SESSION - IV
ELECTRONIC
Devices
ELECTRONIC EVIDENCE
CHANGING TRENDS

Presented by:

M.Sarojanamma

Principal Civil Judge (Junior Division)

Kurnool

INTRODUCTION

The dawn of the Information Technology era has transformed and revolutionized the human world by bringing in its wake a multitude of changes in the way we communicate, connect, transact, function and access information. Technology has become inextricably linked with our day to day lives and the use of communication and technological devices such as mobile phones, laptops, computers, digital cameras etc has become ubiquitous. While enabling us to efficiently carry out our tasks and increase productivity, the virtual world also creates several opportunities for commission of cyber-crimes and provides various forms evidence that may be used to uphold or deny the existence of rights or liabilities. The advent of the Information Technology era has reshaped the landscape of evidence in the courts of law. Being cognizant of the growing electronic means of communication and storing of information in digital form, the legislature, in its abundant wisdom, has enacted the Information Technology Act, 2000 (Act 21 of 2000) to provide legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication and facilitate electronic filings of documents with the government agencies. In addition to the amendments to the Indian Penal Code, 1860 and the Banker‘s Book Evidence Act, 1891, the act has suitably amended the Indian Evidence Act, 1872 to facilitate the admissibility of electronic evidence in the Indian Courts. However, the challenge before the courts is to decide upon the reliability, veracity and integrity of the electronic evidence produced before it.

Scope objective of Digital evidence in Civil and Criminal cases

2. **Scope , object of Digital Evidence in Civil and Criminal Cases:**

What is digital evidence ?

- The evidence is generally termed as proof of records or any relevant information. The explanation to Section 79A of the Information Technology (Amendment) Act (2008) defined the electronic evidence, as any information with values that is stored or transmitted electronically, and it includes evidence such as computer data, digital audio, digital video, cell phones and digital fax machines. Digital evidence refers to stored, transmitted, or collected information that is used as proof before the court of justice. The information is stored, transmitted, or collected in digital media like computers, mobiles, and other electronic devices. The digital evidence may be in numerous forms including, messages, pictures, videos, and other digital forms. There is no need for handwritten notes or fingerprint tests during an investigation with regard to digital evidence. It is always stored in electronic form, not in traditional paper documents.

3. **Scope of digital evidence :**

Nowadays, the scope of digital evidence is widening because of continued growth in the digital world. Digital evidence plays a major role in different areas that include legal proceedings, Cyber security, corporate investigation, e-discovery, intellectual property theft, forensic analysis, and many other areas. Digital evidence is in many forms including electronic communications, digital documents, multimedia files, internet browsing history, computer data, network data, mobile device data, digital signatures, certificates, and many others.

The provisions of Section 65B of Indian Evidence Act (section 63(4) of BNS) apply equally to both civil and criminal proceedings. In essence, electronic evidence is treated as a document and is admissible in court, provided it meets the specific criteria outlined in Section 65B of the Indian Evidence Act.

- There is a greater importance for the digital evidence to substantiate the facts and to prove these cases. Digital evidence is often linked to electronic crimes like identity theft, Cyber stalking, and credit card fraud. It is important in finding Cyber crimes and proving them in court. The use of digital devices assists in uncovering the evidence related to proof of Cyber crimes, data leaks, hacking, and other digital problem and it helps to execute the facts that validate the originality of a work. It will help to mitigate the unauthorized copying or distribution of such property. Property includes literary, artistic, and scientific works, discoveries, performances, phonograms, broadcasts, industrial design, trademarks, service marks, commercial names and designations.

Electronic Devices:

(II) Computer output and output devices:

Computer output means data generated by a computer. This includes data produced at software level. Devices that produced physical output from the computer

are creatively called output devices. Example :

a. CPU **b.**Display Monitor (CRT/LCD/TFT etc.) screens of Mobile Phones,

c. Smart Cards, Dongles and biometric scanners etc:

d. Digital Cameras **e.**Smart Phones

f.Hard Disc Drives g**.** Modems, Routers, Hubs and Switches:

h. Local Area Network (LAN) Card or Network Interface Card (NIC)

i. Servers **j.** Network cables and connectors

k. Printers **l.** Scanners. m**.** Fax machine etc.…

ELECTRONIC EVIDENCE

The term 'Electronic Evidence' signifies a piece of evidence generated by some mechanical or electronic processes which is often relevant in proving or disproving a fact or fact at issue, the information that constitutes evidence before the court. Electronic Evidence is commonly known as Digital evidence. As contemplated Under Section 79A of Information Technology Amendment Act, 2008 defend as electronic evidence.

Digital evidence such as e-mails, computer data digital photographs, word processing documents, spread sheets, internet browser histories, computer backup, secured electronic records and secured electronic signatures, Global Positioning System tracks, system logs, digital- video or audio, digital fax machines, etc., can be permitted by the court to be produced before it during trial in a civil or criminal case.

1. LEGAL LANDSCAPE PERTAINING TO ELECTRONIC EVIDENCE

1.1 Electronic Evidence under the Indian Evidence Act,1872

The Information Technology Act, 2000 has amended S.3 of the Indian Evidence Act, 1872 which defines evidence to include electronic records.

Evidence as defined under S.3 of Indian Evidence Act is as follows:

> "***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; 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*.

However, the term electronic record is defined under the Information Technology Act, 2000.

Section 2(t) of the act defines Electronic Record as follows:

> *"****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."*

Paper documents we used ink for unputs likewise digital word any date is spread into the computer system in binary format.

The word "meta data" means data that provides crucial information about other data in other words it is date about date however speaking legally expression data as defined under Section 20 of Information Technology Act.

The explanation to S.79A of the Information Technology Act defines Electronic Form of Evidence as follows:

> ***"Electronic Form of Evidence"*** *means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.*

A combined reading of the above provisions provides an understanding of what constitutes electronic evidence.

1. Two separate and special provisions deal with electronic evidence. Section 59

says that all facts, except the contents of documents or electronic records, may be proved by oral evidence. It is based on the fundamental principle as best evidence rule.

1. Section 65-A provides that the contents of electronic records may be proved in

accordance with the provisions of Section 65-B. Thus, Section 65-A provides for a special procedure for proving of contents of electronic record. In furtherance thereof,

Section 65-B provides for the procedure.

(I) PROVISIONS OF THE INDIAN EVIDENCE ACT RELATED TO ELECTRONIC EVIDENCE :

• 65A – Special provisions as to evidence relating to electronic record

• 65B – Admissibility of electronic records

• 67A – Proof as to Electronic signature

• 73A – Proof as to verification of Electronic signature• S. 81-A

It contains presumption as to genuineness of every electronic record purporting to be the Official Gazette.

• S. 85-A – Presumption as to electronic agreements- There is a presumption that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

• S. 85-B- Presumption as to electronic records and digital signatures.

• S. 85-C –Presumption as to Electronic signature certificate

• S. 88-A - Presumption\ as to electronic messages

• S. 90-A – Presumption as to electronic records five years old etc..

• Section 131 – Production of documents or electronic records which another person, having possession, could refuse to produce.

- Sec.22A declares that “oral evidence as to the contents of electronic records are not relevant, unless the genuineness of electronic record produced is in the question and in The Information Technology Act, 2000 – Section 2(1) (t) deals with Electronic Record.
- i. The other relevant provisions provided in the Information Technology Act in respect of electronic records are as under:

i. Section 4 relates to the legal recognition of electronic records.

ii. Section 5 relates to the legal recognition of digital signatures.

iii. Section 6 relates to the use of electronic records and digital signatures in Government and its agencies.

iv. Section 7 related with retention of electronic records. It states that if any law provides that documents, records, or information are required to be retained by for any specific period, then, that requirement shall be deemed to have been satisfied if the same is retained in electronic form. Digital evidence is not only limited to that found on computers but may also extend to include evidence of digital device such as telecommunication or electronic multimedia devices. While so, it is appropriate to understand what is computer, computer system and computer network.

1.2 Electronic Evidence under the Bharatiya Sakshya Adhiniyam,2023

The **Bharatiya Sakshya Adhiniyam** (BSA), 2023 has broadened the scope of the Indian Evidence Act, 1872 in respect of admissibility of electronic and digital evidence to keep pace with the contemporary world.

Section 3(d) of the **Bharatiya Sakshya Adhiniyam** (BSA), 2023 has defined a **document** to include electronic and digital records. Thus, the new law considers electronic and digital records to be at par with documents which was not so provided under the Indian Evidence Act. In effect, it provides that such records will have the same legal effect, validity, and enforceability as any other document.

Further, new illustration (vi) added to the definition of documents to account for electronic records – “An electronic record on emails, server logs, documents on computers, laptop, or smartphone, messages, websites, locational evidence and voice mail messages stored on digital devices are documents.”

The definition of "evidence" under Section 2(e)has been made to include "statements given electronically" in addition to statements which the Court permitted or required to be made before it by witnesses in relation to matters of fact under inquiry under subclause (i). Such statements are now called oral evidence under Section 2(e)(i) of BSA.

This contrasts with Section 3(1) of the Evidence Act,1872 which defines oral evidence as statements which the court permits or requires to be made before it by any witnesses, in relation to matters of fact under inquiry.

Thus, the BSA includes the evidence recorded electronically under the ambit of oral evidence and that of digital records within the documentary evidence.

2. RELEVANCY OF ELECTRONIC RECORDS

Section 5 of the Evidence Act provides that evidence can only be given regarding facts in issue or relevant facts. New communication systems and the development of digital technology has necessitated the receipt

of electronic and digital records in evidence to prove or disprove a fact in issue. S.136 of the Evidence Act states that the Judge shall admit evidence if he thinks that the fact, if proved, would be relevant. It means that relevancy must be established before the admissibility aspect can be dealt with. However, as per sections 65A and 65B of the Evidence Act, when read together, the said sections only deal with proof and admissibility of electronic evidence, and not the aspect of relevancy of such evidence. Thus, it is noticed that the relevancy of electronic evidence is determined only after determining the issue of admissibility of such evidence (*i.e., after submission of a certificate under section 65B of the Evidence Act*).

Section 22A of the Evidence Act provides that oral admissions regarding the contents of electronic records are not relevant unless the genuineness of the electronic records produced is in question.

Section 28 of BSA provides that the entries in books of accounts including those in electronic form relevant. Similarly, **Section 29** makes relevant entry in any public or other official book, register or record or an electronic record, stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty.

3. ADMISSIBILITY OF ELECTRONIC RECORDS

Admissibility of evidence refers to whether the court can take such evidence on record and consider it in determining the outcome of the litigation. There are two modes of admissibility of electronic records:

- Original (without certificate) - If a party can produce the original electronic record before the Court, which is a piece of primary evidence8, then there is no necessity to comply with Section 65-B

of the Indian Evidence Act, 1872 and the same is admissible before the Court.

- Computer Output (with certificate) - Documents, including electronic records, must be proved by primary evidence except in those circumstances as enumerated under Section 65 of the Indian Evidence Act, 1872. Whenever an original electronic record cannot be produced before the Court, it can be converted into computer output, i.e., Pen-drive, printout, CDs, etc. makes it secondary evidence. To make this secondary evidence admissible in Court, it must have complied with 65B of the Indian Evidence Act, 1872.

Section 65B of the Indian Evidence Act, 1872 governs the admissibility of the electronic records. The section creates a deeming fiction wherein the 'computer output' which is printed on a paper, stored, recorded, or copied in optical or magnetic media shall also be a document. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer.

Sub-section (1) of S.65B specifies that subject to the conditions specified under S.65B sub-section 2, computer output of the electronic records, which is deemed to be a document, is admissible in evidence without further proof.

3.1 Conditions for Admissibility of Electronic Evidence under the Indian Evidence Act, 1872

Admissibility of a computer output depends on the satisfaction of conditions specified under section 65B(2) which are as follows:

(a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly

to store or process information for the purposes of any activities regularly carried over that period by person having lawful control over the use of the computer;

(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 in ordinary course of the said activities;

(c) Throughout the material part of the said period the computer 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 time, 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 in ordinary course of the said activities.

Thus, compliance with sub-sections (1) and (2) of Section 65B is sufficient to make the electronic records admissible.

3.2 Requirement of Certificate under Section 65B(4) of Evidence Act

Sub-section (4) acts as a crucial authentication tool for certifying the legitimacy of the electronic record and the process of its creation. This sub-section makes admissible an electronic record when certified that the contents of a computer output are generated by a computer satisfying the conditions of sub-section (1) and the certificate being signed by a person holding a responsible official position in relation to the operation and management of the relevant device.

Such a certificate must contain the following particulars:

2. A statement identifying the electronic record containing the statement.
3. A statement describing how the electronic record was produced.
4. Details of the device that produced that electronic record to show it was created by a computer.
5. Statements related to matters enumerated in Section 65B(2) of the Indian Evidence Act, 1872.
6. A statement that the subject matter of certificate is to the best of the knowledge and belief of the person stating it.
7. Should be signed by a person having the official position of that device or management of that device.

There has been some uncertainty regarding the requirement of certificate as to whether it is mandatory. The Honourable Supreme Court has, in the case of ***Arjun Pandit Rao Khotkar vs. Kailash Kushanrao Gorantyal*****(2020) SCC OnLine SC 571,** settled the conflicting rulings on this point and authoritatively ruled that the certificate under S.65B(4) is a condition precedent to the admissibility of electronic records. The Apex Court emphasized the significance of procedural compliance to ensure the authenticity of digital evidence.

3.3Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

To bolster the admissibility of electronic evidence, the BSA introduced **Section 61**, which provides that electronic evidence cannot be declared inadmissible solely by virtue of it being in an electronic form. It provides that no electronic or digital record shall be denied admissibility, if conditions prescribed in Section 63 are met and shall have the same legal effect, validity, and enforceability as any other document.

Section 61 runs as follows:

> Nothing in the Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall have the same legal effect, validity and enforceability as paper records.

This provision bridges the divide between physical and digital evidence, ensuring that electronic records are accorded equal weight and consideration in judicial proceedings.

Section 63 of BSA expands its reach to electronic records in semiconductor memories, in addition to those on paper and stored/recorded/copied in optical or magnetic media.

Sub-section (1) of S.63 is as follows:

> Notwithstanding anything contained in this Adhiniyam, any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or *semiconductor memory* which is produced by a computer *or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output)* shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Furthermore, the provision extends its applicability to encompass 'any communication device,' broadening its scope. Subsection (3) of the provision refines the definition of a computer or a communication device, providing it with a more comprehensive interpretation which includes computers in a standalone mode or those connected in a network.

The BSA introduces robust certification requirements, addressing concerns of data integrity and authenticity more effectively than the IEA.

Section 63(2) of BSA mandates that electronic records must be certified, ensuring that they meet the standards of reliability and integrity.

Section 63(4) mandates a detailed certificate to accompany electronic evidence upon submission.

As per **sub-section (4) of Section 63** of BSA, a stipulation is made as to the submission of certificate along with the electronic record each time electronic evidence is presented before a court. This certification, ensures the record's integrity by confirming that it was produced by a reliable computer or communication device as defined in Section 63(2). This structured certification process, replacing the simpler affidavit system of Section 65B in the IEA, enhances the authenticity and reliability of electronic evidence, reducing the likelihood of disputes regarding legitimacy.

Additionally, the revised provision clarifies that the certificate can be provided by any person 'in charge of the computer or communication device and an expert (whichever is appropriate),' effectively replacing the previous requirement for a person 'occupying a responsible official position.' By bringing in the requirement of certification by experts under sub-section (4) of Section 63, BSA now provides an extra layer of

accountability for admissibility of statements made electronically in evidence (through audio/video mode).

While the IEA did not specify the form of the certificate to be produced for the proof of the secondary evidence, and is often presented as an affidavit in practice, the Section 63(4)(c) of BSA introduced a format of certificate to be produced along with the electronic or digital records. It has introduced a Schedule to the Act containing Parts A and B for this purpose.

Part A needs to be filled by the Party producing the electronic record/output of the digital record, and Part B needs to be filled by an expert to submit that the HASH value of the electronic or digital record is computed from the given algorithms specified in the form itself. HASH value of a file refers to an alphanumeric code which remains the same, until and unless the file has been altered or tampered with. As soon as a file is altered with, its hash value will change and will signify that the file has been changed or altered in some manner.

Section 57 of the BSA has included several forms of electronic evidence into the definition of "primary evidence":

The scope of application of electronic records in evidence is further expanded by the BNS by incorporation of additional explanations 4 to 7 in S.57 of the said Act dealing with Primary Evidence.

As per the **Explanation 4**, electronic or digital records that are stored in an electronic device simultaneously or sequentially in multiple files are to be taken as ‘primary evidence’.

Further, **Explanation 5** provides that electronic or digital records produced from proper custody are to be treated as primary evidence unless they are disputed. Examples include Core-computer systems in

Banks and storing in ‘iCloud’. In this regard, establishing a proper custody of the electronic and digital records would be necessary to lend credence to such evidence. Thus, admission of electronic record contained in a stolen device which has been seized from the custody of accused cannot be considered as being produced from a proper custody.

Explanation 6 lays down that video recordings simultaneously stored in electronic form and transmitted or broadcasted can also be taken as primary evidence.

Explanation 7 stipulates that electronic or digital records is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, are to be treated as primary evidence.

Section 59 of BSA provides that documents shall be proved by primary evidence or secondary evidence except in cases mentioned in the Adhiniyam.

4. ENSURING THE INTEGRITY OF ELECTRONIC EVIDENCE

The peculiar character of electronic evidence is that it may be tampered with or destroyed without even leaving a trace which makes it imperative for the courts to ensure that the integrity of such evidence is not compromised. Integrity of the electronic evidence can be secured by maintaining the chain of custody of evidence. Chain of custody refers to the process of collection, sequence of control, transfer, and analysis. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

The BSA has provided for a format of the certificate, under the Schedule to Section 63(4), which must accompany the electronic evidence. The format of the prescribed certificate requires "*Hash value reports"* of the

electronic/digital records to be declared in addition to also producing the said record. This a significant step in ensuring the integrity of digital record, as Hash value acts as a unique footprint of digital/electronic record, and any tampering of the file would cause a change in the hash value. Hash values have been previously relied upon by courts especially in matters pertaining to cyber-crime to authenticate records, however the current act provides codified recognition to the practice.

The BSA expressly specifies the algorithms that maybe used in computing the hash value of electronic records. They include SHA1, SHA256, MD5 or any other legally acceptable standard algorithm. Hash values are helpful in verifying the integrity of electronic evidence, establishing a chain of custody for electronic records and to detect any tampering or alterations to the evidence.

5. APPRECIATION OF ELECTRONIC EVIDENCE

Appreciation of evidence is a process by which a judge concludes whether or not a fact is proved after evaluation of the evidence on record. It is a duty of the court to appreciate evidence minutely, carefully, and to analyse it.

In ***Tukaram S. Dighole v. Manikrao Shivaji Kokate*, (2010) 4 SCC 329**, it was held that the "Standard of proof" in the form of electronic evidence should be "more accurate and stringent" compared to other documentary evidence.

In ***Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke***, **(2015) 3 SCC 123**, the Supreme Court held that "*source and authenticity* are the two key factors for electronic evidence".

In ***Anvar PV v P.K. Basheer & Ors* (2014) 10 SCC 473**, the Supreme Court held that any documentary evidence by way of an electronic

record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B.

The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer.

The very admissibility of electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2).It is further clarified that the person need only to state in the certificate that the same is to the best of his knowledge and belief. Such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence.

Only if the electronic record is duly produced in the terms of the Section 65-B of Indian Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort cannot be made to Section 45A - opinion of examiner of electronic evidence.

All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic record sought to be used as evidence.

6. PRACTICAL ASPECTS IN DEALING WITH ELECTRONIC EVIDENCE

6.1 Whether the certificate under Section 65B(4) of Evidence Act/Section 63(4) of BSA is mandatory irrespective of whether the electronic record is primary Evidence or secondary evidence

Section 65B is invoked only when a 'computer output' (copy) is used in evidence and it does not pertain to use of original electronic record as evidence in court.

In ***State (NCT of Delhi) v. Navjot Sandhu@ Afsan Guru*** **AIR 2005 SC 3820**, it was held that there is no bar in adducing secondary evidence, under Sections 63 and 65 of the Evidence Act, of an electronic record even without compliance of Section 65B(4).

In ***Anvar PV v. PK Basheer*****, (2014) 10 SCC 473**, the Honourable Supreme Court has overruled the verdict in *Navjot Sandhu's case* and held that Section 65A and 65B of the Evidence Act being special provisions are a complete are a code in themselves and would prevail over the general law. Further, for an electronic record to be admissible as secondary evidence in the absence of the primary evidence, the mandatory requirement of section 65B certification is required to be complied with. The Court observed that:

> "If an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, the same is admissible in evidence, without compliance with the conditions in Section 65B of the Evidence Act."

In ***Vikram Singh and Anr. v. State of Punjab and Anr*** **(2017) 8 SCC 518**, a three-Judge Bench of the Hon'ble Apex Court followed the law laid down in the case of Anvar P.V. (supra), clearly stating that where primary evidence in electronic form has been produced, no certificate under Section 65B would be necessary.

Subsequently, in ***Shafhi Mohammad vs State Of Himachal Pradesh*** **(2018) 2 SCC 801**, a two Judge Bench of the Hon'ble

Supreme Court held that requirement of certificate under Section 65B (4) is not always mandatory.

In view of the 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. The matter was then decided recently by a three-Judge Bench of the Hon’ble apex court.

In ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors*** **(2020) SCC OnLine SC 571**, the Hon’ble Apex Court upheld the law laid down in Anwar PV ‘s case on Section 65B of the Evidence Act and observed that the judgement in *Tomaso Bruno* case is per incuriam and does not lay down the law correctly. Also, the judgment in *Shafhi Mohammad* is found to be not laying down the law correctly and hence overruled.

6.2<u>Relevant stage for production of Section 65B(4) of Evidence Act/ Section 63(4) of BSA certificate</u>

S.65B of the IEA does not specify the stage at which the certificate is to be filed.

In ***Ravindra V Desai*** **(2018) 16 SCC 273**, it was held that non-production of certificate under S.65B(4) of the Evidence Act on an earlier occasion was a curable defect.

In ***State of Karnataka v. M.R. Hiremath (2019) 7 SCC 515***, it was held that the need for production of certificate would arise when the digital record is sought to be produced in evidence at the trial.

In ***Arjun Panditrao Khotkar*** **v.** ***Kailash Kushanrao Gorantyal*****(2020) SCC OnLine SC 571,** the Hon'ble Apex court observed that as long as the hearing in a trial is not over, the requisite certificate can be directed to be produced by the judge at any stage, so that information contained in the electronic form can then be admitted and relied upon as evidence. The court clarified that where either a defective certificate is given, or in cases where such certificate has been demanded and is not given by the concerned person, the trial Judge must summon the person/persons referred to in section 65B(4) of the Evidence Act and require that such certificate be given by such person/persons at the stage when the electronic record is produced in evidence before him without the requisite certificate.

6.3 <u>Appropriate authority for the generation of certificate</u>:

As per section 65(B) of Evidence Act, certificate must be made by a person "occupying a responsible official position". If a person offering the certificate has left the organization, and another person holds that "official capacity," then that another person in the organization can be compelled to give a deposition in a Court instead of insisting the person who had generated the certificate when he was a part of that organization.

In ***Kundan Singh v. The State*** **2015 SCC OnLine Del 13647**, It was held that a person primarily responsible for the management or the use, upkeep or operations of such device can issue the certificate.

In ***Arjun Pandit Rao Khotkar vs. Kailash Kushanrao Gorantyal*****(2020) SCC OnLine SC 571**, the Hon'ble Apex court observed that the certificate under S.65B(4) can be given by -

(1) anyone out of several persons who occupy a ‘responsible official position’ in relation to the operation of the relevant device,

(2) a person who may otherwise be in the ‘management of relevant activities’, and who can give the certificate to the “best of his knowledge and belief”.

The BSA provides a format of certificate consisting of two-parts Part A and Part B. Part A of the certificate is to be filled by the “Party.” Part B of the certificate is to be filled by the “Expert.”

Certificate from the Party Generating the Evidence: This certificate provides firsthand information about the creation, storage, and preservation of the electronic record. It helps to establish the chain of custody and ensures that the record has not been tampered with.

Certificate from an Expert: An expert’s certificate can provide valuable insights into the technical aspects of the electronic record, such as its format, encryption, and potential vulnerabilities. It can also help to authenticate the electronic record and verify its integrity.

It would mean that the certificate must be signed from another person, who has specialized domain knowledge with respect to computers and electronic records. If this interpretation, is taken to be true, would increase the time and costs taken by litigants to procure such certificates.

However, there are no criteria, qualifications or requirements specified by the Adhiniyam, either in Section 63 or in the template of the certificate, which are prerequisite to consider someone as an 'expert'.

6.4 <u>Stage for raising objection to the admissibility of the electronic record for want of 65B certificate</u>.

Any objection pertaining to the non-submission of Section 65B certificate has to be raised at the earliest possible opportunity when the electronic evidence is tendered and such an objection should be dealt with immediately.

In ***Sonu alias Amar v. State of Haryana*** **(2017) 8 SCC 570**, It was held that the challenge to the production of electronic evidence maybe related to its inadmissibility or its mode of proof. In the former case, the objection can be raised at any stage. However, in the latter case, the objection cannot be raised at Appellate stage, if the same was not raised at the time of trial. Since, the non-production of certificate under Section 65B falls under the category of "mode of proof", therefore, the same cannot be raised at the Appellate stage, if the same had not been raised at the trial stage.

In ***Rajender v State (NCT of Delhi)*** **(2019) 10 SCC 623**, the Hon'ble Apex Court has laid down that the objection pertaining to section 65B must be taken at the earliest possible opportunity and that the objection taken for the first time before the high court is not maintainable.

6.5 <u>Admissibility of electronic evidence obtained by illegal means</u>

Article 20(3) of the Constitution guarantees a "right against self-incrimination" meaning that a person shall not be compelled to make any statements, oral or documentary which would militate against his interest.

Courts often come across electronic evidence that is obtained by illegal or not so legal means. For instance, in the matrimonial litigation the parties access the mobile phones, call data records etc of their spouse

to procure evidence. The general approach to be followed by the Court concerning the illegally obtained evidence can be seen from the following judgements.

In ***Umesh Kumar v State of Andhra Pradesh*** **(2013) 10 SCC 591**, the Hon'ble Supreme Court has held that evidence obtained illegally or in violation of any procedural law will not become inadmissible. Such evidence continues to be admissible as long as it is relevant and otherwise admissible.

In ***Deepti Kapur v Kunal Julka*** **(2020) SCC OnLine Del 672**, it was held that though illegally obtained evidence can be read in evidence, it would not absolve the party who obtained such evidence from civil or criminal liability.

6.6 Ensuring integrity and Authenticity of Electronic Evidence

One of the most important challenges when dealing with electronic evidence is preserving its integrity and eliminating the possibility of tampering with it given the volatile nature of such evidence.

Traditional methods of authenticating such evidence include through circumstantial evidence and the chain of custody. Technology based methods include obtaining HASH value of the document, use of Digital Signatures, Time stamping etc.

6.7 Question as to genuineness of the electronic record

In ***Arjun Panditrao's*** case, it was held that the question as to genuineness of an electronic record arises only if such electronic record is duly produced in terms of Section 65-B of the Evidence Act. In such a

case recourse maybe had to Section 45-A of the Evidence Act which provides for the opinion of Examiner of Electronic Evidence.

7. INTERPLAY OF BNS AND BNSS WITH RESPECT TO ELECTRONIC EVIDENCE

The Bharatiya Nagarik Suraksha Sanhitha, 2023 permits all trials, inquiries and proceedings including— (i) issuance, service and execution of summons and warrant; (ii) examination of complainant and witnesses; (iii) recording of evidence in inquiries and trials; and (iv) all appellate proceedings or any other proceeding, to be held in electronic mode, by use of electronic communication or use of audio-video electronic means.

The addition of words "including statements given electronically" under Section 2(e)(i) of the BSA is also in line with the changes brought about in BNSS.

The definition of 'documentary evidence' in BSA now includes digital records and electronic records. The term document has also been redefined to include electronic and digital records. This change is necessitated in view of the changes brought in BNSS which mandate which now mandates audio-video recording in certain scenarios:

- Section 176(3) of BNSS - Videography of evidence collection at the crime scene, where the offence is punishable is made punishable for 7 years or more.
- Section 105 of BNSS – Search
- Section 108 of BNSS – Seizure
- Section 173 of BNSS - In the case of victims of sexual offences, where the victim is physically or mentally disabled.

The inclusion of digital records and virtual testimonies under Sections 2(1)(e) and 63 of the BSA is instrumental in modernizing the judicial

process. It also aligns with Section 530 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), which allows for the electronic examination of witnesses.

8.CONCLUSION

The BSA primarily seeks to broaden the IEA and address the admissibility of digital evidence to keep pace with the contemporary world. The Standing Committee while terming such changes as “forward looking” had, however, expressed concern about the possibility of tampering of electronic evidence when being channelled through the proper chain of custody during the course of investigation. This is especially so considering Section 57, Explanation 5 of the BSA which states that where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed. The Standing Committee recommended adding suitable safeguards in the BNSS to ensure authenticity and genuineness of such electronic or digital records in the BNSS. Changes made by the BSA are in consonance with those made by the BNS and BNSS and will complement each other. These changes will accelerate the trial process resulting in speedy justice dispensation.