SESSION-IV

PAPER PRESENTATION

ON THE

TOPIC OF

ELECTRONIC EVIDENCE

By,
Smt. Sk. Shireen,
V Additional Civil Judge (Junior Division) Cum
V Additional Judicial Magistrate of First class,
Kakinada

Introduction:

The society as on today has developed to the extent where several offences have been taking place by way of electronic and digital means due to which the importance of scientific and electronic evidence during investigation and trial has increased considerably. The Honb'le Supreme Court in ***Tomaso Bruno & Anr vs State Of U.P***[1] observed "*with the increasing impact of technology in everyday life and as a result, the production of electronic evidence in cases has become relevant to establish the guilt of the accused or the liability of the defendant. And that Production of scientific and electronic evidence is of great help to the investigating agency and also to the prosecution.*

As under Section 2 of Bharatiya Sakshya Adhiniyam, 2023 a "***document***" means "*any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records.*"

The word "***Electronic record***" has been defined under Section 2(t) of the Information Technology Act, 2000 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." and "***data***" is defined in Section 2(o) of the Information Technology Act as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."

"***Evidence***" as defined under section 2(e) of Bharatiya Sakshya Adhiniyam, 2023 includes 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; and all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence. Previously Indian

---

[1] **2015 CRI. L. J. 1690**

Evidence Act defined oral evidence as statements permitted to or required to be made before the court by the witnesses, However Section 2(e) of BSA, defines oral evidence as statements including statements given electronically.

Prior to enactment of Bharatiya Sakshya Adhiniyam, 2023, section 3 of Indian Evidence Act, did not include statements given electronically. And a question arose before the Hon'ble Supreme Court, with regard to the question of validity of procedure of recording the oral evidence of witnesses through video conferencing, as Section 273 of the Criminal Procedure Code does not provide for the taking of evidence by video conferencing. The Hon'ble Supreme Court of India in ***State Of Maharashtra vs Dr. Praful B. Desai***[2] held that "*Section 273 provides for dispensation from personal attendance. In such cases evidence can be recorded in the presence of the pleader. The presence of the pleader is thus deemed to be presence of the Accused. Thus Section 273 contemplates constructive presence. This shows that actual physical presence is not a must. This indicates that the term "presence", as used in this Section, is not used in the sense of actual physical presence. A plain reading of Section 273 does not support the restrictive meaning sought to be placed by the Respondent on the word "presence". One must also take note of the definition of the term 'Evidence' as 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 and all documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence" Thus evidence can be both oral and documentary and electronic records can be produced as evidence. This means that evidence, even in criminal matters, can also be by way of electronic records. This would include video- conferencing.*"

The Hon'ble Supreme Court further held that "*Recording of evidence by video conferencing also satisfies the object of providing, in Section 273, that evidence be recorded in the presence of the Accused. The Accused and his pleader can see the witness as clearly as if the witness was actually sitting before them. In fact the Accused may be able to see the witness better than he may have been able to if he was sitting in the dock in a crowded Court room. They can observe his or*

---

2 AIR 2003 SUPREME COURT 2053

her demeanour. In fact the facility to play back would enable better observation of demeanour. They can hear and rehear the deposition of the witness. The Accused would be able to instruct his pleader immediately and thus cross- examination of the witness is as effective, if not better. The facility of play back would give an added advantage whilst cross-examining the witness. The witness can be confronted with documents or other material or statement in the same manner as if he/she was in Court. All these objects would be fully met when evidence is recorded by video conferencing. Thus no prejudice, of whatsoever nature, is caused to the Accused."

Electronic and Digital Records:

Document as under section 2(d) of *BSA* includes both electronic and digital records. A digital record is a computer file that contains information intended to live on a computer or other digital system. This information might be created within the computer system or converted from a physical document into a digital format, e.g., scanned documents. PDFs and multimedia files like audio and video are common digital documents. And also, videos and photographs and presentations etc., While electronic records are also in a digital format, they are typically part of a larger information system, unlike digital records. To read, write, and modify these documents, a supporting platform is required, such as an email server or specific software, like spreadsheet applications. Users can store, access, edit, and share digital documents without needing format conversion. Electronic documents are more system-dependent, and may not be universally compatible. Example, emails, websites, text messages, social media postings, word and excel documents. Electronic records are born and exist solely within computer systems. Whereas, Digital records are digitized versions of physical documents or documents originally created in a digital format. This could be a scanned paper form or a Word document created on a computer.

Electronic Evidence: *The Hon'ble Apex Court in* ***Tomaso Bruno & Anr vs State Of U.P***[3] *observed that the relevance of electronic evidence is also evident in the light of Mohd. Ajmal Mohammad Amir Kasab vs. State of Maharashtra, (2012) 9*

[3] **2015 CRI. L. J. 1690**

SCC 1, wherein production of transcripts of internet transactions helped the prosecution case a great deal in proving the guilt of the accused. Similarly, in the case of State (NCT of Delhi) vs. Navjot Sandhu @ Afsan Guru, (2005) 11 SCC 600, 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." The Honb'le Apex Court also held that non-production and collection of electronic evidence such as CCTV footage, call records and SIM details of mobile phones seized from the accused cannot be said to be mere instances of faulty investigation but amount to withholding of best evidence.

Proviso to section 79A of the Information Technology (Amendment) Act of 2008 states that "electronic form 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 and digital fax machines. And as under BSA, 2023 Electronic evidence includes, oral statements given electronically and electronic or digital records. Illustration (vi) of section 2 (d) of BSA states that electronic records on emails, server logs, documents on computers, laptop or smart phone, messages, websites and voice mail messages stored on digital devices are documents; Electronic evidence includes devices such as mobiles, CD, pen drive, Floppy disk, hard drives or texts, emails, audio and video recordings stored on such devices.

Admissibility of electronic records:

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, states that 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 (referred to as the computer output) shall be deemed to be also a document. Such Electronic record is 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 if the conditions mentioned under section 63 are satisfied.

The conditions as stated under section 63 of BSA are,

(a) that the computer output was produced by the computer or device, during the period over which the computer or 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 contained in the electronic record so derived was regularly fed into the computer or device in the ordinary course of the said activities;

(c) That throughout the material part of the said period, the computer or device was operating properly, in case for any period it was not operating properly or was out of operation, then such part of period, was not such to affect the electronic record or the accuracy of its contents; and

(d) That the information contained in the electronic record reproduces or is derived from such information fed into the computer or device in the ordinary course of the said activities.

Where such creating, storing or processing information for the purposes of any activity regularly carried on over that period was regularly performed by means of one or more computers or communication device, whether in standalone mode (a device or system can function without being connected to something else) or on a computer system; or on a computer network; or on a computer resource; or through an intermediary, all such computers or communication devices used for that purpose during that period shall be treated as a single computer or communication device.

In any proceedings, whether civil or criminal, Section 63 of the *Bharatiya Sakshya Adhiniyam, 2023,* provides for Submission of a certificate along with the Electronic record for:

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) Giving such particulars of any device involved in the production of that electronic record for the purpose of showing that the electronic record was produced by a computer or a device,

(c) Dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and the same shall be signed by the person in charge of the computer or device or the management of the relevant activities and also an expert shall be evidence of any matter stated in the certificate to the best of the knowledge and belief of the person stating it in the certificate.

The schedule of *Bharatiya Sakshya Adhiniyam, 2023,* specifies the following form of certificate to be submitted along with the electronic record:

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: _____

The expert has to state the hash value of the electronic/ digital record and the algorithm through which it is obtained, in his certificate. Hash value is a unique numeric value that represents the contents of a file or data. The hash value of received data can be compared to the hash value of the original data to check if it's been altered. An algorithm is a mathematical function that converts data into a fixed-length string of characters. And SHA-256 is the National

Institute of Standards and Technology's recommended and officially approved standard algorithm.

Section 63 (5) states that information shall be taken to be supplied to a computer or device if it is supplied thereto in any appropriate form whether directly or with or without human intervention or by means of any appropriate equipment; and a computer output shall be taken to have been produced by a computer or device whether it was produced by it directly or with or without human intervention or by means of any appropriate equipment.

Production of certificate under section 63 (section 65-B of IEA):

The interpretation of Law relating to the production of the certificate under erstwhile Section 65-B (4) of the Indian Evidence Act, 1872 along with the electronic record, began with the decision of the Hon'ble Supreme Court of India in ***State (N.C.T. Of Delhi) vs Navjot Sandhu@ Afsan Guru[4],*** Wherein the Hon'ble Apex court while dealing with the call records and printouts of the computerized record held that "*Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the Court. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing Company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge. 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. It may be that the certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65.*"

[4] **2005 (11) SCC 600**

Thereafter in ***Anvar P.V vs. P.K.Basheer & Others***[5]**,** The Hon'ble Apex Court held 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 of the conditions in Section 65B of the Evidence Act. And that an electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. The Hon'ble Supreme Court held that "*notwithstanding anything contained in the Evidence Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document only if the conditions mentioned under sub- Section (2) are satisfied, without further proof or production of the original. The very admissibility of such a document, i.e., electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2).*" Thereby the decision in Navjot Sandhu's case was over ruled.

The Hon'ble Apex Court further 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.

While so, in ***Shafhi Mohammad vs. The State Of Himachal Pradesh***[6], The Honb'le Supreme Court relaxed the condition of production of certificate under section 65-B of the Evidence Act. And held that "The applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing

---

5 AIR 2015 SUPREME COURT 180

6 **(2018) 2 SCC 801**

certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party." And the Hon'ble Apex Court held that "*a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies. And that it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure."* And the Hon'ble Apex Court held that the, requirement of certificate under Section 65B(h) is not always mandatory.

Again the matter was referred to a Three Judge Bench of Hon'ble Supreme Court of India in ***Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal***[7] And the Hon'ble Apex Courrt held that the major premise of *Shafhi Mohammad's case (supra)* that such certificate cannot be secured by persons who are not in possession of an electronic device is wholly incorrect. And held that an application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B(4) in cases in which such person refuses to give it. And thereby the law laid down in Shafhi Mohammed's case was overruled.

The Hon'ble Apex court further held that where the certificate has been applied for from the person or the authority concerned, and the person or authority either refuses to give such certificate, or does not reply to such demand, the party asking for such certificate can apply to the Court for its production under the provisions of the Evidence Act, CPC or CrPC. And when once such application is made to the Court, and the Court orders or directs that the requisite certificate be produced by a person, and the party asking for the certificate has done all that he can possibly do to obtain the requisite certificate. Two Latin maxims become important at this stage, first is *lex non cogit ad impossibilia* i.e. the law does not demand the impossible, and *impotentia excusat legem* i.e. when there is a disability that makes it impossible to obey the law, the alleged disobedience of the law is excused. It was held that the requisite

[7] **(2020) 7 SCC 1**

certificate in Section 65B (4) of the Indian Evidence Act, 1872 is unnecessary if the original document itself is produced. The Hon'ble Apex Court of India held that the provisions of Section 62 of the Indian Evidence Act, 1872 are not applicable to electronic records, and that the certificate as required under Section 65B (4) of the Indian Evidence Act, 1872 is mandatory for admitting secondary evidence of electronic record.

Time of Producing such Certificate:

The Hon'ble Apex Court in *Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal,* held that Section 65B does not speak of the stage at which such certificate must be furnished to the Court. But In Anvar P.V, the Hon'ble Apex Court observed that such certificate must accompany the electronic record when the same is produced in evidence. The Hon'ble Apex court also held that "*We may only add that this is so in cases where such certificate could be procured by the person seeking to rely upon an electronic record. However, in cases 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 Judge conducting the trial 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. This, the trial Judge ought to do when the electronic record is produced in evidence before him without the requisite certificate in the circumstances aforementioned. This is, of course, subject to discretion being exercised in civil cases in accordance with law, and in accordance with the requirements of justice on the facts of each case. When it comes to criminal trials, it is important to keep in mind the general principle that the accused must be supplied all documents that the prosecution seeks to rely upon before commencement of the trial, under the relevant sections of the CrPC.*"

Electronic and Digital Signatures: Electronic signature is a general term for any method of signing a document electronically, such as an image of a signature, a drawn signature, or clicking an "Accept" button. Electronic signatures are often used to replace handwritten signatures and can be fast and easy to create. However, they don't always include proof of identity, so anyone could upload an image of a signature. Digital signature is a type of electronic signature that uses encryption and a digital certificate to verify the identity of the signer and the authenticity of the document. Digital signatures are often used in

regulated industries or when additional identity verification is required. They are considered more secure than electronic signatures.

Proof of Electronic signature: Section 66 of the *Bharatiya Sakshya Adhiniyam, 2023,* provides that an electronic signature must be proved to be the electronic signature of any subscriber which has been affixed to an electronic record, except in the case of a secure electronic signature. Therefore, except in case of secure electronic signature, where an electronic signature is affixed on an electronic record, it must be proved that the electronic signature belongs to the subscriber.

Proof of Digital signature: Section 73 of the Bharatiya Sakshya Adhiniyam, 2023, provides that in order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct the person or the Controller or the Certifying Authority to produce the Digital Signature Certificate; or any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person. Section 73 allows the court to require production of the digital Signature certificate, or Apply public key verification methods to ensure that the digital signatures are authentic or Direct a person to create new writing or signatures in court for comparison purposes, in order to prove the Digital Signature.

Presumption as to Electronic Signature Certificates:

Section 87 of the Bharatiya Sakshya Adhiniyam, 2023, creates a presumption that the information listed in an Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber, unless contrary is proved. Therefore, the court has to presume that the information in an electronic signature certificate is accurate, unless the certificate contains subscriber information that has not been verified.

Presumption as to electronic messages:

Section 90 of the Bharatiya Sakshya Adhiniyam, 2023, creates a presumption that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed

corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent. The Court has to presume that an electronic message's content is accurate as it was when it was input for transmission. However, the presumption cannot be raised as to the identity of the sender.

Presumption as to electronic records five years old:

Section 93 of the Bharatiya Sakshya Adhiniyam, 2023, creates a presumption in case of an electronic record purporting to be or proved to be of five years old, and when the same is produced from any custody which the Court in the particular case considers proper, the Court may presume that the electronic signature which purports to be the electronic signature of any particular person was so affixed by him or any person authorized by him in this behalf. Where the court considers that the the five year old electronic record is produced from proper custody, it shall presume that the electronic signature thereon was affixed by the person it purports to be of or the person authorized by him/her.

Explanation of section 81 of BSA, elucidates, that electronic records are said to be in proper custody if they are in the place in which, and looked after by the person with whom such document is required to be kept; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render that origin probable.

Opinion of expert as to Electronic record:

When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 (21 of 2000), is a relevant fact. This section corresponds to the old section 45-A of the Indian Evidence Act. As under *section 79A of the Information Technology Act,* 2000 the Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Investigation and Trial through electronic means under Bharatiya Nagarik Suraksha Sanhitha, 2023:

Section 532 of BNSS, states that all trials, inquires and proceedings under this Code, including—

(i) summons and warrant, issuance, service and execution thereof;

(ii) holding of inquiry;

(iii) examination of complainant and witnesses;

(iv) trial before a Court of Session, trial in warrant cases, trial in summons-cases, summary trials and plea bargaining;

(v) recording of evidence in inquiries and trials;

(vi) trials before High Courts;

(vii) all appellate proceedings and such other proceedings,

may be held in electronic mode, by use of electronic communication or use of audio-video electronic means.

Section 2 of BNSS, defines "*audio-video electronic*" to include use of any communication device for the purposes of video conferencing, recording of processes of identification, search and seizure or evidence, transmission of electronic communication and for such other purposes and by such other means as the State Government may, by rules provide;

Section 173 of BNSS states that information relating to the commission of a cognizable offence, may also be given by electronic communication to an officer in charge of a police station, and when such information is given by electronic communication, it shall be taken on record by the officer in charge of a police station, on being signed within three days by the person giving information, and the substance of the same shall be entered in a book to be kept by such officer in such form as may be prescribed.

Search and Seizure by electronic means:

Section 105 of BNSS, provides that the process of conducting search of a place or taking possession of any property, article or thing under section 105 or under section 185, including preparation of 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 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.

THE BANKERS' BOOKS EVIDENCE ACT, 1891

The Bankers' Books Evidence Act, 1891 was amended in the year 2000 and 2003 after the enactment of the Information Technology Act, 2000. And it amended section 2(8) and defines *certified copy* to include printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, and a printout of any entry in the books of a bank stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such printout as a copy of such entry. The amended provision provides that such printout of such entry shall contain the certificate in accordance with the provisions of section 2A.

Certificate under Section 2-A:

The printout of entry or a copy stated under section 2(8) of the Act, shall be accompanied by

(a) A certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) A certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of

- The safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons;
- The safeguards adopted to prevent and detect unauthorized change of data;
- The safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
- The manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;
- The mode of verification in order to ensure that data has been accurately transferred to such removable media;
- The mode of identification of such data storage devices;
- The arrangements for the storage and custody of such storage devices;
- The safeguards to prevent and detect any tampering with the system; and any other factor which will vouch for the integrity and accuracy of the system.

(c) A further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge, such computer system operated properly at the material time, he was provided with all the relevant data and that the printout represents correctly, or is appropriately derived from, the relevant data.

Conclusion:

Several offences have been taking place due to the increased use of technology in our day to day lives. Even simple chats in whats app, SMS can be spoofed and modified. And the caller ID and emails of individuals can be spoofed. Therefore, electronic and digital records become relevant in all these cases as evidence. However, the electronic and digital records have to be evaluated carefully. The chain of custody of such records have to be prepared to show who handled the evidence, as mishandling the same can corrupt the evidence. Special skills and infrastructure are required for handling and preserving electronic and digital records. And there is need to formulate safeguards for ensuring the information contained in the electronic records is protected, also ensuring to protect the privacy and confidentiality in such information.

****