ISSN (O): 2584-2196

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 3 | Issue 2

2025

Website: www.ijlae.com

Email: editor@ijlae.com

THE IMPACT OF DIGITAL EVIDENCE ON BHARATIYA SAKSHYA ADHINIYAM: IMPLICATION FOR THE LAW ENFORCEMENT AND CYBER CRIME INVESTIGATION

Dhruba Kolay

LL.M. Scholar, Department of Law, University of North Bengal.

ABSTRACT

"Take nothing on its looks; take everything on evidence. There's no better rule."

Charles Dickens, an English Novelist and Journalist

Our legislative system must evolve with technology, especially in the era of rapid transformation. In a tremendous judicial reform, Bharatiya Sakshya Adhiniyam, 2023 is came to enforce to create a modernize framework for establishing digital evidence in India. This new BSA has totally replaced the Indian Evidence Act, 1872 relating to Evidence in India. They found provisions of digital records in the IEA yet there was no specific clear guidance. The BSA, 2023 designated digital texts (emails, SMS. MMS), IP addresses and electronic bank records as primary evidence under sections 57, 58, 61, and 63 of BSA, 2023. This is the digital evidence reform India needs to address cybercrime incidents and align its laws closer.

Keywords: Advancement, Admissibility, Cybercrime, Evidence, Robust, Technology.

INTRODUCTION

We cannot deny the relevance of the Bharatiya Sakshya Adhiniyam for technological advancement in India. Replacing Sections 65-A and 65-B of the Indian Evidence Act with Sections 61, 62, and 63, strengthens the admissibility and credibility of electronic evidence. The BSA,2023 established a landmark step in India's legal digital metamorphosis. The IT Act, of 2000, also played a key role in integrating digital evidence by amending major laws like the Indian Evidence Act, IPC, and Banker's Book Act. Courts now readily rely on electronic evidence, that is securely stored, easily transmitted, and effectively utilized in trials and increasing judicial efficiency. Bharatiya Sakshya Adhiniyam 2023 plays a big role in today's era. Digital evidence is very crucial in cybercrime investigations. Unlike, the eighteen centuries, where crime involved tangible objects, modern offences mainly rely on digital instruments like computers and mobile devices. when such technology is used to commit crime then digital evidence serves as proof of guilt. Apart from that collecting electronic and digital evidence is more difficult than in tangible crime, especially it is very difficult when extraterritorial operations come into the picture. Cyber offenders can operate entire crime from different countries of the world. In recent times hacking, phishing and identity theft are common examples of cybercrime. Supreme Court has also extended the meaning of electronic and digital evidence to include social media like Facebook and WhatsApp messages and posts because many crimes have been committed on social media platforms.

HISTORICAL EVOLUTION OF ELECTRONIC AND DIGITAL EVIDENCE

With digital communication and electronic media everywhere since the beginning of this century, it has become necessary worldwide. The growth of information technology has created a need for laws as people are using electronic payments during e-commerce and information storage processes. In 2000 Indian Parliament introduced Information Technology Act to give legal status to electronic transactions and electronic communication. Indian Evidence Act of 1872 was amended to introduce Sections 65A and 65B to allow digital evidence as admissible in court. Rules for electronic transactions were created by amending Banker's Book Evidence Act regulated by Indian Penal Code of 1860. Judges decide through compelling evidence what

electronic devices show – emails, digital photos, ATM activity reports, GPS coordinates and computer system files. Digital evidence management in India is governed by Sections 61 and 62 and 63 of Bharatiya Sakshya Adhiniyam, 2023 which supersede the earlier provisions of Sections 65A and 65B.

MEANING OF ELECTRONIC EVIDENCE

Digital evidence is a kind of evidence where any information stored or transmitted in digital form can be used in legal and investigation proceedings. It includes various data forms like computers and devices, such as emails, files, metadata and others. Digital means the distribution of analogue world data as a binary numeric encoding in computing and electronics, most commonly heard with digital audio, and digital photography (S Mittal 2021).

Digital evidence: Information of probative value stored or transmitted in binary form; or Information, which is in binary form and capable of being introduced as evidence in presentism. The term is not clear (the word 'digital') as we know that 'binary' does not indicate much tighter, because not all data is analogification. Electronic evidence: Data (consisting of the output of all analogue devices or digitized data), verifiable to any man-made device computer or computer system upon which reflected act that will cause a party's factual account to be more or less probative than it would be without evidence and transmitted as part of the communication system (Dubey, 2017).

Section 4 of Information Technology Act 2000 — LEGAL STAND ON ELECTRONIC RECORDS, legal recognition of electronic records – if a law requires that certain information or other matters be written, typewritten, or printed form then the requirement is considered satisfied if the information or matter is presented on an equivalent or alternative format presented the same meaning like – a) provided or displayed in a digital format, b) Readily accessible for future retrieval and use. (Electronic Governance Sec.4 to 10A, n.d.)

Elements of digital evidence are stated as follows:

1. Any data generated, processed, or stored within a communication device, apart from the human brain and cases of nullification.

2. This includes storage and transmission media such as computer telecommunication systems, smart cards, and navigation units.
3. It is limited to information relevant to the dispute, with admissibility depending on the method collection and potential bias, as determined by the discretion of the adjudicator

EFFECT OF ELECTRONIC AND DIGITAL EVIDENCE ON THE BHARATIYA SAKSHYA ADHINIYAM, 2023

I. Legal effect of electronic and digital evidence

The first Article of Bharatiya Sakshya Adhiniyam2023 proclaims Official electronic and digital records shall be recognised as original sources of evidence right at the entry. Electronic evidence is crucial in the legal field, with courts acknowledging the importance of electronic evidence, such as emails and server logs. even when we submit without physical copies, these digital documents should be filed. The key ends of entering digital evidence in new Adhiniyam are hardly expected like three points to ensure prevention of any cyber crime and proper investigation into cyber-offence. ***State of U.P v. Raj Narain, (1975) 4 SCC 428,*** the court took an extensive approach, to accepting all forms of evidence from various sources, whether entirely should or not, and granting them consideration in proceeding unless probative.

II. Admissibility and authenticity of electronic evidence in Bharatiya Sakshya Adhiniyam

In 2023 The Bharatiya Sakshya Adhiniyam (BSA) established several guidelines for the admissibility of electronic records, digital signatures, and electronic evidence. It helps in providing directions for the preservation and checking the genuineness of digital evidence as Indian Evidence Act, 1872 has some lacunas The BSA guidance also involves aspects of electronic evidence to secure it from any tampering. Admissibility prescribed the requirements in para 23 for keeping authenticated electronic records within protection as original.

III. Admissibility of the Digital Evidence under the Bharatiya Sakshya Adhiniyam

The BSA, 2023 provides the same importance of digital evidence and non-digital evidence in terms of admissibility and authenticity. Digital/Computer record is to be submitted, evaluated and attested by the BSA 2023 guidelines. This novel legal framework is much more concerned of the credence of digital evidence and additionally has fears on that the digital evidence must be unalterable.

Key provisions for admissibility of digital records in Bharatiya Sakshya Adhiniyam, 2023 are as under.

Section 57 of the Bharatiya Sakshya Adhiniyam,2023 stated as follows: In this article, we emphasize those explanations related to digital and electronic evidence, that are the primary focus of this article.

Explanation 4. - Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.

Explanation 5. - Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed.

Explanation 6. - Where a video recording is simultaneously stored in electronic form and transmitted broadcast or transferred

Explanation 7.- Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.

Illustration. A person is shown to have been in possession of a number of placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original (Bharatiya Sakshya Adhiniyam, 2023 section 57)

Section 57 of the BSA by explanations 4, 5 and 6 mostly have centred up admissibility to electronic digital Evidence and it is considered first-class evidence.

4 explanations, explanations under the heading of Section 57. where data and content live and spread across multiple storage files —Explanations 4, BSA referred Explanatory on almost case. When the digital and electronic records are stored in a number of PDF files, each files are treated as primary evidence. Explanation 5 of BSA,2023, primarily addresses the authenticity and proper custody of digital and electronic records. According to section 57, such evidence is treated as primary evidence until proven otherwise. The customer received a copy of Bank Statement from the Bank officers. This is primary (Absolute) Evidence. In this 1, that particular electronic record originated with custody by the agency of institution. Telemetrically Recorded Electronic record type- (Stored, simultaneously stored every current) sent by broadcast or portable (movable) to another: all stored monitoring because all are duplicates. Explanation 6 of (BSA 2023) It is the recording that was filmed and submitted to the same system of transmission transceiver for broadcast and where we store a recording, all as primary Evidence due to set mains of CCTV cameras so each camera or communication device which can capture video. When CCTV footage is recorded then it is recognised as primary evidence when presented in a court of law Those will be treated as primary evidence by the court.

Different case laws show that various electronic records have been accepted as evidence in court. For example, in a number of cases, the court accepted computer printouts ***State NCT of Delhi vs. Navjot Sandhu (AIR 2005 SC 3820)***, emails ***[M/S P.R. Transport Agency vs. Union of India (AIR 2006), Allahabad***, SMS and MMS ***State of Delhi vs. Md Afzal & others, (2015)*** Call records, IP addresses, and electronic bank statements (Mali, 2015). The Supreme Court has expanded the definition of electronic records and digital evidence to include social media platforms like Facebook and WhatsApp messages and posts. Social media platforms have their policies for identifying post creators. However, the extraterritorial jurisdiction of the IT Act, 2000 can compel these websites to disclose the identities of users responsible for offensive posts or communications from particular profiles.

Section 61 of Bharatiya Sakshya Adhiniyam,2023 stated as follows.

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. (Bharatiya Sakshya Adhiniyam ,2023 section 61)

As per this section, the court cannot reject evidence in its entirety on an electronic and digital record. In such cases Courts attach the same legal weight to electronic and digital records as they do to other forms of documentary evidence. Additionally, this provision improves credibility and pliability with court proceedings for electronic and digital evidence.

Section 62 of the Bharatiya Sakshya Adhiniyam,2023 stated as follows.

Special provisions as to evidence relating to electronic record

The contents of electronic records may be proved by the provisions of section 63.

Under this section specifically concerns the importance of electronic records and states that the provision of electronic records may be proved according to section 63 of the Bharatiya Sakshya Adhiniyam, 2023. (Bharatiya Sakshya Adhiniyam ,2023 section 62)

Section 63 of the BSA also discusses the **Admissibility of the Electronic records.**

(1) 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 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.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: -

(a) the computer output containing the information was produced by the computer or communication device during the period over which the computer or communication

device was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication device;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or communication device in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

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

(3) Where over any period, the function of creating, storing or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by means of one or more computers or communication device, whether

(a) in standalone mode; or

(b) on a computer system; or

(c) on a computer network; or

(d) on a computer resource enabling information creation or providing information processing and storage; or

(e) through an intermediary, all the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly.

(4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely: -

(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 as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3);

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.

(5) For the purposes of this section, -

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

(b) a computer output shall be taken to have been produced by a computer or communication device whether it was produced by it directly or (with or without human intervention) using any appropriate equipment or by other electronic means as referred to in clauses (a) to (e) of sub-section (3). (Bharatiya Sakshya Adhiniyam,2023 section 63)

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 indicates that electronic documents can be submitted and is not an extract of Section 65B from the Indian Evidence Act, 1872. A numerous changes have been made to this section. Subsection (1) encompasses information that is stored in semiconductor memory, computer or communication equipment, or saved in an electronic storage device. Section 65B (3) of the Indian Evidence Act, 1872 is a variation of Subsection (3) that alters the provisions for information storage and processing. This is magnificent of BSA. According to the new definition under BSA, data stored and saved over time can be referred to as either an individual computer or other communications system. A certificate also required along with the electronic record under sub-section (4), which also

introduces necessary changes. Additionally, the individual responsible for programming the electronic file must sign the certificate.'? BSA, 2023 is subject to these changes in the legal framework that governs electronic evidence.

Within the case of ***NCT Delhi v. Navjot Sandhu, (2005)*** also broadly known as Afsan Guru, the Supreme Court affirmed electronic evidence could be included in the same category as documentary evidence and the necessities per sections 59 to 65 of the Indian Evidence Act of 1872. Nonetheless, it ultimately unintentionally formed an obstacle to the straightforward acceptance of electronic evidence. The scenario has substantially changed since 2014, with the case of Anvar ***P.V v. P.K Basheer, (2014)*** where, for the first time, the Supreme Court overruled the earlier judgement in Navjot Sandhu. The court aimed to define the parameters under which the electronic records could serve as standard evidence and in conformity with the law by further expounding on the sections 63, 65 and 65B of the Indian Evidence Act. The present provisions of the Bharatiya Sakshya Adhiniyam, more popularly known as the Indian Evidence Act, of 2023 in sections 61 to 65 have lifted all doubts regarding the acceptability of electronic evidence.

In the case of the Supreme Court of India, which is reported by ***Thomas Bruno and ANR vs. State of U.P, (2015) the*** prosecution contended that the two foreign men killed another person from abroad, who were in India for tourism purposes. The events transpired within the confines of a hotel room, where these appellants and the deceased were together. By this, we mean that there were no other people there, except for those who had the opportunity to do the crime. The second retort of the appellants was that they had left the room briefly, and when they returned, they found the friend in a critical condition. They were the ones who, first and foremost, notified the hotel manager, and the other staff members took him to the hospital. The courts below found the appellants guilty as the evidence proved their involvement in the crime beyond reasonable doubt, under Sections 302/34 of the Indian Penal Code. However, the court held that, in the second instance, the CCTV footage, which established the basic evidence, was not there, and therefore, the appeal succeeded. It was an essential task of the prosecution to introduce improper evidence to mislead the jury, and the shortcomings of its case shattered its credibility. The lower courts additionally were inattentive to the flawed investigation, which somehow relied on symptomology that was not even present in the medical reports. Taking into account this unbroken chain of circumstantial evidence and the following reasonable doubt, the prosecution was not able to prove guilt beyond an evil eye. The appellate courts carefully reviewed the case and decided to give the appellate the benefit of the doubt.

On the relevance of electronic records under Section 65B of the Indian Evidence Act, 1872, in addition to the courts, CCTV footage from cameras mounted in strategic places in the compound sets as strong evidence in a murder case. The prosecution's badly prepared argument to show the footage of that nature constituted an indisputable weakness of the prosecution's case.

Analysis

In this case indicates the fact that evidence cannot be dependent solely on observation and unfortunately, the footage from the hotel room is not available because there was no eyewitness. These were allegations made based on the statements of the hotel manager and the police. Courts determined that CCTV footage, although it was never shown in common areas, is the best type of evidence, even for the case in the appeal. The second Explanation (6) of Section 53 of the Indian Evidence Act treats the stored and transmitted electronic video recordings as primary and best evidence with emphasis.

In ***Shamsher Singh Verma vs State of Haryana,*** Criminal Appeal No. 1215, dated November 24, 2015, the court deliberated that the term "document" in the Evidence Act comprehends a compact disc, and it too is a document. Thus, in the case of ***Balasaheb Gurling Todkar and Ors v. State of Maharashtra and Ors (2015 B.M. 1060),*** it was established that it is indeed the case of compact disc, DVD, chip, which has to be accompanied by a certificate in the terms of "65B" at the time of taking the said documents. The same clause has been specified in the Bharatiya Sakshya Adhiniyam, 2023, as Section 63 with a little modification. This is a section whose validity depends on the signature of the person who is in charge of that device.

IV. Tape and Call Recordings as Evidence (BSA, 2023): under the Indian Evidence Act, 1872 as well as the BSA, 2023 both these gave equal importance to admissibility and relevancy of call recording in criminal proceedings.

In the case of ***R.M. Malkani vs. State of Maharashtra, (1973)***,

Now, in the ***State of NCT of Delhi vs. Navjot Sandhu*** case, the person on trial didn't want the phone call record used because the other side didn't have the certificate required by section 65B

of the Evidence Act of 1872. But the Supreme Court grilled the person in charge of the computer at the time to make sure the call record printouts were done right. In the end, that was good enough to use the call record as proof.

V. Admissibility of Email as Electronic Record in court

The admissibility of emails in court depends on the context. The Court generally recognizes emails as emails as electronic records. In the case ***Bharati Rao vs Sri Pramod G. Rao MANU /KA / 3242/2013,*** the court ruled that emails fall under the definition of electronic records as per section 2(f) pf the IT Act, 2000. This means emails can be used as legal evidence in court proceedings. Similarly, In ***Abdul Rohman Kunji vs The State of West Bengal, 2016 CrLj 1159,*** the court stated that emails, once downloaded and printed form an account of an individual, can be varied using sections 65B and 88A of the Indian Evidence Act, along with section 63 and 90 of the Bharatiya Sakshya Adhiniyam, 2023. The person who recovers and prints the emails can be considered a credible source in proving its authenticity.

Section 90 of the BSA,2023 stated as follows,

> ***Presumption as to electronic message*** *– the court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addresses to whom the message purports to the 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 a message was sent.* (Bharatiya Sakshya Adhiniyam ,2023 section 90)

In the case of ***S. Karunakaran vs Srileka, (2019)*** the court stated that, usually court shall not make any presumption as to the person by whom such a message was sent. Therefore, it is clear that the mere filling of an email does not raise a presumption that it was sent by the original originator.

IV. Admissibility WhatsApp message in the court of law

WhatsApp messages, along with Facebook chats, are admissible in court. A blue tick on WhatsApp confirms the recipient reads the message, making it valid evidence. In (the **State *of Delhi vs Mohd. Afzaland others,* 2003)** the court stated that WhatsApp, text messages, Facebook messages, and other electronic evidence are fully admissible in the Indian court of law. Also referred to the ***Afzal Guru case***, the Supreme Court of India held that electronic

evidence is admissible in the court. A certificate bearing the signature of the person who is in charge of the computer device is required during the time of producing evidence before the court of law.

The court also stated that the burden of proof shall be imposed on the person who contesting the electronic data.

MAJOR CHANGES INTRODUCED BY BSA REGARDING ELECTRONIC AND DIGITAL RECORD

1) The Bharatiya Sakshya Adhiniyam has extended the nature and scope of the definition of the term "Document" and stated that Electronic and digital records shall come in the ambit of the definition of the document under section 2(d) of BSA, 2023. In addition, the definition of evidence that shall be included is 'information given electronically' that comes under the ambit of oral evidence.
2) On the other hand, section 57 of BSA defines the term of primary evidence. And also stated the several explanations which is considered the primary evidence. Especially focusing on the explanations 4, 5, 6 and 7 of section 57 of BSA.
3) Sections 61, 62, and 63 have been introduced by the BSA, 2023 which increased the ambit of the digital and electronic evidence. The BSA also added certain modifications with those section that more effectively implemented the function of digital evidence in the court of Law.

LANDSCAPE OF SUPREME COURT REGARDING ELECTRONIC EVIDENCE IN INDIA

In ***Som Prakash vs. State of Delhi,*** **(1974)** the Supreme Court stated that depending solely on the traditional form of evidence in a technological age is now traditional and it prevent forensic progress. The scientific method of investigation is crucial for solving modern challenges in criminal trials.

In ***SIL Import, USA v vs. Exim Aides Exporters, Bangalore*****, (1999)** the Supreme Court held that "*Technological advancement like facsimile, Internet, e-mail, etc. were in swift progress even before the Bill for the Amendment Act was discussed by Parliament. when Parliament*

contemplated notice in writing to be given, we cannot overlook the fact that Parliament was aware of modern devices and equipment already in vogue." (Sharma, 2019)

In ***State vs. Mohd. Afzal And Ors*****, (2003)** the court stated that electronic records which are derived from computer devices and any other communication devices are admissible before the court of law and may be considered the substantive piece of evidence. But the condition is that the record was produced before the court according to the provision of section 65 B of the Indian Evidence Act,1872, and now section 63 of Bharatiya Sakshya Adhiniyam,2023.

In ***Avnish Bajaj vs. State*****, (2008**) this court observed that what kind of difference we draw between the Internet Service Provider and Content Provider was raised. The burden of proof was raised on the accused because of that he was the Service Provider and not the Content Provider. It has raised a lot of issues and controversies regarding how the police should prevent cyber offences and a lot of education is required.

In 2017, the court ruled that certificates under section 65B (4) are just a "mode of proof " **Sonu@Amar V. State of Haryana, (2027)**. Earlier, not having a certificate was seen as a flexible issue. This view was reinforced in ***Shafhi Mohammad vs State of Haryana, AIR (2018) 2 SCC 801*****,** where the court held that the certificate requirement is procedural, not mandatory, especially when the original device is beyond the control of a party. As a result, section 65B is not a standalone rule and now falls under section 63 of the BSA. After this landmark judgment, there are several contradictions and confusion were created between the interoperation of law. This problem of interpretation was solved by the case which is ***Arjun Panditrao Khotkar vs Kailash Krishanro*****, (2014)** in this case court resolved the dispute completely. The court held that the certificate of electronic document is necessary when it is produced by secondary sources. But when the original electronic evidence is produced before the by the owner itself then the submission of electronic evidence is not required and the court treated it as the primary evidence. The owner of any communication device like a computer, mobile, etc… the owner testifies to the document by itself and in this case, the owner of such device should produce the original electronic record as the form of evidence.

But subsection 4 of section 63 of the BSA stated that,

In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely: -

(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 as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3);

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate, and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.(Bharatiya Sakshya Adhiniyam ,2023 section 63(4))

Above mentioned things shall be submitted before the court along with the electronic record. section 63 of BSA is the modified version of section 65B of the Indian Evidence Act.

HOW FAR IS THE DIGITAL AND ELECTRONIC EVIDENCE RELEVANT TO CONDUCTING CYBERCRIME INVESTIGATION

Digital and Electronic evidence play very significant roles in cybercrime investigations in today's world. The technology is within the capability of law enforcement agencies and therefore they can trace communication devices, trace locations, and investigate crime in cyberspace. Several investigation techniques are based on digital evidence to help solve cybercrimes.

1. With Crime: IP addresses, MAC addresses, and metadata enable cybercrime investigators to trace back attacks to devices, where they came from, and who the attackers are. Server logs, firewalls, and software keep an eye on what people do, enabling it to follow attackers with ease and build timelines. And then they all end up in court as evidence.

2. Identify the perpetrators by Login details, websites browsed, and purged chats giving the police clues to attribute the subject to the crimes. Computer forensic examination of computers analyzes confiscated computers to demonstrate information saved and routine, open evidence of being an active participant in cybercrimes.

3. Chronology of Events Building:

Timed evidence helps agencies create event timelines and link them with suspicious behaviour in the process. Messenger and email logs keep a record of chats, with senders and receivers, and are accepted as evidence in courts.

4. Importance of Documentary Evidence:

Together with Physical Evidence, it is of the most crucial significance in cybercrime investigation. we can never overemphasize Documentary evidence's power to unveil the offender. Digital evidence can corroborate physical evidence. e.g. mobile phone location evidence can support eyewitness evidence or be used to identify suspects at a crime scene. Also, use a Chain of Custody: While performing electronic forensics, an electronic evidence chain be followed strictly so that electronic evidence is maintained in its original state to be able to legally present it in court.

5. Motive and Intent Evidence: different motives of crimes, monetary transactions, i.e., crypto wallets and accounts, reflect motive for ransomware and fraud crimes. Search history and messages can be recovered as evidence of intent, primarily in hacks or malware attacks.

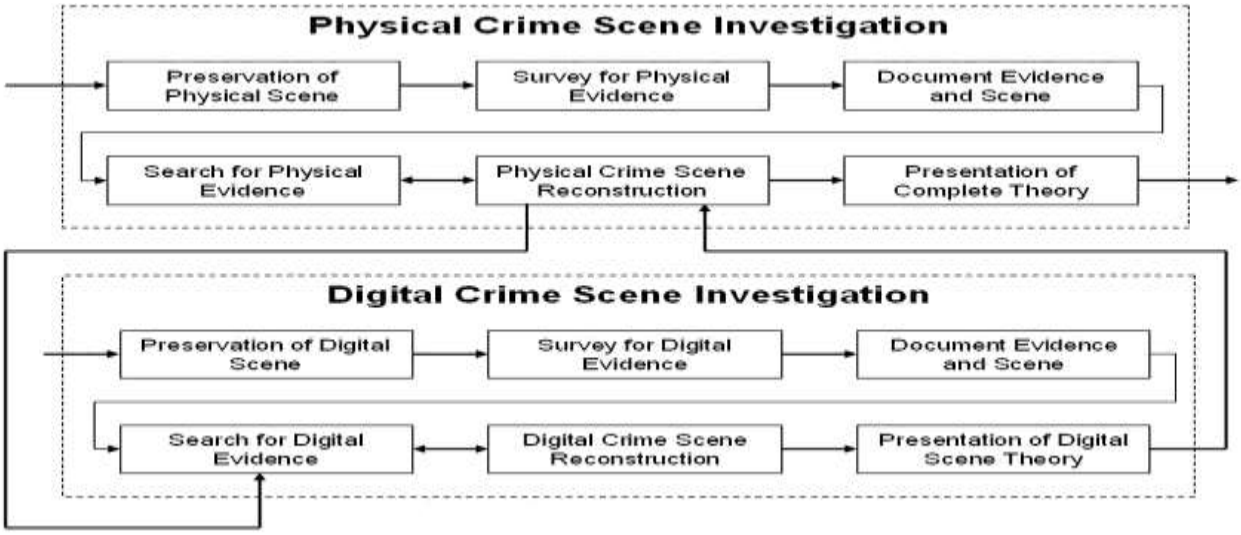
6. Prosecution and court Hearing

Electronic evidence is largely introduced in court to directly link suspects with cybercrime investigations. It has to be used carefully because it will achieve nothing if it's not applied effectively. It also has to be used in Refuting or Supporting Alibis. Electronic data, including geolocation data, can be used to validate or refute an alibi, showing whether the suspect was there or not at the crime scene.

HOW TO COLLECT THE DIGITAL EVIDENCE FOR CYBERCRIME INVESTIGATION

Digital evidence in cybercrime cases can be collected in two ways:

Fast Adaptive Re-sampling: During its forensic investigation, police confiscate the suspect's mobile, and submit it to a forensic lab for analysis. If not technically competent, forensic officers retrieve evidence from WhatsApp, call detail records, social networking sites and emails. Secondly Victim Evidence: Aware victims can keep the evidence of the crime from getting erased by; not deleting messages or chats, not responding to threatening posts, taking screenshots of threatening posts and the links, not responding to the sender without opening the suspicious links, saving the sender email address of the attack. It's necessary to save social media Evidence so that it doesn't delete as kind of Evidence. In such cases, both victims and police must do that because the Evidence can be collected as best it can be.



(Dnyotech, n.d.)

Our above diagram indicates the procedure of the cybercrime investigation in India as well as in foreign countries. The cybercrime investigation is almost the same as a physical crime investigation like, Murder, Rape, Dacoity. First preservation and conservation of digital evidence, properly surveying the digital evidence by investigating authority. The third stage is

document evidence which means the proper function and methods used to properly document the crime scene. This method consists of written notes which are ultimately used to prepare the final report, the crime scene photograph of the physical crime, and in the case of cybercrime analyzing the website and examining the screenshot of the site and obscene materials. In the 4th stage various cybercrime scene evidences which are need to be searched. In the case of cybercrime, the police officer needs to search several things like; the website from which any link has been sent, any chat from WhatsApp and Facebook, and also check the mail of the victim. The fifth stage is crime scene rebuilding is the method where a police officer tries to determine how a crime was committed and also reconstructs it by interviewing the witnesses. In this investigation, the authority examines the victim and also examines the motive of the offender and finds out the suspect. And finally, the investigating authority presents the complete theory about cybercrime and finds out who is the actual culprit. However, the investigating authority and policy are not always successful in finding the actual offender.

LOOPHOLES OF DIGITAL AND ELECTRONIC EVIDENCE FOR CYBERCRIME INVESTIGATION IN INDIA

For its sensitive and unique nature and the way it needs to be handled, depositing digital evidence in court comes with huge complications. Here are a few of the most main challenges and difficulties investigating agencies face during their investigations, which are essential to our discussion:

1. Authenticity and Integrity

With digital evidence, it's easy to change or even create fake messages so proof has to be provided for its authenticity. There needs to be a clear record for the chain of custody because any break in it can result in the loss of evidence integrity and admissibility.

2. Legal Standards for Admissibility

Like many other rules, digital evidence also has to comply with the requirements for relevance, reliability proofs, and authenticity; Otherwise, it will most certainly be left out. There are too

few precedents to guide the application and presentation of evidence with the new BSA 2022 and so much new case law may complicate matters.

3. Privacy and Data Protection Issues

Using advanced proof techniques can be easily destroyed by cyber intrusions because of the use of high technology. Cases like phishing, spear phishing, hacking, and malware are very common.

4. Technical Complexity and Interpretation

Judges and lawyers not having the requisite technical knowledge is undoubtedly specialized knowledge, which can result in the misinterpretation of digital proof. Experts in digital information are often considered to be credible by the courts, but their competence and clarity can be questionable.

5. Preservation and Volatility of Evidence

Digital evidence is potentially volatile and can be crumbled or destroyed if the capturing functionality does not work properly. The authorities must take charge of the evidence at the right time, as either the data could change or can disappear which may cause reservations on the preservation efforts. The preservation of digital evidence requires specific procedures and techniques of storage and handling to minimize or endanger the degradation or accidental alteration of the artefacts. Errors in these processes can cast doubts about the reliability of the evidence.

6. Encryption and Access Barriers

Effective encryption can impermissibly obstruct access to digital evidence, which makes it difficult legally or technically to have this evidence decrypted. The courts need to balance the privacy rights of citizens against law enforcement needs, and thus warrants need to be acquired instead of random searches.

7. Cybersecurity Threats to Evidence Integrity

Cyber-attacks may likely occur. Digital evidence is open to cyber-attacks such as hacking and ransomware, which disrupt the integrity of the evidence. Spoofing and deepfakes are pressured.

Thus, identical evidence, including videos and photos, is manipulated or faked using advanced techniques that are more troublesome to determine the authenticity of the evidence.

8. Time and Cost Constraints

Resource Intensive: Digital forensic investigations are time-demanding and have great needs of resources, for example, for examination of medium or large size networks with many connected devices. It is often needed to employ expert personnel who possess high analytical skills so that the verification of the findings might be costly. Digital forensics tools and experts might have less technology with an evidence-based chain, especially in cases with limited resources.

SUMMARY AND CONCLUSION

The Bharatiya Sakshya Adhiniyam (BSA), 2023 modernizes India's evidence laws to align with digital advancements. It strengthens the credibility and admissibility of electronic records through Sections 57, 61, 62, and 63, addressing data privacy, security, and proper handling of digital evidence. Essential for prosecuting cybercrimes like data breaches and phishing, it enables courts to rely on digital records, reducing dependency on physical documents and speeding up trials. By enhancing the legal framework for electronic evidence, BSA 2023 makes the judicial system more efficient in handling cyber-related cases.

REFERENCES

ARTICLES

Dubey, V., (2017). *Admissibility of Electronic Evidence*: An Indian Perspective. Forensic Research & Criminology Internation Journal, 4 (2).

https://doi.org/10.15406/frcij.2017.04.00109

Mittal, s (2021). *E – evidencing and its admissibility*. Journal of Legal Studies and Research, 7(3), 74-93. The Law Brigade (Publishing) Group.

https://thelawbrigade.com/

Sharma, H. (2019, July 1). *Admissibility of electronic evidence under Indian laws*—a brief overview. Lawyersclubindia.

https://www.lawyersclubindia.com/articles/admissibility-of -electronic-evidence-under-indian-laws-a-brief-overview-10310.asp

CASES

Anvar P.V vs P.K Basheer, (2014) 10 SCC 473 (India).

Arjun Panditrao Khotkar vs Kailash Krishanro, (2014), (10) SCC 473

Avnish Bajaj vs. State, (2008) (105) DRJ 721 MANU/DE/0851/2008

NCT Delhi v. Navjot Sandhu alias Afsan Guru, (2005) 11 SCC 600 (India).

S. Karunakaran vs Srileka, Appeal Suit No .292 of 2019 (Madras High Court, 2019)

SIL Import, USA v vs. Exim Aides Silk Exporters, Bangalore, (1999) 4 SCC 567

Som Prakash vs. State of Delhi, (1974) SC 1974 cri. LJ 784, MANU / SC / 0213/ 1974

Sonu@Amar V. State of Haryana, (2027) 8 SCC 570

State of Delhi vs Mohd. Afzaland others, (2003) 107 DLT 385 (India)

State vs. Mohd. Afzal And Ors, (2003) DLT 385, 2003(71) DRJ 17

Thomas Bruno & ANR. vs. State of U.P, (2015) SCC 178 (India).

IMAGE

Dynotech. (n, d.). crime scene [photograph]. Dnyotech.

http://www.dynotech.com/articles/image/crimescene.jpg

STATUTES

Electronic Governance (section 4 to 10A). (n.d)

http://informationtechnologyactindia.blogspot.com/p/electronic-governance.html?m=1

Government of India. Bharatiya Sakshya Adhiniyam, 2023 (Act No.47 of 2023), section 57.

https://www.indiancode.nic.in/handle/123456789/20063

Government of India. Bharatiya Sakshya Adhiniyam, 2023 (Act No.47 of 2023), section 61.

https://www.indiancode.nic.in/handle/123456789/20063

Government of India. Bharatiya Sakshya Adhiniyam, 2023 (Act No.47 of 2023), section 62.

https://www.indiancode.nic.in/handle/123456789/20063

Government of India. Bharatiya Sakshya Adhiniyam, 2023 (Act No.47 of 2023), section 63.

https://www.indiancode.nic.in/handle/123456789/20063

Government of India. Bharatiya Sakshya Adhiniyam, 2023 (Act No.47 of 2023), section 63(4)

https://www.indiancode.nic.in/handle/123456789/20063

Government of India. Bharatiya Sakshya Adhiniyam, 2023 (Act No.47 of 2023), section 90

https://www.indiancode.nic.in/handle/123456789/20063