contents of a document can be led under section 65 of the Evidence Act

Shafhi Mohammad v. State of Himachal Pradesh — (2018) 2 SCC 801	
Facts :	Use of the videography of the scene of crime is the subject matter of consideration herein.
Held :	A two Judge Bench of the Hon'ble Supreme Court held that requirement of certificate under Section 65B (4) is not always mandatory. As there was dichotomy of decisions in between Anwar PV's case and Shafhi Mohammad's case, in the year 2019, a two-Judge Bench of the apex court referred the matter to a another three-judge bench for clarification on the point

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal — (2020) 7 SCC 1	
Facts :	The Hon'ble Court had to adjudicate on an election petition which challenged the election of Mr. Arjun Panditrao Khotkar from Jalna-101 Legislative Assembly Constituency, on the ground that the nomination papers were filed after the stipulated deadline. The Respondents wished to rely on video camera recordings of the office of Returning Officer to prove that the candidate had filed his nomination after the stipulated deadline. The Election Commission produced CDs which

	contained a copy of the video camera recordings, in accordance with the direction given by the Hon'ble High Court. However, the necessary certificates were not produced in accordance with Section 65B(4) by the Election Commission, despite multiple requests made by the Petitioner
Relevancy of electronic evidence :	The question arises whether the Video Compact Disk containing video recordings could be admitted in the absence of certificate
Held :	The Hon'ble Supreme Court upheld the impugned judgment of the High Court wherein during the cross examination , an officer of the Election Commission testified that the video camera recordings were authentic. Based on this testimony, the High Court admitted the evidence of the video recordings even though the certificate in accordance with Section 65B (4) had not been produced. The High Court held that it was satisfied that there was "substantial compliance" with Section 65B, as a competent officer had testified that the video recordings were authentic. Moreover , apart from electronic record , other evidence was also relied upon by High Court. <u>Arjun Panditrao Khotkar Case also considered three key issues with regards to Section 65B of the IEA.</u> A - Whether or not section 65B constitutes the complete code in India as to the admissibility of secondary digital evidence ? Answer :- Special provisions of ss.65A and 65B are a complete Code in themselves when it comes to admissibility of evidence of information contained in electronic records. B - Whether the requirement of a certificate was mandatory in all cases ?

Answer :- A written certificate u/s.65B(4) is a sine qua non for admissibility of such evidence – Oral evidence in place of such certificate cannot suffice as s.65B(4) is mandatory. Further, the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4).

C - Finally at which stage of the proceedings in a criminal or civil trial would the certificate need be produced ?

Answer :- It has been held in Arjun Panditrao Case that "So long as the hearing in a trial is not yet over, the requisite certificate can be directed to be produced by the learned Judge at any stage, so that information contained in electronic record form can then be admitted and relied upon in evidence ."

The Overruling - Hon'ble Supreme Court in Arjun Panditrao Khotkar Vs. Kailash Kushanrao Gorantyal & Others (2020) SCC OnLine SC 571 held that Anvar P.V. (supra), is the law declared by this Court on Section 65B of the Evidence Act. The judgment in Tomaso Bruno (supra), being per incuriam, does

	not lay down the law correctly. Also, the judgment in SLP (Crl.) No. 9431 of 2011 reported as Shafhi Mohammad (supra) (2018) 5 SCC 311, do not lay down the law correctly and are therefore overruled.

State of Karnataka v. T. Naseer @ Nasir — 2023 LiveLaw (SC) 965 | 06.11.2023	
Issue / Facts :	CFSL report rejected for absence of Section 65B certificate; prosecution later obtained certificate and filed application under Section 311 CrPC.
Held :	Certificate under Section 65B can be produced at any stage of trial. Application under Section 311 CrPC allowed. Consistent with Arjun Panditrao.

Sonu @ Amar v. State of Haryana — (2017) 8 SCC 570	
Issue / Facts :	Objection to CDR admissibility (no 65B certificate) raised for first time at appellate stage.
Held :	Objection as to mode/method of proof must be raised at trial stage at the time of marking the exhibit — not at appellate stage. Objection as to per se inadmissibility may be raised at any stage.

Foundational Decisions on Admissibility

Sonu @ Amar Vs. State of Haryana

[PROCEDURAL — GOOD LAW] (2017) 8 SCC 570

Objections to admissibility of electronic evidence must be raised at the trial stage. Failure to do so precludes raising such objections at a later stage, including before the High Court. This decision introduces procedural discipline, prevents strategic litigation, and encourages early examination of evidentiary issues. Trial courts must note and record all objections to electronic evidence at the time of its tendering.

Mukesh Vs. State (NCT of Delhi)

[Nirbhaya Case] [CORROBORATION PRINCIPLE]

(2017) 6 SCC 1

Electronic evidence — call detail records and location data — was accepted as crucial corroborative evidence. The Court held that such evidence must be examined in conjunction with other evidence, not in isolation. Electronic evidence has moved from a supplementary to a central role in criminal trials. Judges must treat it as highly probative but not self-sufficient; corroboration must be sought wherever possible.

State of Karnataka Vs. M.R. Hiremath [STRICT COMPLIANCE]

(2019) 7 SCC 515

Failure to produce a certificate under Section 65B (IEA) renders

electronic evidence inadmissible regardless of its apparent reliability. The provisions governing electronic evidence override general rules of evidence. Reinforces the 'complete code' doctrine from Anvar. Trial courts must insist on strict compliance with certification requirements and may not admit electronic evidence on equitable or discretionary grounds.

Ram Singh v. Col. Ram Singh

[FOUNDATIONAL — RECORDINGS]

1985 Supp SCC 611

Laid down the foundational tests for admissibility of tape-recorded evidence: accuracy of recording, absence of tampering, and proper custody. Although predating digital technology, these authenticity tests continue to inform the law of electronic evidence and provide the conceptual bedrock for the conditions prescribed in Section 63(2) of the BSA.

Deepak Kumar v. State [WhatsApp Evidence] [SOCIAL MEDIA — AUTHENTICATION]

High Court | Social Media Evidence

Mere production of screenshots or printouts of WhatsApp messages is insufficient for admissibility. Proper authentication including certification and corroborative evidence is necessary. Messages can be deleted, edited, or fabricated; accounts can be impersonated. Courts must treat social media evidence with heightened caution, require strong corroboration, and verify authorship and account ownership through additional means.

Kailas Vs. The State of Maharashra

2025 LiveLaw (SC) 914

The Hon'ble Supreme Court held that a video recording of the seizure of contraband is admissible in evidence without requiring its transcript. The Court clarified that once a valid electronic certificate under Section 65B of the Evidence Act is produced, the video's authenticity stands proved, and it is unnecessary to play the recording before each witness shown in it during their testimony to make the video recording admissible..

Chandrabhan Sudam Sanap Vs. The State of Maharashtra

2025 LiveLaw (SC) 119

Admissibility of CCTV footage

The Court first made observations in regard to the admissibility of the CCTV footage. It found various infirmities in the evidence led by the prosecution. Most importantly, the prosecution did not furnish the Section 65-B(4) certificate under the Indian Evidence Act while collecting the electronic evidence. In this context, the Court perused various judgments and considered the settled position of law which was Section 65-B(4) certificate as a condition precedent to the admissibility of evidence by way of electronic evidence as held in Anvar P.V. v. P.K. Basheer (2014).

In this regard, the Hon'ble Court said: "Thus, when the prosecution was aware of the need for the 65-B (4) certificate and they themselves collected it for the CDRs there was no reason as to why they did not collect the same for the CCTV footage...In view of the above, there is no manner of doubt that certificate under Section 65-B(4) is a condition

precedent to the admissibility of evidence by way of electronic record and further it is clear that the Court has also held Anvar P.V. (supra) to be the correct position of law."

Further, the Hon'ble Supreme Court stated that when a matter pertains to the death penalty, the case must be considered in light of the Anvar P.V. judgment. In light of this, in Mohd. Arif v. State (NCT) of Delhi , the Court eschewed the electronic evidence for want of a certificate. Relying on this, the Court in this regard held that it cannot rely on CCTV footage:

"In view of the above, we are not able to place any reliance on the CCTV footage, insofar as an attempt is made by the prosecution to attribute that the appellant and the deceased EA were last seen together based on the CCTV footage. We eschew the same from consideration."

Pooranmal Vs. The State of Rajasthan & Another

2026 LiveLaw (SC) 227

The Hon'ble Supreme Court acquitted a man convicted in a murder case, holding that Call Detail Records (CDRs) cannot be relied upon in evidence unless accompanied by the mandatory certificate under Section 65B of the Indian Evidence Act.

Concluding Observations : Towards a Coherent Judicial Approach

The law of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 represents a significant and carefully calibrated step towards modernising India's evidentiary framework. Section 63 is not merely a technical provision; it embodies a broader philosophy that seeks to ensure that evidence is both accessible and reliable. The judicial task is to give effect to this philosophy through careful, reasoned, and consistent application.

The judge must act as a gatekeeper — ensuring that only those electronic records that meet the required standards are admitted — while remaining mindful that the ultimate objective of evidence law is the discovery of truth. This requires a balanced approach that combines legal rigour with practical wisdom and technological awareness.

Three Pillars of a Coherent Judicial Approach

LEGAL RIGOUR: Strict compliance with Section 63 and certification requirements; no equitable relaxation; every condition of Section 63(2) must be independently satisfied and recorded.

PRACTICAL WISDOM: A calibrated response to defects — distinguishing between curable and fatal gaps; facilitating procurement of certification where parties face genuine difficulty; avoiding hyper-technical exclusions.

TECHNOLOGICAL AWARENESS: Active judicial engagement with digital forensics, hash values, metadata, chain of custody, and expert testimony; willingness to seek clarification and exercise informed judgment on

technical matters.

The BSA has laid the statutory foundation. The eSakshya portal has provided the institutional infrastructure. The jurisprudence of Anvar P.V. and Arjun Panditrao Khotkar has supplied the doctrinal framework. It now falls to the trial courts — as the first and most consequential gatekeepers of evidence — to ensure that electronic evidence serves as a reliable instrument of truth, rather than a source of uncertainty or manipulation in the judicial process.

Thank You.