HOW TO PROVE ELECTRONIC EVIDENCE: LEGAL FRAMEWORK, CHALLENGES AND JUDICIAL INTERPRETATION

Victoria Joshy, Haveli Institute of Legal Studies and Research

ABSTRACT

In today's digital age, electronic evidence has become a vital element in the administration of justice. As technology rapidly advances, communications and transactions are increasingly conducted electronically, making digital records such as emails, CCTV footage, WhatsApp chats, and electronic documents are essential in both civil and criminal cases. The legal framework in India that governs electronic evidence primarily stems from The Indian Evidence Act of 1872, specifically Sections 65A and 65B and from Sections 61 to 63 in The Bharatiya Sakshya Adhiniyam, 2023, in conjunction with the Information Technology Act of 2000. These provisions outline the procedures for the admissibility and proof of electronic records, highlighting the necessity of a certificate under Section 65B in The Indian Evidence Act, 1872 which is corresponding to Section 63 of The Bharatiya Sakshya Adhiniyam, 2023 to ensure their authenticity and reliability. Landmark judgments, like Anvar P.V. v. P.K. Basheer & Ors.[1] and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors.[2], have clarified these provisions. Practical difficulties persist despite judicial advancements, highlighting the need for a unified approach and updated legal mechanisms to improve the evidentiary value of electronic records in court.

Keywords: Evidence, Electronic and Digital record, Admissibility, Prove, The Indian Evidence Act, 1872, The Bharatiya Sakshya Adhiniyam, 2023, The Information Technology Act, 2000.

[1] (2014) 11 S.C.R. 399, (Civil Appeal No.4226 of 2012)
[2] (2020) 7 S.C.R. 180, (Civil Appeal Nos.20825-20826 of 2017)

Abbreviations:

(1) IEA –The Indian Evidence Act, 1872

(2) BSA - The Bharatiya Sakshya Adhiniyam, 2023

(3) IT Act – The Information Technology Act, 2000

I. INTRODUCTION

People frequently express various statements or claims that they genuinely believe to be true. However, the nature of truth can be subjective, meaning that what one person perceives as a fact might be considered false or disputable by another. The individual making the claim may have either witnessed an event firsthand or heard about it from a reliable source. Yet, when this information is conveyed to another person, it raises two critical questions: "Can we truly trust what we see or hear?" and "Should we rely solely on someone's account because they claim to have witnessed it?"

These questions highlight the essential need for authenticity in the information we receive. As a result, people often seek to verify the validity of these claims before accepting them as truth. This is where the concept of evidence becomes crucial. Evidence serves as the cornerstone for determining the veracity of a statement; it can either substantiate a claim or refute it entirely. Therefore, understanding the role of evidence in evaluating the truth is vital for making informed decisions and forming accurate beliefs.

In ancient times, the methods of proving facts were very different from what we accept as evidence today. Earlier, people relied more on oral testimony, oaths, or even divine tests (like ordeals or duels) to determine truth. With the development of law and technology, these primitive methods were replaced by scientific and documentary forms of evidence, such as written records, electronic data, photographs, and forensic reports etc. has made significant position in society for proving a fact. For example, in olden days, a witness's oath before a deity might have been enough to prove a fact. But today, such a method would not be accepted in a court of law. Instead, oral, documentary or electronic evidence, like CCTV footage or digital communication records, would be considered valid proof.

Thus, the concept of evidence has undergone significant evolution throughout history,

transitioning from reliance on belief and tradition to a foundation rooted in logic and advanced technology. This transformation is driven by the fundamental goal of ensuring that truth and justice prevail, thereby safeguarding innocent individuals from being wrongfully condemned for crimes they did not commit.

In contemporary legal systems, scientific methods have emerged as the most dependable means for establishing the veracity of facts. These methods leverage rigorous testing, objective analysis, and empirical data, offering a level of precision that traditional forms of evidence cannot match.

Within the realm of law, both oral and documentary evidence hold substantial weight, serving as essential tools for demonstrating the truth of a matter in court. Oral evidence, provided by witnesses, can convey personal accounts and observations, while documentary evidence encompasses a wide range of physical records, such as contracts, letters, and photographs. Moreover, with the advent of technology and subsequent amendments to legal standards, electronic records have also been recognized as legitimate forms of evidence. This inclusion reflects the growing importance of digital information in our society, further enhancing the ability to present a comprehensive and factual case in legal proceedings. By integrating these various forms of evidence, the justice system aims to uphold the integrity of the legal process and ensure that outcomes are fair and just.

WHAT IS EVIDENCE?

The term "evidence" originates from the Latin word "evidere," which translates to show clearly, make certain, prove, or discover.

According to **Section 3**[3] of The Indian Evidence Act, 1872 an **"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;]*[4]*such documents are called documentary evidence*.

[3] https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf
[4]Subs. by Act 21 of 2000, s. 92 and the Second Schedule, for the words "all documents produced for the inspection of the Court" (w.e.f. 17-10-2000)

And according to **Section 2 (e)**[5] of The Bharatiya Sakshya Adhiniyam, 2023 an "**Evidence"** means and include- "*(i) 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; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence".*

Both definitions primarily address oral and documentary evidence; however, an important distinction arises regarding the treatment of electronic records. In the earlier definition, electronic records were introduced following the implementation of the Information Technology Act of 2000. This addition specifically pertained to documentary evidence, limiting the scope of electronic records to written forms of proof.

In more straightforward terms, evidence encompasses any material or information that supports or challenges the validity of a fact, and it must be relevant and admissible in a court of law. This can include various forms, such as oral statements made by witnesses, documents like contracts or emails, physical objects like weapons or clothing, or even electronic records such as videos and digital correspondence. Each type of evidence serves the purpose of substantiating claims or disproving assertions, ultimately aiming to clarify the truth of a matter in legal proceedings.

In contrast, The Bharatiya Sakshya Adhiniyam, 2023, significantly expands this framework by explicitly including electronically provided statements within the category of oral evidence. This change acknowledges the evolving nature of communication and technology in legal contexts. As a result, the 2023 legislation offers a much broader interpretation of what constitutes electronic records, allowing for a more comprehensive understanding of evidence in today's digital age. This means that not only traditional written documents but also oral statements delivered electronically are now recognized as valid forms of evidence, reflecting a more contemporary approach to legal proceedings.

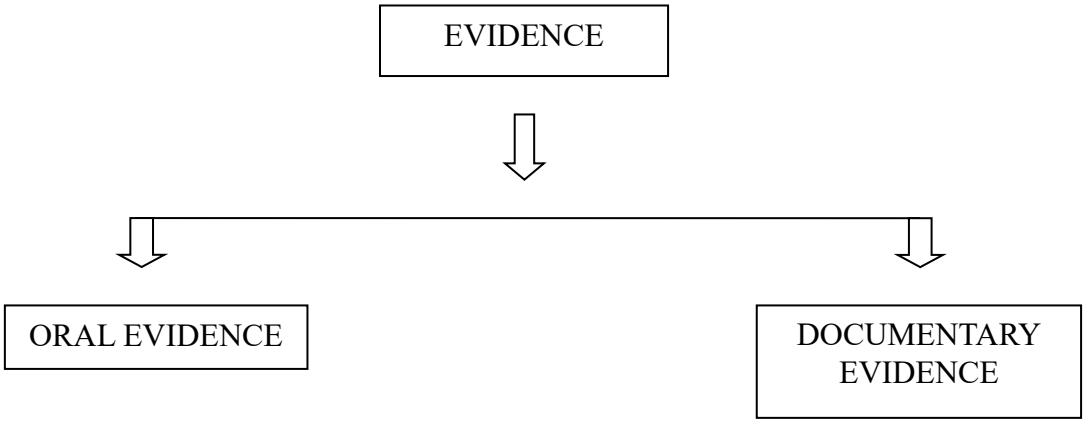
This raises an important question: what exactly is electronic evidence, and how can we effectively utilize it within our legal system? Electronic evidence encompasses a wide range of digital information, including emails, text messages, social media posts, and various forms of

[5] https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf

digital documents. Understanding its significance and application is crucial for modern legal practices. Before we dive into the main topic how to prove electronic evidence let us first understand the 2 types of Evidence recognized by the Court.

II. TYPES OF EVIDENCE

According to statutes of India, Evidence can be classified into two categories and they are: -



As earlier discussed, the term Oral Evidence and Documentary Evidence are already defined in **Section 3** of **The Indian Evidence Act, 1872** and also in **Section 2(e)** of The **Bharatiya Sakshya Adhiniyam, 2023** where the term Evidence is explained, now will see it in detail. Hence, we can see that there is a slight variation in their meaning due to advancement in technology and recognition of it.

(i) ORAL EVIDENCE

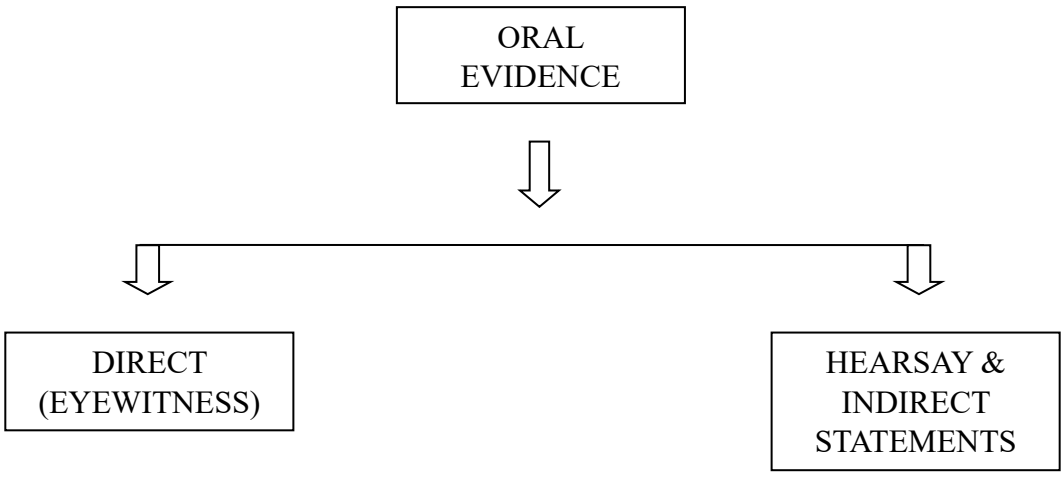
The word "Oral" comes from the Latin term "oralis", which is derived from "os" (genitive: "oris"), meaning "mouth". The term transitioned into Old French as "oral" and eventually made its way into English, retaining the same meaning.

In simple terms:

The word "oral" means "of the mouth" or "spoken". It refers to anything which is verbally expressed.

As per Section 3 and Section 2(e) oral evidence means statements made by a living person before the Court through verbally. It is presented orally in the course of legal proceedings and which cannot be proved only by documents or physical things.

Further, the Oral Evidence is also classified into two groups and i.e.: -



(a) **Direct Evidence**: Direct evidence is the type of evidence that directly establishes a fact in question without needing any inference or assumption. It relies on the personal knowledge or observation of a witness regarding the fact. This type of evidence includes testimony from a witness who personally saw, heard, or experienced the event. In simpler terms, it is a statement made by someone who directly sensed the occurrence themselves, rather than recounting what they heard from others.

In direct evidence also one of the most authentic or genuine type of evidence is Ocular Evidence. Ocular evidence refers to the evidence given by a person who has actually seen an incident or event that has taken place. The word "ocular" comes from the Latin word "oculus", which means "eye". Therefore, ocular evidence is also known as eye-witness evidence. It is considered one of the most direct and primary forms of evidence because it is based on what the witness personally observed. The person giving such evidence is called an eye-witness or ocular witness.

Under Section 60 of The Indian Evidence Act,1872 (corresponding to Section 55 of the BSA, 2023) in detail lays down what are the requisites for a direct Oral Evidence.

For e.g.: -Video and audio recordings, Eyewitness testimony, Confessions etc.

Judicial Interpretation: - Pruthviraj Jayantibhai Vanol vs Dinesh Dayabhai Vala

and Ors.,7[6] wherein it was laid down that: "17. Ocular evidence is considered the best evidence unless there are reasons to doubt it. The evidence of PW-2 and PW-10 is unimpeachable. It is only in a case where there is a gross contradiction between medical evidence and oral evidence, and the medical evidence makes the ocular testimony improbable and rules out all possibility of ocular evidence being true, the ocular evidence may be disbelieved."

(b) **Indirect Statements & Hearsay Evidence:** This evidence refers to the evidence given by person who tends to believe and agree or share their particular opinion about an incident which they saw, heard or experienced. Generally, hearsay are not admissible and indirect statements are admissible in the Court of Law. Indirect statements must be in relation to other facts of the case that means it must be cleared beyond reasonable doubts, as the person is not the actual witness of fact and may turnout either true or false. This type of evidence is used to support the fact of the case that can lead to an accurate conclusion.

However, there are exceptions for such evidences and it is laid down in **Sections 32 & 33 of IEA, 1872 (Sections 26 & 27 of the BSA, 2023)**. That means the exceptions mentioned in this Sections are admissible.

For e.g.: -**The witness repeating gossip, A reported confession, A relayed accusation, circumstantial evidence of state of mind, to prove the words were spoken etc.**

Judicial Interpretation: - Santhoshkumar Vs State rep. by Inspector of Police Perundurai Police Station[7] wherein it has been held that oral evidence cannot take the place of section 65-B (4) certificate.

Also in **Ravinder Singh VS State of Punjab**[8] that the certificate under Section 65B(4) of the Evidence Act is mandatory to produce electronic evidence and that the oral evidence in the place of such certificate cannot possibly suffice.

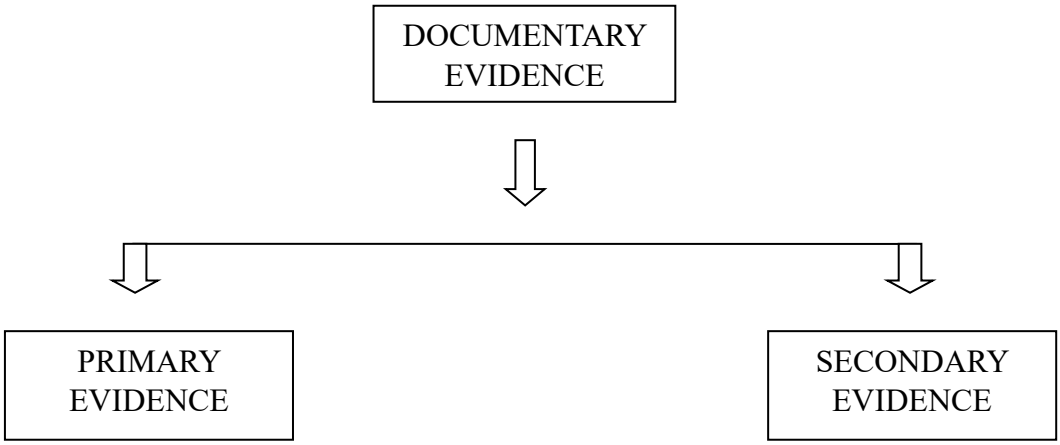
[6] CRIMINAL APPEAL NO. 177 OF 2014
[7] 2021(2) MLJ (Crl) 225
[8] 2022(7) SCC 581

(ii) DOCUMENTARY EVIDENCE

The term **DOCUMENT** is defined in **Section 2(d)** of The Bharatiya Sakshya Adhiniyam, 2023 as - *"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".*

In general terms documentary evidence means any written, typed, printed or recorded material that contains information or data which are in their physical/tangible form or recorded electronically.

The Documentary Evidence is also classified into two categories and they are: -



(a) Primary Evidence: - Primary Evidence means that evidence which is original in nature and which is admissible or legally acceptable by the Hon'ble Court in cases. Primary evidences are explained in **Sections 61 & 62 of IEA, 1872 (Sections 56 & 57 of BSA, 2023)**.

Essentials of primary evidences are laid down in Section 57 of BSA, 2023 (Section 62 of IEA, 1872) and they are as follow:

(1) Original document

(2) Multiple parts execution

(3) Counterparts' execution

(4) Uniform process documents

(5) Electronic/ digital records

For e.g.: - Original art works, printed books, handwritten works etc.

Judicial Interpretation: In **G. Subbaraman vs. State**[9] case, the Court held that normally, any party who wants to prove the content of the document is required to lead evidence by production of the original document before the court through its author. Under Section 61, the original document can be presented before the Court through the author, who created the document and it can be proved.

(b) Secondary Evidence: - Secondary evidence means that evidence which can be used in place of primary evidence if it as some impracticability for presenting it before the Hon'ble Court. These evidences are copy of original evidence or can be transmitted from an original electronic record. According to **Section 58 of BSA, 2023 (Section 63 of IEA, 1872)**, Secondary evidence essential are as follow:

(1) Certified copies

(2) Mechanical process copies

(3) Copies made from original

(4) Counterparts of documents

(5) Oral and Written admissions

(6) Oral accounts of documents contents

(7) Evidence of examination

For e.g.: -Certified Copies, Photocopies, Carbon Copies, Pen drives etc.

Judicial Interpretation: -In the decision reported in **M. Chandra vs. M.**

[9] 2018 Cri. LJ 2377 (Mad)

Thangamuthu[10], it is held that: "It is true that a party who wishes to rely upon the contents of a document must adduce primary evidence of the contents, and only in the exceptional cases will secondary evidence be admissible. However, if secondary evidence is admissible, it may be adduced in any form in which lit may be available, whether by production of a copy, duplicate copy of a copy, by oral evidence of the contents or in another form. The secondary evidence must be authenticated by foundational evidence that the alleged copy is in fact a true copy of the original. It should be emphasized that the exceptions to the rule requiring primary evidence are designed to provide relief in a case where party is genuinely unable to produce the original through no fault of that party".

III. INTERPRETATION OF ELECTRONIC EVIDENCE

Recently, electronic records have been incorporated into legal statutes. In ancient times, people did not utilize electronic or digital means for their daily activities; as such technology had not yet been invented. However, in recent years, advancements in technology have led to an increased reliance on electronic means for communication and various transactions. Today, electronic or digital means have become an integral part of everyday life, to the extent that many cannot imagine living without them.

While these electronic devices offer numerous benefits, they also come with potential risks and misuse. Every technology has its pros and cons. To protect individuals from the negative impacts associated with these technologies, legislation has been enacted; specifically, the Information Technology Act of 2000, trying to protect the people from its negative impact and that no one can misuse it.

It must be borne in mind that possession of electronic evidence is one thing, and proving it is another.

The term **"Electronic Evidence"** has been not explained in any of the Act but the term "**Electronic Record**" is explained in **Section 2 (t)** of The Information Technology Act, 2000 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"*.

[10] 2010 AIR SCW 6362

So, we can say that electronic evidence means electronic record. That means whatever we consider electronic record are electronic evidence

However, it is essential to know what a Data is, it is explained in **Section 2 (o)** of IT Act, 2000, **Data** means **"***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"*

It means that we can say electronic evidence is defined as any information that possesses probative value, meaning it has the potential to impact the outcome of legal proceedings. This type of evidence is stored or transmitted in a digital format, including but not limited to emails, text messages, digital images, video recordings, social media interactions, and data extracted from electronic devices such as computers and smartphones. Due to its ability to establish facts, demonstrate, conduct, and provide essential insights into events pertinent to a case, electronic evidence plays a critical role in judicial proceedings.

Provisions relating to electronic devices or records are given in The Information Technology Act, 2000. Different Acts and special provisions also address electronic evidence. For instance, Section 59 states that all facts, except for the contents of documents or electronic records, may be proven through oral evidence. This is based on the fundamental principle of the best evidence rule. Section 65-A indicates that the contents of electronic records can be proven according to the provisions outlined in Section 65-B. Therefore, Section 65-A establishes a special procedure for proving the contents of electronic records, and Section 65-B provides the detailed procedure for this process.

Some provisions in relation to Electronic Evidence as per The Information Technology Act, 2000 are as follows:

> **(a) Section 4** addresses the legal recognition of electronic records. It states that if any information or matter is made available in electronic form and is accessible, it will be considered to have met the legal requirements that stipulate information or other matters must be in writing or typed form.

(b) Section 5 pertains to the legal recognition of digital signatures.

(c) Section 6 discusses the use of electronic records and digital signatures within government agencies.

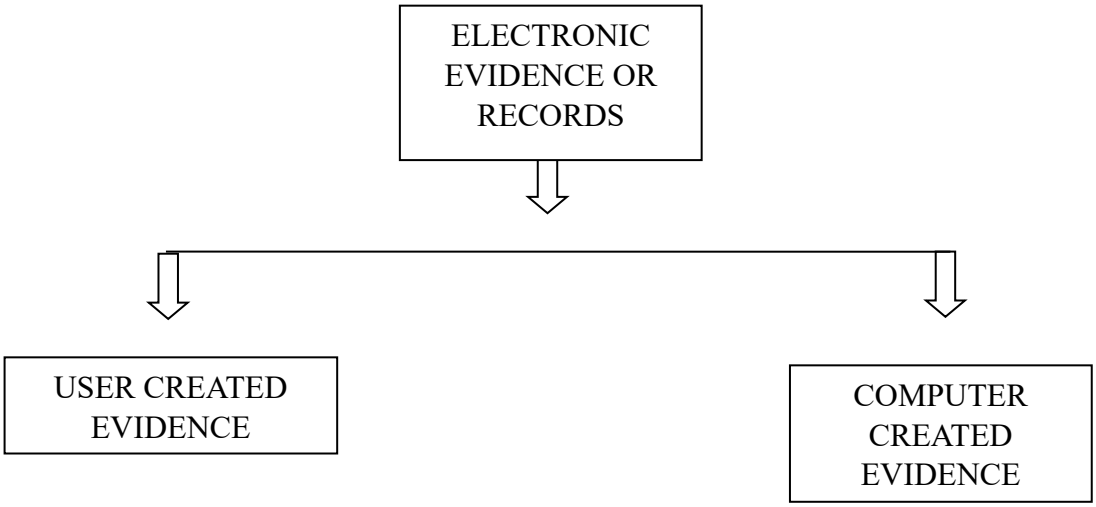
(d) Section 7 relates to the retention of electronic records. It specifies that if any law requires documents, records, or information to be kept for a specific period, that requirement will be considered satisfied if the records are retained in electronic form.

Furthermore, digital evidence refers to information of probative value that is stored or transmitted in binary form. This type of evidence is not limited to data found on computers; it can also include evidence from digital devices such as telecommunications equipment or electronic multimedia devices.

Data generated by a computer encompasses a wide range of information, including those produced at the software level, such as processed data, user commands, and results from various applications. Devices that convert this digital information into a tangible form for users are referred to as output devices. These devices play a crucial role in the interaction between humans and computers, as they display or disseminate information that has been processed by the computer. Examples of output include text appearing on a monitor, printed documents from a printer, and sound emitted from speakers. Essentially, any information that has been processed and then transmitted out from a computer or similar device is classified as output. All the electronic record and devices has different functions and so the ways to manage them are also different.

Electronic evidence is used to clarify the actual fact which is the cause of any issue and to prove an accurate conclusion, so we need to understand its characteristics.

Now, in electronic evidence or records there are two categories and they are as follows:



Sr. No.	**Basis**	**User- created Electronic Evidence/Records**	**Computer-created Electronic Evidence/Records**
1.	Meaning	Electronic Evidence that is created or input by a human user using an electronic device.	Electronic Evidence that is automatically generated by a computer system or software without human intervention.
2.	Nature	It is created intentionally by a person using an electronic medium.	Generated automatically by the computer as part of its normal functioning or system process.
3.	Dependence	Highly dependent on human interactions. User directly creates, edits or sends the contents.	None or Low human involvement. Computer generates the data itself.
4.	Reliability	Depends on the truthfulness and intention of the user who created it.	More reliable because it is system-generated and less prone to human manipulation (unless tampered).
5.	Evidentiary Value	Must be proved under Section 63 of BSA, 2023 (Section 65B of IEA, 1872 with a certificate showing the authenticity of the electronic record.	Admissible as primary evidence if given for inspection from the actual source and sometimes needs certification to ensure system integrity and reliability.
6.	Authentication	Requires proving the authorship and intent of the users.	Requires proving the accuracy and functioning of the computer system that generated the record.

7.	Examples	Emails, Word Documents, PDFs, Digital photographs, social media, Chat or WhatsApp messages etc.	CCTV footage automatically recorded by a surveillance system, Server logs or system logs, ATM transaction records, Call details records (CDRs), GPS data, Metadata or timestamps generated by computer etc.

IV. APPLICABILITY OF ELECTRONIC EVIDENCE IN CIVIL & CRIMINAL PROCEEDINGS

Electronic evidence, often referred to as digital evidence, encompasses any information that is created, stored, or transmitted in digital form that can be presented in a court of law. As society increasingly relies on digital technology for communication and data storage, electronic evidence has emerged as a critical asset in both civil and criminal legal proceedings. Its significance lies in its ability to provide clear, tangible proof that can substantiate claims, identify parties involved, and reveal the sequence of events leading to a dispute or crime.

(i) Role of Electronic Evidence in Civil Cases

In civil litigation, electronic evidence plays a pivotal role in establishing key facts, defining contractual obligations, and clarifying communications between parties involved in a dispute. This type of evidence is diverse and can include various forms of digital documentation, ranging from emails and text messages to recorded video footage and financial statements stored in digital formats.

Key areas where Electronic Evidence is utilized are as follows:

(a) Contractual Disputes: In cases where the terms of an agreement are contested, electronic evidence such as emails, digital contracts, and electronic signatures can substantiate claims regarding offer and acceptance, fulfillment of duties, or instances of breach.

(b) Property and Family Matters: In disputes surrounding property ownership or family-related issues, evidence like CCTV footage can confirm possession or property

use, while digital communication may help establish intentions or agreements made between parties.

(c) Corporate Litigation: In the realm of corporate disputes, electronic evidence is indispensable. Digital accounting records, emails between company officials, and detailed audit trails can either support or refute financial claims, making them vital for fair resolution.

For electronic evidence to be accepted in court, it must meet specific legal standards as outlined in Sections stated in IEA and BSA. This involves presenting a certificate to validate that the electronic evidence originated from a legitimate source, ensuring it has remained unaltered.

Case Law:

Anvar P.V. v. P.K. Basheer & Ors.[11]: Section 65B of Evidence Act deals with the admissibility of the electronic record. The Evidence Act does not contemplate or permit the proof of an electronic record by oral evidence if requirements under Section 65B of the Evidence Act are not complied with. The evidence relating to electronic record is a special provision. Generalia specialibus non derogant, special law will always prevail over the general law. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65A and 65B. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65B are satisfied. Thus, 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. The appellant admittedly has not produced any certificate in terms of Section 65B in respect of the CDs. Therefore, the same cannot be admitted in evidence. [Paras 13, 17, 22 to 23].

(ii) Role of Electronic Evidence in Criminal Cases

In criminal cases, electronic evidence is invaluable for investigation, prosecution, and defense strategies. It plays a crucial role in linking individuals to crimes through digital footprints and helps establish guilt or innocence through detailed communication

[11] (2014) 11 S.C.R. 399, (Civil Appeal No.4226 of 2012)

records and surveillance data.

Key Areas Where Electronic Evidence is Essential are as follows:

(a) Cybercrimes: In cases involving cybercrime, electronic evidence such as emails, IP addresses, and server logs are critical for identifying suspects and establishing intent, shedding light on the methods and tools used in the commission of the crime.

(b) Terrorism and National Security Cases: Digital data, including intercepted communications and social media activity, can be instrumental in revealing criminal conspiracies, thereby assisting law enforcement in preventing potential threats to national security.

(c) Murder or Theft Cases: Technical evidence such as CCTV footage, GPS tracking data, and call detail records (CDRs) often serves as compelling evidence that can directly support or contradict claims made by the parties involved.

(d)Sexual Offenses: In cases involving sexual misconduct, electronic evidence like chat logs, text messages, and shared online content becomes critical in establishing intent, consent, or involvement, often influencing the course of justice.

In criminal trials, the expectations for the authenticity and integrity of electronic evidence are significantly heightened. Courts require:

- A well-documented chain of custody to ensure that the evidence has not been altered or tampered with, safeguarding its integrity.

- A **Section 65B of IEA** or **Section 63 of BSA** certificate to validate the authenticity of the electronic record and confirm its permissible use in court.

- Expert testimony from forensic specialists or cyber experts to clarify complex technical data when necessary, enhancing the understanding and relevance of the evidence presented.

Case Law:

In cases such as ***Shafhi Mohammad***[12], where the parties involved do not have first-hand

[12] (2018) 2 SCC 801

possession of the data and are unable to obtain a certificate, the said court provided some relaxation. It stated that an application must be presented to the judge to seek relaxation of the mandatory requirement under Section 65B (4). However, the subsequent judgment in ***Arjun Panditrao***[13] overruled this decision. It held that the portion of Section 349 of the Criminal Procedure Code (CrPC) stating "...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.

In summary, electronic evidence has become an integral part of the legal landscape, serving as a powerful tool for establishing truth and accountability in both civil and criminal contexts. Its effective use hinges on careful adherence to legal standards and procedural requirements; ensuring justice is served in an increasingly digital world.

V. ADMISSIBILITY & PROVING OF ELECTRONIC EVIDENCE SECTION

In simple terms, Admissibility decides whether the Court can look at that particular evidence in a matter or not and Proof decides what value the Court should give to that evidence and this will lead to the final judgement. Admissibility and proving are two different things. The Court must first accept the evidence and then it is the later process of proving those facts through such admissible evidences. In **Arjun Panditrao Khotkar**[14] the Hon'ble Supreme Court has observed that Section 65 differentiates between existence, condition and contents of a document. Existence goes to 'admissibility' of document and 'contents' of a document are to be proved after a document becomes admissible in evidence. Section 22-A of the Evidence Act provides that if the genuineness of the electronic record produced is questioned, the oral evidence would be admissible as to the contents of the electronic records and also only if the electronic record is duly produced in terms of Section 65-B of the Evidence Act, would the question arise as to the genuineness thereof and in that situation, resort can be made to Section 45-A opinion of Examiner of Electronic Evidence.

First let's see the provisions governing admissibility and proving of electronic evidence under The Bharatiya Sakshya Adhiniyam, 2023. According to this act one new Section is added

[13] (Civil Appeal Nos. 20825-20826 of 2017)
[14] (2020 (5) CTC 200)

related Electronic Evidence validity which is as follows: -

Section 61[15]- *Nothing in this 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, subject to section 63, have the same legal effect, validity and enforceability as other document.*

In this section, it is explicitly stated that electronic evidence will carry the same legal weight as traditional documents when submitted as evidence in court proceedings. This emphasizes the significance of digital records and communications, acknowledging their role in the judicial process and ensuring they are treated with equal importance in the pursuit of justice.

The provisions relating to the admissibility of electronic evidence is given in both the Indian Evidence Act under **Section 65B**[16] and also in the Bharatiya Sakshya Adhiniyam under Section 63. Admissibility of Evidence means when court accepts evidence as relevant and also legally valid. Section 65 B of IEA, 1872 (Section 63 of BSA, 2023) makes electronic evidence admissible; it does not dispense with the relevancy and probative value. In **State of Uttar Pradesh Vs. Raj Narain[17]**, it has been held that facts should not be received in evidence unless they are both relevancy and admissible. The Apex Court in **State of Bihar Vs Sri Radha Krishna Singh[18]** has further held that admissibility of document is one thing and its probative value is quite another thing – these two aspects cannot be combined.

It is also pertinent to bear in mind that non-production of certificate at an earlier stage is not fatal, it is a curable defect. In **Union of India & Ors. v/s CDR Ravindra Vs Desai[19]** The Hon'ble Supreme Court has held as follow: "We are in agreement with the aforesaid findings. Learned counsel for the appellants rightly argued that non-production of the certificate under Section 65-B of the Indian Evidence Act, 1872 on an earlier occasion was a curable defect which stood cured".

The term **proved** is explained in **Section 2 (j)** as "*A fact is said to be proved when, after considering the matters before it, the Court either believes it to exist, or considers its existence*

[15] https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf
[16] https://www.indiacode.nic.in/bitstream/123456789/15351/1/iea_1872.pdf
[17] (1975)4 SCC 428
[18] 1983 AIR 684
[19] (2018 Law Suit (SC) 358)

so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists".

And also the term **not proved** is explained in **Section 2(i)** as "A fact is said to be not proved when it is neither proved nor disproved".

For proving of Electronic Evidence some steps are essential and they are as follows:

1) The electronic record as to be submitted before Court without any tampering or change from the original form.

2) The person who created or handled the evidence must testify its authenticity or a statutory certificate is attached.

3) The evidence and witness statements are observed and decide its accuracy and truthfulness.

4) The judge examines all the facts; oral admissions made by witnesses and also admissible evidences and then sees whether it is creating a link to the fact alleged and bring a reasonable answer for the issues raised before the Court.

Example of Proving evidence before the Court: -

A CCTV video is presented in a murder case:

The videos admissibility will be checked under Section 62 & 63 of BSA, 2023 (65A & 65B. Once the Court admits it, the prosecution must prove it. It can be done by claiming & authenticating that the footage is from the crime scene or the camera was in proper function or the video was not tampered etc.

Electronic records come in various forms, each playing a significant role in modern legal proceedings. The process of establishing the authenticity of these records can differ greatly depending on the specifics of each case. To better understand this, let's explore several frequently encountered types of electronic records in court, along with the legal precedents that guide their validation. By examining these examples, we can gain insight into the methods used to prove the reliability and integrity of electronic evidence.

(1) Proving of Emails

In **Smt Bharathi V Rao Vs. Sri Pramod G. Rao[20],** it has been held that email comes under the definition of electronic record under section 2(t) of IT Act and is admissible in evidence.

It is further held in **Babu Ram Aggarwal & Anr v/s Krishan Kumar Bhatnagar & Ors.[21]** that as per Section 65B of The Indian Evidence Act, 1872, for such emails to be proved, it has to be proved/established that the computer during the relevant period was in the lawful control of the person proving the email; that information was regularly fed into the computer in the ordinary course of the activities; that the computer was operating properly and the contents printed on paper are derived from the information fed into the computer in the ordinary course of activities and a certificate identifying the electronic record has to be proved.

(2) Proving of Call Data Record

In **State of NCT of Delhi Vs Navjot Sadhu[22]**, the accused side raised a submission that no reliance can be placed on the mobile phone call records , because the prosecution has failed to produce the relevant certificate under section 65-B of the Evidence Act, The Supreme Court has concluded that a cross examination of the competent witness acquainted with the functioning of the computer during the relevant point of time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.

(3) Proving of Tape-recorded conversation

In **Yusufalli Esmail Nagree v. State of Maharashtra[23]** it has been reiterated that if a statement is relevant, an accurate tape record of the statement is also relevant and admissible. The time and place and accuracy of the recording must be proved by a competent witness and the voices must be properly identified. One of the features of magnetic tape recording is the ability to erase and re-use the recording medium. Because of this facility of erasure and re-use, the evidence must be received with caution. The court must be satisfied beyond reasonable doubt that the record has not been tampered with. The tape was not sealed and was kept in the custody

[20] MANU/KA/3242/2013
[21] 2013 Law Suit (Delhi 422 at Para 19)
[22] AIR 2005 SC 3820
[23] [1967] 3 S.C.R. 720

of Mahajan. The absence of sealing naturally gives rise to the argument that the recording medium might have been tempered with before it was replayed.

These examples illustrate the process by which an electronic record is authenticated in a court of law. They demonstrate the meticulous scrutiny that each detail undergoes during examination, showcasing the rigorous standards and procedures involved in ensuring the integrity and reliability of electronic evidence. It guarantees that no innocent person suffers for another's wrongdoing, upholding the principles of justice and the interests of all.

VI. LEGAL RECOGNITION OF ELECTRONIC EVIDENCE AT INTERNATIONAL LEVEL

At the international level, various conventions and model laws have been established to harmonize the legal recognition of electronic records, ensuring that these records are afforded the same legal validity as traditional paper documents. This is crucial as governments and organizations move towards digitalization in an increasingly interconnected world.

The **United Nations Commission on International Trade Law (UNCITRAL)**[24] has been instrumental in shaping the global landscape of electronic records. The UNCITRAL Model Law on Electronic Commerce, introduced in 1996, and the Model Law on Electronic Signatures, implemented in 2001, represents significant progress toward achieving universal acceptance of digital communication and documentation. These groundbreaking model laws introduced the principle of functional equivalence, which asserts that if an electronic record serves the same purpose and performs the same function as a paper document, it must be recognized as valid evidence in legal proceedings. This foundational principle has influenced numerous countries, including India, Singapore, South Korea, and Australia, which have adopted national laws and regulations closely aligned with these international frameworks.

United States: In the U.S., electronic evidence is primarily governed by the **Federal Rules of Evidence (FRE)** and the **Federal Rules of Civil Procedure (FRCP)**[25]. These legal frameworks recognize "electronically stored information" (ESI) as equivalent to traditional documents, thereby allowing the use of digital records in court. Under Rule 901, parties are required to establish the authenticity of ESI, which can be demonstrated using metadata, hash

[24] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
[25] https://www.uscourts.gov/forms-rules/current-rules-practice-procedure/federal-rules-evidence

values, or the testimony of expert witnesses. U.S. courts have developed a robust forensic examination system designed to verify both data integrity and the chain of custody for digital evidence. This practical, fact-based approach emphasizes the reliability and relevance of the evidence presented, regardless of its format. However, the discretionary power of Judge's means that the admissibility of electronic evidence can vary significantly based on the technical proof offered in each case.

United Kingdom and Commonwealth Countries: In the United Kingdom, as well as in Canada and Australia, the legal systems have enacted specific provisions recognizing electronic records as valid evidence. **The Civil Evidence Act of 1995**[26] in the U.K. and subsequent regulations allow electronic documents to be admitted as evidence, provided their authenticity and relevance are demonstrated. Commonwealth nations like Singapore and Malaysia have also adopted legislation inspired by UNCITRAL's model laws, reinforcing international standards. For example, Singapore's Evidence (Amendment) Act 2012 explicitly recognizes electronic records as primary evidence. These countries focus on the integrity and reliability of the information, irrespective of the medium storing it, thereby ensuring that judicial processes are both flexible and efficient in the handling of digital cases.

European Union: Within the European Union, the **eIDAS Regulation**[27] mandates that all member states treat electronic signatures and documents as possessing the same legal weight as handwritten signatures and traditional paper records. This regulation has established a tiered system that includes simple, advanced, and qualified electronic signatures. Qualified signatures, in particular, are endowed with a presumption of authenticity in legal proceedings, simplifying judicial processes and enhancing confidence in the validity of digital documents. Consequently, courts across Europe can rely on electronic evidence without the need for supplementary verification, as long as the evidence meets the stringent standards for authentication and security outlined in the regulation.

India: The Information Technology Act of **2000** and **Sections 65A** and **65B** of the **Indian Evidence Act of 1872,** now represented in wider way in **The Bharatiya Sakshya Adhiniyam, 2023.** These provisions detail the procedures for proving electronic records in court, highlighting the necessity of a certificate to confirm authenticity. Indian law closely follows

[26] https://www.legislation.gov.uk/ukpga/1995/38/contents/enacted
[27] https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

UNCITRAL's principles of functional equivalence and reliability, although the practical implementation of the certification requirement often presents challenges due to procedural intricacies.

Globally, electronic evidence is now widely admissible, yet the methods of authentication and the criteria for admissibility differ significantly across jurisdictions. In many European countries, the process has been formalized, with legal presumptions granted to certified electronic signatures, which streamline the admission of such records. Conversely, in the United States and Commonwealth jurisdictions, the emphasis is placed on detailed technical proof—including expert testimony and forensic validation—to establish credibility and reliability. While India has made notable advances in adopting international standards, practical hurdles remain in effectively implementing the certification procedure.

As international cooperation becomes increasingly vital, frameworks like the **Budapest Convention** is instrumental in facilitating the exchange and recognition of digital evidence across national borders. This trend toward global harmonization of digital evidence laws is evident as nations continue to craft international treaties, model laws, and domestic reforms. These efforts aim to create a unified legal approach that balances the rapid pace of technological advancement with the need for legal certainty and clarity.

Countries worldwide are focusing on technology-neutral laws, advocating the use of digital forensics, and providing training for judicial officers to foster a deeper understanding of electronic evidence. To tackle cross-border challenges, there is a strong recommendation for stronger data-sharing protocols and mutual legal assistance treaties (MLATs). Furthermore, as international transactions continue to flourish, the global recognition of digital signatures and cloud-stored data will be essential for facilitating seamless and efficient legal processes in the digital landscape.

VII. CHALLENGES

Electronic evidence, often referred to as digital evidence, encompasses any information that is stored or transmitted in an electronic format and can be utilized in legal proceedings. As technology continues to evolve and pervade our lives, electronic evidence has increasingly become a cornerstone of modern litigation. However, the distinct nature of this evidence brings forth numerous technical, legal, and procedural challenges that must be navigated carefully in

order to ensure its effectiveness in court.

1. **Authenticity and Integrity**

One of the most significant hurdles in using electronic evidence lies in establishing its authenticity and integrity. Unlike traditional physical evidence, digital data can be easily altered, tampered with, or manipulated without leaving noticeable traces. Courts require thorough assurances that the evidence presented is genuine and retains its original form.

2. **Chain of Custody**

Break in chain of custody of electronic evidence. This refers to the meticulous chronological records that outline who collected, handled, transferred, or examined the digital data at any given time gets tampered.

3. **Admissibility and Technical Compliance**

Courts frequently encounter confusion regarding the technical requirements laid out in the Acts which can lead to significant legal complications. Many cases have been dismissed due to the lack of a proper certificate—an essential document that authenticates the methods by which the data was produced.

4. **Preservation and Storage Issues**

The preservation and storage of electronic evidence present formidable challenges due to the inherent volatility and perish ability of digital data. A seemingly innocuous event, such as formatting a drive, experiencing a power failure, or performing a routine software update, can lead to the irreversible loss or corruption of critical information.

5. **Jurisdictional and Cross-Border Issues**

In our interconnected world, electronic data often transcends national borders, posing intricate jurisdictional challenges. The question of which country's laws apply and how to effectively obtain data stored abroad—especially when confronted with foreign privacy regulations—can complicate investigations.

6. Lack of Technical Expertise

A significant obstacle in handling electronic evidence is the lack of technical expertise among judges, lawyers, and law enforcement officials. Many may not possess adequate knowledge of digital systems, encryption protocols, or metadata analysis, which can lead to improper examination and interpretation of electronic evidence.

7. Privacy and Data Protection Concerns

The process of collecting electronic evidence often involves accessing personal data, which can create significant conflicts with individuals' privacy rights guaranteed under Article 21 of the Indian Constitution (Right to Privacy). Striking a careful balance between the needs of an investigation and the protection of individual privacy remains a challenging and critical issue.

8. Lack of Standardized Forensic Procedures

The absence of uniform protocols across various agencies for the collection, imaging, and analysis of digital evidence can result in inconsistencies that pose significant risks. Such inconsistencies may lead to contamination of evidence, data loss, or procedural irregularities, ultimately undermining the integrity of legal processes.

Overall, the challenges associated with electronic evidence are complex and multifaceted, requiring careful consideration and diligence to navigate effectively in legal contexts.

VIII. SOLUTIONS

In today's digital age, electronic evidence has become a critical factor in both civil and criminal proceedings. However, it presents a series of complex challenges concerning authenticity, preservation, and admissibility in legal contexts. To enhance the reliability and effectiveness of such evidence, some practical solutions are in need to address such procedural, legal, and technological aspects.

1. The need for clear and consistent guidelines governing the collection, preservation, examination, and presentation of electronic evidence is paramount. These **Standard Operating Procedures** should be adopted by all investigating agencies to ensure

uniformity and credibility across cases. This procedural framework must include detailed protocols on data imaging—ensuring an exact replica of the original data—and metadata preservation, as well as meticulous documentation of every action taken in the evidence-handling process. The government and judiciary must collaborate to issue standardized protocols, akin to the internationally recognized Digital Evidence Examination Guidelines employed by forensic agencies such as the FBI and INTERPOL. This would help create a solid foundation for handling electronic evidence reliably.

2. A robust chain of custody is essential for maintaining the integrity of evidence, ensuring it remains unhampered from collection to courtroom presentation. Each person interacting with the evidence must be clearly identified, and a comprehensive record of every movement or transfer of data must be meticulously documented to uphold credibility in legal proceedings. Implement advanced digital tracking systems or block-chain-based tools that can log every instance of access or modification to the evidence. This technology would not only enhance transparency but also reinforce trust in the integrity of the evidence throughout its lifecycle.

3. The Statutes requires uniform interpretation and frequent updates to keep pace with rapidly evolving technology. Numerous cases have faltered due to improper certification or misinterpretation of legal standards, complicating the admissibility of electronic evidence. It is imperative to amend Acts to simplify and clarify the certification process. This could include providing greater flexibility in cases where the original electronic device is available and allowing verified digital signatures or forensic authentication to serve as sufficient proof in lieu of stringent certification strictures.

4. The globalization of data storage, often resulting in evidence residing on servers across international borders, creates complexities in obtaining crucial evidence from foreign jurisdictions. Encourage the development of cross-border electronic evidence agreements to streamline and clarify the processes involved in obtaining electronic evidence internationally.

5. As technology advances at a lightning pace, existing laws often struggle to keep up. It is crucial to conduct ongoing reviews of cyber and evidence-related legislation to ensure they remain relevant and effective. Establish a permanent law reform committee tasked with the periodic review and update acts governing Electronic od digital means. This

committee would ensure that the legal framework is continually adapted to address the challenges posed by new technologies and evolving societal norms.

IX. CONCLUSION

In conclusion, the admissibility and proving of electronic evidence play a vital role in ensuring justice in the digital age. Under the Bharatiya Sakshya Adhiniyam, 2023 (formerly Section 65B of the Indian Evidence Act, 1872), electronic records are treated as documents and are admissible if they meet the legal requirements regarding authenticity, integrity, and reliability. Proper certification and compliance with procedural safeguards are essential to establish their evidentiary value. Courts have consistently emphasized that electronic evidence must be accompanied by proof of its origin, accuracy, and unaltered condition. Thus, the effective handling and proving of electronic evidence strengthen the credibility of digital records and uphold the integrity of judicial proceedings in an increasingly technology-driven world.