

DIVISIONAL JUDICIAL SEMINAR RAIPUR DIVISION: 26 JULY
2026 (DISTRICTS- RAIPUR, MAHASAMUND, DHAMTARI,
BALODABAZAR-BHATAPARA)

Paper Presentation

On

***“ ZERO FIR AND E-FIR LEGALITIES AND ADMISSIBILITY OF
ELECTRONIC RECORDS AND PRACTICAL CHALLENGES IN
RECORDING ”***



सत्यमेव जयते

SUBMITTED BY

DISTRICT – BALODABAZAR- BHATAPARA (C.G.)

ACKNOWLEDGEMENT

We feel highly elated to work on the topic “Zero Fir And E-Fir Legalities and Admissibility of Electronic Records and Practical Challenges in Recording.”

We would like to thank the Hon’ble High Court of Chhattisgarh and Chhattisgarh State Judicial Academy for organizing this Divisional Seminar and providing us a platform to discuss on such crucial legal points. We like to express our deepest regard and gratitude for Principal District and Sessions Judge, Balodabazar-Bhatapara (C.G.). Her consistent supervision, constant inspiration and invaluable guidance have been of immense help in understanding and carrying out the nuances of the preparation of paper. Some printing errors might have crept in, which are deeply regretted. We would be grateful to receive comments and suggestions to further improve this presentation.

Finally, we express our gratitude towards each and every one, who helped in providing contents, materials and various data and information, which greatly aided to prepare this presentation.

JUDICIAL OFFICERS

DISTRICT - BALODABAZAR-BHATAPARA(C.G.)

TABLE OF CONTENTS

1. INTRODUCTION -----	4
2. ZERO FIR -----	5-6
2.1. HISTORICAL BACKGROUND – ZERO FIR -----	5-6
2.2. LEGAL PROVISIONS -----	6
3. MEANING AND CONCEPT OF E-FIR -----	6-9
3.1. LEGAL PROVISIONS FOR E-FIR -----	7
3.2. PROCEDURE FOR FILING AN E-FIR -----	7-9
3.3. CURRENT SCENARIO RELATED TO E-FIR -----	9
4. ADMISSIBILITY OF ELECTRONIC RECORDS -----	9-18
4.1. MEANING AND DEFINITION -----	9
4.2. HISTORY AND EVOLUTION -----	10-11
4.3. JUDICIAL PRONOUNCEMENTS -----	11-12
4.4. PRIMARY AND SECONDARY EVIDENCE -----	12-14
4.5. REQUIREMENT OF CERTIFICATE -----	14-16
4.6. STAGE OF FILING THE CERTIFICATE -----	17
4.7. TYPES OF ELECTRONIC EVIDENCE -----	17-18
4.8. ROLE OF EXPERT EVIDENCE -----	18
5. E-SAKSHYA -----	19-21
6. CHALLENGES TO CREDIBILITY AND ADMISSIBILITY OF ELECTRONIC EVIDENCE -----	19-21
7. CONCLUSION -----	21

1. INTRODUCTION

The First Information Report (FIR) is the foundation of the criminal justice process, as it sets the law in motion and enables the police to investigate cognizable offences. With the rapid advancement of technology and the growing emphasis on ensuring easy access to justice, the criminal justice system has evolved to adopt more victim-centric and technology-driven mechanisms.

Zero FIR addresses the issue of territorial jurisdiction whereas an E-FIR addresses the issue of physical accessibility by enabling the complainant to lodge information remotely. Thus, while both mechanisms seek to ensure timely registration of offences, they operate in different domains and complement each other in promoting a victim-centric criminal justice system.

The enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 (hereinafter referred to as 'BNSS') has further strengthened these reforms by expressly recognizing the principles governing Zero FIR and permitting the furnishing of information relating to cognizable offences through electronic communication.

Electronic evidence plays a crucial role in modern legal proceedings. The admissibility and evidentiary value of electronic evidence depend upon various factors, including its relevancy, authenticity, the manner in which it was obtained and preserved. Given the growing reliance on digital technologies in both personal and commercial spheres, understanding the nuances of electronic evidence has become essential for legal practitioners and judicial officers alike, for better administration of justice.

A computer can be a tool for the commission of an offence and it can be a repository of electronic evidence. Realising the importance of computer knowledge to Judges, the Hon'ble Supreme Court in the case of ***Vijendra Kumar Verma v. Public Service Commission, Uttarakhand & Others***¹ has observed as follows –

“The Indian judiciary is taking steps to apply e-governance for efficient management of courts. In the near future, all the courts in the country will be computerized. In that respect, the new judges who are being appointed are expected to have basic knowledge of the computer operation. It will be unfair to overlook basic knowledge of computer operation to be an essential condition for being a judge in view of the recent development being adopted.”

¹ *Vijendra Kumar Verma v. Public Service Commission, Uttarakhand & Others*, 2011 (1) S.C.C. 150.

2. ZERO FIR

A Zero FIR is an FIR registered by any police station irrespective of territorial jurisdiction. It is assigned the serial number “0” (Zero) and is subsequently transferred to the police station having territorial jurisdiction for investigation. The police Officer or officer in charge of police station is bound to register an FIR of every offence, whether such offences have been occurred in their jurisdiction or not. Zero FIR ensures prompt registration and investigation of case, thus helping prevent delays in the criminal justice process.

2.1. HISTORICAL BACKGROUND – ZERO FIR

The FIR is the important component in the legal system and for the initiation of investigation by the police officer and officer in charge of police station. Under the legal system the FIR is filed under the jurisdiction where the offence is committed, but there are some logistic reasons due to which victim cannot file FIR under the jurisdiction where the crime is occurred. Here the concept of Zero FIR comes into the play. The provision of Zero FIR was introduced to ensure that victim of crime did not face procedural hurdles that delay justice. The primary objective of Zero FIR is that police officer can take immediate cognizance on the complaint without worrying of the jurisdictional boundaries of a police station. The objective of the provisions is to give the victim prompt redress so that prompt action can be taken after filing FIR.

In *Satvinder Singh v. State (Govt of N.C.T Delhi)*,² the question arose before The Hon’ble Supreme Court that it is valid to quash an FIR that the police officer has no territorial jurisdiction over the matter even if it is cognizable case. The Hon’ble Supreme Court held that it does not matter whether police officer have territorial jurisdiction over an area, police have to do needful and it is not a valid ground for quashing an FIR. The police can investigate under Zero FIR, and such investigation is protected and cannot be challenged only on the basis that there was no territorial jurisdiction.

In *Ramesh Kumari v. State (NCT of Delhi)*,³ the Hon’ble Supreme Court held that the provision of Section 154 is mandatory. Hence, the police officer concerned is duty-bound to register the case on receiving information disclosing cognizable offence. Genuineness or credibility of the information is not a condition precedent for registration of a case. That can only be considered after registration of the case.

² *Satvinder Singh v. State (Govt of N.C.T Delhi)*, A.I.R. 1999 S.C. 3596.

³ *Ramesh Kumari v. State (NCT of Delhi)*, A.I.R. 2006 S.C. 1322.

In the case of *Lalita kumari v. State of Uttar Pradesh*,⁴ The Hon'ble Supreme court ruled that police officer must register FIR whenever the cognizable offence is reported, even when the offence did not occur in their jurisdiction. In some case when the offence does not disclose a cognizable offence a preliminary inquiry can be conducted before filing a FIR such as matrimonial dispute, commercial offence, medical negligence case and corruption case. If preliminary inquiry is done, it should be completed within 7 days and the reasons must be recorded in writing.

2.2. LEGAL PROVISION FOR ZERO FIR

For the first time, the principle underlying Zero FIR received express statutory recognition through Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), which came into force on 1 July 2024.

Section 173(1) provides that information relating to the commission of a cognizable offence may be given irrespective of the area where the offence is committed, thereby legislatively recognising the principle that territorial jurisdiction cannot be a ground for refusing registration of an FIR.

3. MEANING AND CONCEPT OF E-FIR

The advancement of information and communication technology has significantly transformed the functioning of the criminal justice system. In furtherance of the objectives of Digital India and Ease of Access to Justice, the concept of Electronic First Information Report (E-FIR) has emerged as a modern mechanism enabling citizens to report cognizable offences through electronic means without the necessity of physically visiting a police station.

An E-FIR refers to the electronic registration of information relating to the commission of a cognizable offence through digital platforms such as official police portals, mobile applications, e-mail, or other electronic modes prescribed by law. It aims to facilitate prompt reporting of crimes, reduce procedural delays, improve accessibility, and enhance transparency in police functioning. The concept of E-FIR is particularly beneficial for victims of cybercrime, women, senior citizens, persons with disabilities, and individuals residing in remote areas, who may face practical difficulties in approaching a police station immediately after the commission of an offence.

⁴ Lalita kumari v. State of Uttar Pradesh, A.I.R. 2014 S.C. 187.

3.1. LEGAL PROVISION FOR E-FIR

Although several States had introduced online complaint portals before the enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), there was no uniform statutory recognition of electronic registration of FIRs under the Code of Criminal Procedure, 1973. The BNSS has now formally recognized the use of electronic communication for furnishing information relating to cognizable offences, thereby giving statutory legitimacy to the concept of E-FIR.

Section 173(1) BNSS expressly provides that information relating to the commission of a cognizable offence may be given through electronic communication. The provision further stipulates that where such information is furnished electronically, it shall be signed by the informant within three days, thereby ensuring both convenience and authenticity. This is the first comprehensive statutory recognition of electronic reporting of cognizable offences in Indian criminal procedure.

3.2. PROCEDURE FOR FILING AN E-FIR IN CHHATTISGARH

The State of Chhattisgarh has implemented online police services through the Chhattisgarh Police Citizen Service Portal, which is integrated with the Crime and Criminal Tracking Network & Systems (CCTNS). The portal enables citizens to submit complaints, access various police services, and track the status of cases electronically. The general procedure is as follows:

- a.) Citizen Registration – The complainant is required to create a user account on the Chhattisgarh Police Citizen Service Portal by providing basic details such as name, mobile number, e-mail address, and identity credentials. After verification through OTP, login credentials are generated.
- b.) Login and Selection of Service – After logging into the portal, the complainant selects the appropriate service. The portal provides facilities such as:
 - Online Complaint Registration
 - View FIR
 - Case Status Search
 - Missing Person Search
 - Stolen Vehicle/Mobile Search
 - Character Certificate and other citizen services.

- c.) Submission of Complaint** – The complainant fills in the prescribed online form containing:
- Personal particulars of the complainant;
 - Date, time and place of occurrence;
 - Nature of the offence;
 - Details of the accused, if known;
 - Brief facts of the incident; and
 - Contact details for future communication.
 - Relevant supporting documents, photographs, screenshots, videos or other electronic evidence may also be uploaded wherever necessary.
- d.) Generation of Acknowledgement** – After successful submission, the system generates an electronic acknowledgement or reference number. This enables the complainant to monitor the status of the complaint through the portal and serves as proof of submission.
- e.) Scrutiny by the Police** – The complaint is electronically transmitted to the concerned police authorities for scrutiny. The Station House Officer or the designated officer examines whether the complaint discloses the commission of a cognizable offence. If further clarification or documents are required, the complainant may be contacted telephonically or through electronic communication.
- f.) Registration of FIR** – Where the information discloses a cognizable offence and satisfies the requirements of Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, the complaint is converted into a formal FIR and assigned an FIR number. If the complaint does not disclose a cognizable offence, appropriate action is taken in accordance with law.
- g.) Authentication of Electronic Information** – In accordance with Section 173(1) BNSS, where information is furnished through electronic communication, the informant is required to authenticate or sign the information within three days. Compliance with this statutory requirement ensures the authenticity and legal validity of the electronically furnished information.

- h.) Commencement of Investigation – Upon registration of the FIR, the Investigating Officer commences investigation under the BNSS by collecting evidence, examining witnesses, conducting searches and seizures where necessary, and taking all lawful steps for effective investigation.
- i.) Tracking the Case – The complainant can subsequently use the Citizen Service Portal to view the FIR (subject to applicable access rules), check the status of the case, and obtain updates regarding the progress of the investigation.

3.3. CURRENT SCENARIO RELATED TO E-FIR

It is important to mention that as of now, Chhattisgarh has not introduced a universal online E-FIR system for every category of cognizable offence. The State primarily provides an online complaint registration mechanism through its Citizen Service Portal. Where the complaint reveals a cognizable offence, the police scrutinize it and, after compliance with the requirements of Section 173 BNSS, register a formal FIR. Thus, in practice, Chhattisgarh presently follows a hybrid model combining online complaint registration with statutory FIR registration by the police.

4. ADMISSIBILITY OF ELECTRONIC RECORDS

The word ‘admissible’ means the evidence which can be admitted in court and taken on record. The concept of admissibility is completely different from concept of relevancy and probative value of the evidence adduced.

Admissibility of electronic evidence means the legal recognition and acceptance of digital records by a court, subject to compliance with statutory safeguards ensuring authenticity and reliability of the electronic records produced before it.

4.1. ELECTRONIC RECORDS AND ELECTRONIC EVIDENCE – MEANING AND DEFINITION

The term electronic record was first introduced when the Information Technology Act 2000 was enacted. The term ‘electronic record’ is defined as –

“Data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche”⁵

⁵ The Information Technology Act, 2000, § 2(t), No. 21, Acts of Parliament, 2000 (India).

The word ‘Evidence’ is defined as under –

“Evidence means and includes – (1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry and such statements are called oral evidence; (2.) all documents including electronic records produced for the inspection of the Court, such documents are called documentary evidence.”⁶

Now, after the introduction of the new criminal laws in the year 2023, the word ‘evidence’ has been given a broader definition so as to mean –

*“Evidence means and includes – (1) all statements **including statements given electronically** which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry and such statements are called oral evidence; (2.) all documents **including electronic or digital records** produced for the inspection of the Court and such documents are called documentary evidence.”⁷*

4.2. HISTORY AND EVOLUTION OF ELECTRONIC EVIDENCE

The rapid growth of computers and internet communication in the late 20th century led to a major legal shift with the enactment of the Information Technology Act, 2000, which granted legal recognition to electronic records. This law added Sections 65A and 65B to the Indian Evidence Act of 1872, giving digital signatures and electronic recordings legal status.

In the Indian Evidence Act, 1872, as amended after the Information Technology Act, 2000 Section 65B is incorporated, which specifically governs the admissibility of electronic records. Section 65B requires that electronic records be accompanied by a certificate authenticating their production, specifying details such as:

- a.) The manner in which the record was produced,
- b.) The device used to produce the record, and
- c.) Assurance that the record has not been tampered with.

This certificate acts as a safeguard against manipulation, ensuring the integrity of digital evidence and without such certification, electronic evidence is generally considered as inadmissible.

The Parliament introduced the Bharatiya Sakshya Adhiniyam 2023 (hereinafter BSA, 2023) which is a comprehensive legislative effort to amend India's evidentiary framework as

⁶ The Indian Evidence Act, 1872, § 3, No. 1, Acts of Parliament, 1872 (India).

⁷ The Bharatiya Sakshya Adhiniyam, 2023, § 2(e), No. 47, Acts of Parliament, 2023 (India).

part of a broader restructuring of criminal laws. The new Act claims to modernize and simplify evidentiary rules, particularly those relating to digital and electronic evidence.

4.3. JUDICIAL PRONOUNCEMENTS REGARDING THE ADMISSIBILITY OF ELECTRONIC EVIDENCE

Section 65B of the Indian Evidence Act, 1872 makes electronic evidence admissible.

- **State (NCT of Delhi) v. Navjot Sandhu, AIR 2005 SC 3820⁸** - In this case the Hon'ble Supreme Court has held that courts could admit electronic records such as printouts and compact discs (CDs) as *prima facie* evidence without authentication. This case dealt with the proof and admissibility of the records of mobile telephone calls. The accused made a submission that no reliance could be placed on the mobile telephone records because the prosecution had failed to produce the relevant certificate under Section 65B (4) of the Evidence Act and that the procedure set out in section 65B of the Evidence Act was not followed. The Hon'ble Supreme Court concluded that a cross examination of the competent witness acquainted with the functioning of the computer during the relevant time and manner in which the printouts of the call records were taken was sufficient to prove the call records. As a result, it was made admissible without the production of certificate under Section 65B (4) of the Evidence Act
- **Anvar P. V. v. P.K Basheer and Others., (2014) 10 SCC 473⁹** - In this case the Hon'ble Supreme Court overruled the decision in the case of *Navjot Sandhu case (supra)*, and redefined the evidentiary admissibility of electronic records to correctly reflect the letter of the Evidence Act by re-interpreting the application of sections 63, 65 and 65B of the Evidence Act. The Hon'ble Supreme Court declined to accept the view that the courts could admit electronic records as *prima facie* evidence without authentication. It was held that in case of any electronic record, for instance a CD, VCD, chip, etc., the same must be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record is inadmissible. It was further held that

⁸ State (NCT of Delhi) v. Navjot Sandhu, A.I.R. 2005 S.C. 3820.

⁹ Anvar P.V. v. P.K. Basheer and Others, (2014) 10 S.C.C. 473.

Section 65B is a complete code, and evidence from any other source would not be permissible.

- **Shafhi Mohammad v. State of H.P., (2018) 2 SCC 801¹⁰** - In this case, the Hon'ble Supreme Court stated that the requirement of a certificate is procedural and not mandatory. It can be relaxed in certain circumstances, such as when a party does not have control over the original device. Consequently, Section 65B is not considered a complete code.
- **Arjun Panditrao Khotkar v. Kailash Kushanrao, (2020) 7 SCC 1¹¹** - In this case, the three-judge bench of the Hon'ble Supreme Court has provided a definitive and comprehensive clarification. This landmark judgment stands as the latest interpretation of the relevant provisions, offering a consistent approach in line with the legislative intent. It was held that the stand that '*who are not in possession of an electronic device*' is entirely incorrect. The Court clarified that an application can always be made to a judge for the production of such a certificate from the relevant person under Section 65B (4), even if the person refuses to provide it at the first instance. The Hon'ble Supreme Court clarified two issues –
 - a.) A certificate is necessary when presenting electronic evidence as secondary evidence, not when the original record is available.
 - b.) Compliance with Section 65B (4) is mandatory, even if obtaining a certificate is not possible.

4.4. PRIMARY AND SECONDARY EVIDENCE WITH RESPECT TO ELECTRONIC EVIDENCE

PRIMARY EVIDENCE - SECTION 57 BSA	SECONDARY EVIDENCE - SECTION 63 BSA
• Explanation 4 – Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files,	Section 63 BSA is the complete code for admitting secondary electronic evidence, if it fulfils the necessary 4 essentials as specified under Section 63(2) of BSA – a.) The computer output containing the

¹⁰ Shafhi Mohammad v. State of H.P., (2018) 2 S.C.C. 801.

¹¹ Arjun Panditrao Khotkar v. Kailash Kushanrao, (2020) 7 S.C.C. 1.

each such file is primary evidence. • Explanation 5 – Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed. • Explanation 6 – Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence. • Explanation 7 – Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.	information was produced by the computer or communication device during the period over which the computer or communication device was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication device; b.) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or communication device in the ordinary course of the said activities; c.) Throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and d.) The information contained 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.
--	--

4.5. REQUIREMENT OF CERTIFICATE WHEN ELECTRONIC RECORD IS PRODUCED AS SECONDARY EVIDENCE

Under Section 63 (4) of BSA, 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 63 (2) of BSA;
- e.) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device; and
- f.) The certificate issued by the expert.

All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to the admissibility of electronic record.

THE SCHEDULE

[See section 63(4)(c)]

CERTIFICATE

PART A

(To be filled by the Party)

I, _____ (Name), Son/daughter/spouse of _____
residing/employed at _____ do hereby solemnly affirm and
sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following
device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____

Serial Number: _____

IMEI/UIN/UID/MAC/Cloud ID _____ (as applicable)

and any other relevant information, if any, about the device/digital record ____ (specify).

The digital device or the digital record source was under the lawful control for regularly
creating, storing or processing information for the purposes of carrying out regular
activities and during this period, the computer or the communication device was working
properly and the relevant information was regularly fed into the computer during the
ordinary course of business. If the computer/digital device at any point of time was not
working properly or out of operation, then it has not affected the electronic/digital
record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is _____,
obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____

PART B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____
residing/employed at _____ do hereby solemnly affirm and
sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following
device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____

Serial Number: _____

IMEI/UIN/UID/MAC/Cloud ID _____ (as applicable)

and any other relevant information, if any, about the device/digital record _____ (specify).

I state that the HASH value/s of the electronic/digital record/s is _____,
obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____

4.6. STAGE OF FILING THE CERTIFICATE

In the case of *State by Karnataka Lokayukta, Police Station, Bengaluru v. M.R. Hiremath*,¹² the Hon'ble Supreme Court held that –

- a.) The failure to produce a certificate under Section 65B (4) of the Evidence Act at the stage when the charge-sheet is filed is not fatal to the prosecution.
- b.) The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise.

However, this position has changed in view of Section 63 (4) of BSA which provides that a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission.

4.7. TYPES OF ELECTRONIC EVIDENCE AND THEIR ADMISSIBILITY

There are various forms of electronic records. Let us consider some of the important electronic records often produced before the court of law and how it can be proved –

- **PROOF OF IDENTITY OF MOBILE TELEPHONE** – Whenever the identity of mobile number is questioned, it is the duty of the investigation agency to prove the IMEI number of the mobile instrument number. Therefore, it is clear that identity of the mobile number can be proved by proving IMEI number.
- **COMPACT DISC** – In *Shamsher Singh Verma v. State of Haryana*,¹³ it is clearly held by the Hon'ble Supreme Court that the definition of 'document' in Evidence Act includes the compact disc within its ambit. Therefore, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible. So far as authentication of CD is concerned, it needs to be noted that comparison of hash values of original data and the data copied on CD is an important means of authentication. If the CD cannot stand the test of authenticity by its comparison with its hash value with the source, then the transcript of what has been obtained through its audio footage or what it purports to capture cannot be taken as of value.

¹² State by Karnataka Lokayukta, Police Station, Bengaluru v. M.R. Hiremath, (2019) 7 S.C.C. 515.

¹³ Shamsher Singh Verma v. State of Haryana, (2016) 15 S.C.C. 485.

- **PROOF OF VIDEO/AUDIO TAPE RECORDED CONVERSATIONS** – In the case of *Ram Singh v. Col Ram Singh*,¹⁴ the Hon'ble Supreme Court has laid down the following conditions for admissibility of Telephonic conversations as evidence –
 - a.) The voice of the person alleged to be speaking must be duly identified by the maker of the record or by others who knew it.
 - b.) Accuracy of what was actually recorded had to be proved by the maker of the record and satisfactory evidence, direct or circumstances had to be there so as to rule out possibilities of tampering with the record.
 - c.) The subject matter recorded had to be shown to be relevant according to rules of relevancy found in the Evidence Act.
- **PROOF OF CALL DATA RECORDS AND CCTV FOOTAGE** – Regarding the proof and admissibility of mobile phone call records and CCTV Footage, it needs to be proved by producing certificate under Section 63(4) BSA.
- **PROOF OF E-MAIL AND WHATSAPP MESSAGES** – Since mobile phone is computer, the print out taken is a computer output, and hence it requires certificate under Section 63 of the Bhartiya Sakshya Adhiniyam. However, the mere production of a screenshot or printout with the certificate is insufficient to establish authenticity, rather verification of account ownership and device linkage and corroboration with other independent evidence is also crucial.

4.8. ROLE OF EXPERT EVIDENCE

The BSA highlights the value of expert advice due to the technical complexity of electronic records. Experts in digital forensics might assist the court comprehend encryption, tampering detection, recovery procedures, and metadata. Establishing chain of custody and system dependability requires expert testimony. This illustrates the judicial tendency of incorporating technological expertise into court proceedings, particularly in criminal cases involving financial fraud, cybercrimes, or digital monitoring.

¹⁴ Ram Singh v. Col. Ram Singh, A.I.R. 1986 S.C. 3.

5. E-SAKSHYA

E-Sakshya is a digital evidence management system (Mobile App and Web Portal) developed by Ministry of Home Affairs and NIC.

Key Features of the e-Sakshya App are –

- **Real-Time Capture** – Users can instantly record videos and images of evidence and witness statements using the mobile app.
- **Secure Storage & Preservation** – Captured evidence is securely stored, ensuring tamper-proof documentation for legal proceedings.
- **Digital Authentication** – The system verifies and timestamps all recorded materials, maintaining their integrity and credibility.
- **Web Portal Integration** – The app works in sync with a centralized web portal, allowing authorized users to access and review digital evidence
- **Legal Compliance** – Developed as per the latest BNS criminal laws, ensuring that all evidence collection meets updated judicial standards

The Government of Chhattisgarh, after consultation with the Hon'ble High Court of Chhattisgarh drafted the 'Chhattisgarh e-Sakshya Management Rules, 2025'. Rule 3 specifies that every investigating officer shall record the video and photo evidence through the e-Sakshya Mobile Application and under rule 4, the investigating officer is required to generate a certificate in terms of Section 63(4)(c) Part A of the Schedule of BSA through the e-Sakshya Mobile Application.

Further, rule 6 specifies that the sakshya uploaded shall be construed to be forwarded to the Magistrate as required under Section 105 and 185 of BNSS and the Courts can view and manage all the sakshya concerning their jurisdiction in the CIS application/sakshya portal on ICJS and the Court may permit sharing of sakshya with the accused.

6. CHALLENGES TO CREDIBILITY AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

As digital technology has advanced, it has become more difficult to verify the legitimacy of electronic evidence. While the Bharatiya Sakshya Adhiniyam, 2023 offers a legal framework, practical challenges remain due to technical constraints, lack of experience, and the possibility of tampering.

- a.) **POSSIBILITY OF TAMPERING AND MODIFICATION** – Even if the source of electronic record is established, the Court must still be satisfied that the record has

not been altered or tampered with. Digital data can easily be modified without leaving any visible changes, unlike physical documents, which may show signs of erasure or alteration, electronic records may be edited seamlessly. This creates a significant evidentiary risk. Courts must thus rely on forensic experts to identify any possible tampering, falsification, modification and verify authenticity of electronic records.

- b.) **VOLATILITY AND FRAGILITY** – Digital evidence is inherently volatile. Unlike physical documents, which can remain intact for years if stored properly, electronic data is fragile and prone to being lost due to hardware failures, software crashes, accidental deletion, or system malfunctions. If evidence is not promptly preserved or backed up in a secure environment, it risks becoming permanently inaccessible.
- c.) **THREATS FROM DEEPAKES AND SYNTHETIC MEDIA** – Deepfakes, or extremely realistic fake audio and video recordings, are a new threat brought about by artificial intelligence. Even specialists find it challenging to spot falsification because these AI-generated files can make people appear to say or do things they never did. The validity of audiovisual evidence is gravely threatened by this, necessitating the use of more robust forensic instruments and modernised legal requirements.
- d.) **TECHNICAL EXPERT GAP** – One major issue is that many judges, attorneys, and police officers lack technological skills. The legal profession frequently lacks the expertise in digital forensics and cybersecurity needed to handle electronic evidence. Regular training and professional assistance are crucial because this gap may result in mistakes or delays.
- e.) **CHAIN OF CUSTODY** – Failure to properly document the collection, handling, storage, and transfer of electronic evidence can always cast doubt on its integrity. Therefore, the Court must examine whether the electronic evidence was securely handled and documented throughout – from seizure to its production before the Court, including who handled it, whether transfers were properly recorded, and whether integrity checks such as hash value generation confirmed that the evidence remained unaltered.

f.) **MECHANICAL ADMISSION OF ELECTRONIC EVIDENCE** – Courts often admits electronic evidence in routine manner on mere production of certificate without examining the adequacy and reliability of the certificate. Courts must satisfy itself that the statutory requirements for the contents of the certificate have been fulfilled.

7. CONCLUSION

The BNSS, 2023, represents a paradigm shift in India's criminal justice delivery system. While the E-FIR provision under the BNSS, 2023 is a commendable step towards digitizing the criminal justice process, its effective implementation hinges on strengthening the digital infrastructure, ensuring uniform access, and equipping the police force with adequate training and tools. Until these systemic gaps are addressed, the promise of accessible and efficient justice through digital means will remain largely unfulfilled.

The admissibility of electronic evidence is a complex issue that requires careful consideration of a variety of factors. While technology has made it easier to create and store electronic data, it has also created new challenges for courts in assessing the authenticity, reliability, and relevance of such evidence. Courts must balance the need to admit relevant evidence with the need to protect the fairness and integrity of legal proceedings.