CRIMINAL LAW – PRACTICE AND PROCEDURE

f) Electronic Evidence

by

Sri Mude Anil Kumar Naik,
II Additional Civil Judge
(Junior Division), Proddatur

S.No.	Description
1.	**Introduction**
2.	**What is Digital Evidence**
3.	**Scope of Digital Evidence**
4.	**Need for Digital Evidence**
5.	**Types of Digital Evidence**
6.	**Admissibility of digital evidence in Indian Law**
6.1	Indian Evidence Act, 1872
6.2	Evidentiary value of the digital evidence with reference to Bharatiya Sakshya Adhinayam, 2023
6.3	Information Technology Act, 2000
6.4	Banker's Book Evidence Act, 1891
7.	**Role of digital evidence in Cyber Crime Investigation**
8.	**Significance of Digital Evidence in Protecting the Intellectual Property Rights (IPR)**
9.	**Importance of Digital Evidence in Forensic Investigation**
9.1	The major types of digital forensics
10.	**Judicial Pronouncements Surrounding Digital Evidence**
10.1	State (N.C.T of Delhi) vs. Navjot Sandhu (2005) 11 SCC 600
10.2	Sidhartha Vashisht @ Manu Sharma vs. The State (NCT of Delhi) (2010) 6 SCC 1
10.3	Unnikrishnan @ Unni vs. The State by Inspector of Police (2011)
10.4	Konnadan Abdul Gafoor vs. The State of Kerala (2015) SCC OnLine Ker 35800
10.5	Anver P.V vs. P.K Basheer & Ors AIR 2015 SC 180
10.6	Tomaso Bruno & Anr vs. State of U.P (2015) 7 SCC 178
10.7	Shafhi Mahommad vs. The State of Himachal Pradesh (2018) 2 SCC 801
10.8	Arjun Panditrao Khotkar vs. Kailash Kishanrao (2020) 3 SCC 216
10.9	Overruling of Judicial Decisions
11.	**Benefits of Digital Evidence in Legal Proceedings**
12.	**Challenges in Handling Digital Evidence in India**
12.1	Legal Framework

1. Introduction

In the Indian Justice system, evidence holds a pivotal role in order to establish the claim and defence of both the parties involved in a case. Evidence can be in many forms, but its admissibility depends on the court's discretionary powers by following established rules and laws. As technology is growing consistently, digital evidence also known as electronic evidence is considered relevant evidence in the Indian Court of Justice. Digital evidence can be in many forms including computers, smartphones, pen drives, and other digital media. Its admissibility depends upon the circumstances of each case.

2. What is digital evidence

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

3. Scope of digital evidence

Nowadays, the scope of digital evidence is widening because of continued growth in the digital world. Digital evidence plays a major role in different areas that include legal proceedings, Cyber security, corporate investigation, e-discovery, intellectual property theft, forensic analysis, and many other areas. Digital

evidence is in many forms including electronic communications, digital documents, multimedia files, internet browsing history, computer data, network data, mobile device data, digital signatures, certificates, and many others.

4. Need for digital evidence

In India, digital evidence plays a significant role in establishing the claims of each party before the court of law. Some of the major reasons for the need for digital evidence are as follows:

- Digital evidence serves as a detailed and authentic record of electronic records such as emails, text messages, and social media interactions, and helps to present the comprehensive facts in an easier manner.
- In criminal and civil cases, digital evidence assists legal professionals and law enforcement agencies such as the judiciary to investigate and reconstruct events. Digital evidence assists in identifying people, tracing financial transactions and discovering connections between people and entities.
- Well-established digital evidence is more trustworthy and reliable. Electronic records are maintained safely by putting passwords and security. It is hard to change or mess up as compared to traditional paper documents.
- Digital evidence helps to establish intellectual property theft, copyright infringement, or violation of digital rights by providing a clear record of data through different digitized methods. It helps to establish ownership and provides proof of unauthorized use or distribution of digital assets.
- Digital evidence plays a crucial role in establishing facts in concern with the Cyber crimes, which have been occurring more recently. In order to combat Cyber crimes like Cyber harassment, online bullying, online fraud and other related offences, digital proof is essential to establish real facts.
- The role of digital records in electronic contracts and transactions is pivotal. Due to growth in the digital world, almost every business prefers to engage in electronic contracts and many electronic transactions. In such situations, a digital proof is required to establish the reliability of these documents. This includes emails, digital contracts, and records of transactions.
- When there are issues with keeping information safe or if someone's private details get leaked, digital evidence plays a very important role in order to prove what actually happened.

- In matters that deal with national security, the role of digital evidence is phenomenal. Due to technological advancements, the government stores its important documents in the form of electronic records by establishing its official sites. If any security issues arise then it assists in enhancing accessibility, efficiency and facilitates the secure management of sensitive information. Digital evidence helps to determine Cyber criminals by finding out where attracts come from and giving proof to court. It also helps to stop future attacks by finding weaknesses in a system and fixing them. For instance, if there's a pattern that shows a possible threat, digital evidence can help to take action before an attack happens. Thus, it protects the national interest.

5. Types of digital evidence

Digital evidence is the information or data which is in the electronic forms. The widespread use of technology in different aspects of life has led to an increase in the different forms of digital evidence. Here are some of the types of digital evidence:

- Communications through text messages, emails, instant messaging, and other electronic messaging platforms can be used as digital evidence.
- Social media posts, comments, messages, and other content from any other social media platforms like Facebook, Twitter, Instagram, etc., can be used as valuable digital evidence.
- Digital documents, spreadsheets, presentations, and other file types are also forms of digital evidence. Metadata within these files may also provide important information.
- Digital photos and videos can be powerful evidence. Metadata, such as timestamps, and Geo location data, can be crucial in order to establish authenticity and context of media files.
- Logs that record computer and internet activities, including browsing history, file access and system logs, can be analyzed as digital evidence.
- Mobile devices and some digital cameras record GPS and location data, and are also considered as digital evidence.
- Records of phone calls, including call logs, durations and time stamps, can be treated as digital evidence.
- Digital records of financial transactions are considered digital evidence. That includes bank statements, online purchases and electronic fund transfers, which can be important in financial investigations.

- Fingerprints, facial recognition data, and recording of unique voice characteristics may be used as digital evidence.
- Information related to network traffic, IP addresses, and connection logs can be important for Cyber security and digital forensics.
- Information that is related to software usage, application logs and system configurations can be treated as digital evidence.
- Data which is stored in cloud services such as Google Drive, Dropbox, or One drive, can be used as evidence.
- Metadata associated with digital files, such as creation data, modification history, and user information is also considered digital evidence that is used for forensic purposes.
- Cryptocurrencies, and blockchain transactions, can also serve as digital evidence.

6. Admissibility of digital evidence in Indian Law

In India, the admissibility of digital evidence depends on the different laws, and court rulings. The Indian legal system has given legal recognition to digital evidence and such recognition of digital evidence is covered under different laws that include the following:

6.1. Indian Evidence Act, 1872

The Indian Evidence Act, 1872 is one of the foundational legislation that continues to be highly relevant in the Indian legal system. Under this legislation, certain provisions direct how evidence is treated in the court. Initially, the Indian Evidence Act didn't bear direct provisions for the admissibility of digital evidence. Later in the year 2000, an amendment was made to the Indian Evidence Act, accordingly, Section 65B of the Indian Evidence Act, has given legal recognition to digital evidence. Section 65B specifically addresses the admissibility of the electronic records before the court. As per the section, the electronic records include emails, or digital documents or other documents acceptable as evidence in Court. Those documents can be used as evidence in court without having to show the original digital file, subject to some conditions mentioned in the section that needs to be followed. This allows easier use of electronic information as evidence. Section 65B(2) of the Act prescribes the rules that need to be satisfied for the information stored in the computer to be considered valid in legal proceedings:

- The information in the electronic record must be produced by the computer during the regular use of that computer for storing or processing information related to ongoing activities.
- During this regular use, the kind of information in the electronic record was regularly input into the computer as part of the usual activities.
- The computer must have been working correctly during the relevant time, and any issues with its operation should not affect the accuracy of the electronic record.
- The information in the electronic record must match the information that is initially fed into the computer during regular activities.

As per Section 65B(4) of the Act, in order to present a statement from the electronic record in court, a certificate can be used. The certificate should be signed by a responsible official who can confirm how the electronic record was produced, provide details about the devices involved, and address the conditions mentioned earlier. In the case of Anver P.V v/s P.K Basheer, the Honourable Supreme Court decided that a certificate under Section 65B(4) of the Indian Evidence Act is essential for admitting electronic evidence. The court emphasized that this certificate ensures the source and authenticity of the electronic record. However, in the case of Shafhi Mohammad vs State of Himachal Pradesh, the Supreme Court provided a different decision. They said that the certificate requirement under Section 65B(4) of the Indian Evidence Act is not always mandatory. According to this case, the certificate is only needed when the person presenting the evidence has control over such a device, not when it's the other party.

6.2. Evidentiary value of the digital evidence with reference to Bharatiya Sakshya Adhinayam, 2023

The Indian Parliament on August 11, 2023, introduced the Bharatiya Sakshya Adhiniyam that replaced the Indian Evidence Act, 1872. The President of India gave their approval on December 5, 2023. The Act has changed many provisions of the Indian Evidence Act and some of the provisions remain the same. For the admissibility of electronic records or digital evidence, the Act has many provisions. The Act has validated the evidentiary value of the digital evidence. Some of the major changes with regard to electronic records are as follows:

- Section 2(e) of the Act has provided the legal frameworks for the admissibility of digital evidence. Accordingly, this Section states that evidence includes two forms of evidence. That includes oral evidence and documentary evidence. Oral evidence involves the statements or information provided electronically, by the witnesses in the court, that contribute to the investigation of facts. Such statements are acceptable and it is termed as oral evidence. On the other hand, documentary evidence includes documents that are extended to cover electronic or digital records that are presented to court for the examination. The Section thereby covers the electronic evidence orally as well as through documents.
- Section 32 of the Act consists of electronic records in reference to the laws of the other country. Whenever a court needs to understand the laws of another country, any statement about such laws is found in a book claiming to be published under the authority of that country's government, including electronic or digital form which is considered as relevant.
- The Act has expanded the evidentiary value of electronic or digital evidence, by considering digital evidence as primary evidence. As per the Section 57 of the Act primary evidence refers to actual documents presented for the court's examination. Section 65B of the Indian Evidence Act 1872, digital evidence was considered secondary evidence. Section 63 of the Indian Evidence Act stated the meaning of the Secondary evidence. However, the Act has provided more importance to digital evidence in the legal proceedings by considering the digital evidence as primary evidence. Section 57 of the Act prescribes the provisions for digital evidence as primary evidence. The Section in its explanation part 4 says that, when an electronic or digital record is created or stored, and this storage happens at the same time or one after another in multiple files, each of these files is considered primary evidence. Explanation 5 states that if an electronic or digital record is produced from proper custody and is not disputed, it is also considered as primary evidence. Explanation 6 states that video is simultaneously stored in electronic form and transmitted, broadcast or transferred elsewhere, each of these stored recordings is considered primary evidence. Explanation 7 further extends the concept to situations where an electronic or digital record is stored in various locations within a computer resource, including temporary files. In such cases, each automated storage space is considered primary evidence.

6.3. Information Technology Act, 2000

The Information Technology Act was enacted by the Indian Parliament on June 9, 2000. The main purpose of the Act is to give legal recognition to electronic records and digital signatures which is enumerated under Section 4 and Section 5 of the Act. Digital signatures and electronic records are the forms of digital evidence. Some of major provisions in this Act that relates to electronic evidence are:

- Section 4 of the Act states that if any law specifies that information or any other thing must be in written, typewritten or printed form, this requirement is still satisfied if the information is presented in electronic form. Additionally, it should be easily accessible and usable for future reference.
- Section 5 of the Act states the legal recognition of electronic signatures. If any law mandates that information or any other thing requires authentication through a physical signature, a document must bear the signature of a person. This provision overrides such requirements. It asserts that legal criteria for authentication are fulfilled if the information is authenticated through an electronic signature. The explanation part of section 5 states that if a law requires a person's signature on a document, the term 'signed' means putting a handwritten signature or any mark on it. It also means that the term signature is understood in the same way. The provisions make it clear that electronic signatures are considered just as valid as traditional handwritten. However, electronic signatures are valid as long as they follow the specific electronic signature standards set by the central government.
- Section 79A of the Act which was amended in 2008 states that, it is necessary for the central government to appoint an examiner of electronic evidence. That person's role is to give their expert suggestions on electronic evidence in court or other authorities.

6.4. Banker's Book Evidence Act, 1891

The Banker's Book Evidence Act came into existence in 1891. It was amended in the year 2000. This amendment introduced specific changes that relate to the admissibility of digital records. Subsequently, the Information Technology Act was enacted, and it served as an update to the Banker's Book Evidence Act. The amendment has made significant changes in the banking evidence. Accordingly, Section 2 of the Act states that evidence that is taken

from the banker's book as defined under this section is reliable evidence before the legal proceedings. In addition to this, Section 2A speaks about the use of printouts of electronic data that are also considered as evidence before the court. Thereby, amendment was made to this Act that provides legal frameworks for the admissibility of digital evidence in conjunction with banking evidence.

7. Role of digital evidence in Cyber crime investigation

Cyber crimes are one of the serious issues in India. As technology is growing, some people are misusing it for fraudulent purposes. As per the report of the National Crime Record Bureau (NCRB), As of 2024, India continues to experience a high volume of pending Cyber crime cases, with significant numbers reported in states like Karnataka, Uttar Pradesh, Maharashtra, and Delhi. In recent years, Karnataka has emerged as a hotchpot, registering over 16% of all Cyber crimes in the nation. Delhi, as a union territory, also faces considerable case backlogs, with fraud and identity theft being some of the most common Cyber offences. The majority of the cases fall under computer related offences as per Section 66 of the Information Technology Act. There is a greater importance for the digital evidence to substantiate the facts and to prove these cases. Digital evidence is often linked to electronic crimes like identity theft, Cyber stalking, and credit card fraud. Digital evidence is important in finding Cyber crimes and proving them in court. The use of digital devices assists in uncovering the evidence related to proof of Cyber crimes, data leaks, hacking, and other digital problems.

8. Significance of Digital Evidence in Protecting the Intellectual Property Rights (IPR)

Intellectual property is gaining prominence in India as a lucrative source of income. In order to prove the ownership of intellectual property, strong evidence is very essential. The infringement may have occurred due to copying, distributing and modifying digital content without the permission of the authorized person. In these situations, the digital evidence helps to execute the facts that validate the originality of a work. It will help to mitigate the unauthorized copying or distribution of such property. Intellectual property is the product of intellect. Property includes literary, artistic, and scientific works, discoveries, performances, phonograms, broadcasts, industrial design, trademarks, service marks, commercial names and designations.

Property rights are confirmed on the basis of the uniqueness of ideas and creation of the mind. It is essential to prospect the rights of the original owner. Digital copies like journals, publications and books are readily available online. In case of infringement of such assets by electronic means, it is very essential to protect such rights through the use of digital evidence. Digital evidence helps to safeguard intellectual property rights in case of infringement of such rights. In this regard metadata, digital fingerprints, digital certificates and watermarks play a very important role that includes:

- Metadata will be used to describe other data by encompassing information like creation, date author and software used for a file. Digital fingerprints also serve a major role. It identifies the integrity of a file. Along with it, identical hash values indicate identical files.
- Digital certificates are used to verify the identity of a person or any organization. This will help to prove the specific work that is created by that individual or entity.

The watermarks are considered digital marks which are embedded in a file to show ownership of a work. They are commonly applied to various digital media such as images, videos or documents. The primary purpose of watermarks is to identify and protect intellectual property by visibly and invisibly marking the content.

9. Importance of Digital Evidence in Forensic Investigation

In India, the role of digital evidence in forensic investigation is phenomenal. Forensic investigation commonly involves scientific methods of investigation. The forensic investigation includes taking physical evidence such as fingerprints, DNA, blood stains, or weapons, autopsy, post-mortem reports, and some other evidence. Along with this physical evidence, digital forensics methods also contribute a significant role in forensic investigations. This is particularly important in dealing with the cases where information is stored electronically. The information may be in any form that includes emails, files and history, all are accounted for as digital evidence while conducting forensic investigation. However, in India, digital forensic investigation is still developing.

In 2008, a terror attack occurred at Mumbai in India highlighted that the country was still figuring out how to handle and investigate digital crimes. The investigation into the attack was criticized for missing important digital information from the US that warned about the possible terror attack. After this attack, investigators found that digital evidence played a big role in planning and carrying

out these terror attacks. In this regard, the Indian government created a report which pointed out that digital devices are very important. The report also highlighted the importance of information satellite phone, Direct Inward Dialing (DID) facilities, GPS equipment and the tracking of emails/IP addresses.

In the Mumbai train bombings of 2006, terrorists used advanced technology. They used things like masking their IP addresses and using proxy services to hide their communications. After these incidents, India became more conscious of the importance of digital evidence in forensic investigation and many concerns are raised on this behalf. They suggested that there is a need to improve Cyber forensics and Cyber security professionals to protect India's information technology from potential harm.

In Bharat Jatav vs State of Madhya Pradesh (2021) in this case, the Honourable High Court while hearing the matter with regards to grant of bail under Section 439 of the Criminal procedure Code emphasized the importance of technology in forensic science and held that the scope of forensic science extends beyond the DNA reports and blood samples.

9.1. The major types of digital forensics are as follows:

1. **Database Forensics** - which helps in checking databases for information
2. **Network Forensics** - used for the understanding of data flow in networks to prevent issues and find out what happened
3. **Mobile Forensics**- this will help to get information from phones or tablets to solve cases
4. **Malware Forensics** - which is used for harmful computer viruses to know who made them and what it will cause
5. **Email Forensics -** using emails to check out its source from whom it is sent and confirming the date and contents of the mail
6. **Memory Forensics** - used for checking hidden memories or information from the computers

10. Judicial Pronouncements Surrounding Digital Evidence

10.1. State (N.C.T of Delhi) vs. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600

This case is also known as the Parliament attack case. In this case, the Supreme Court decided on a very significant aspect of the admissibility of the electronic records as evidence in court. This case revolved around the 2001 terrorist attack on the Indian Parliament. Navjot Sandhu, former President of Punjab Pradesh Congress Politician, was accused of being involved in the

conspiracy. The issue arose when the prosecution wanted to present call records as evidence. However, the defence objected on the ground that the records didn't have the required certificate as per Section 65B(4) of the Indian Evidence Act. The Honourable Supreme Court of India had made an important ruling in this case. It was held that the electronic records could be accepted as evidence even without a specific certificate mentioned in Section 65B(4) of the Indian Evidence Act. The court further states the admissibility of electronic record as evidence depends on the details of each case. Facts like the reliability of evidence, where it came from and how it was presented had to be considered. After this case, the rules about admitting electronic records become more flexible. Parties could be allowed to either bring an original record to court and prove it as primary evidence. They could use a copy of the original record accompanied by a certificate under Section 65B(4) of the Evidence Act. However, this decision was overruled by the Supreme Court in the later case of Anver P.V. in 2015.

10.2. Manu Sharma vs. The State (NCT of Delhi) (2010) 6 SCC 1

The case is known as the Jessica Lal murder case. The Hon'ble court had the opportunity of delving into the intricacies of digital evidence while deciding this case. In 1999, Jessica Lal, a model, was shot dead at a party. The case gained nationwide attention due to the accused's influential background and the perceived lack of justice for the victim. One of the pivotal aspects of the case was the court has given recognition to the electronic evidence during the trial. The court acknowledged the admissibility of electronic evidence, including call records and CDs. It had played an important role in establishing the involvement of the accused in the crime. The court had given prominence in adopting technological advancement and incorporated such evidence in criminal proceedings. Meanwhile, the media played a major role in bringing the case into the national spotlight. Finally, in 2010 Honourable Supreme Court of India upheld the conviction of the accused and sentenced them to life imprisonment. This case is considered as one of the prominent cases that allowed the admissibility of digital evidence and upheld the rule of law by ensuring justice without considering the standing of the accused.

10.3. Unnikrishnan @ Unni vs. The State by Inspector of Police (2011)

In this case, contentions were raised before the Madras High Court. The issue revolved around the admissibility of digital photographs as evidence in a criminal trial. The trial court initially considered the digital photographs inadmissible as evidence. The reason was that the negatives of the photo (this is created during the process of exposing photographic film to light, and it serves as an inverted version of the original scene) were not presented during the trial. However, the High Court took a different stance.

The court emphasized that in the past, when photographs were captured using cameras with photo films, the negatives were considered primary evidence. Without the production of negatives, the photographs were treated as inadmissible secondary evidence. The High Court highlighted that advancement in technology and inception of modern digital cameras, reliance on traditional photo films reduced. In the case of digital cameras, the photograph itself, or its printout, is considered the primary evidence. The court further held that the requirement of producing negative, as applicable to older cameras. It doesn't need to apply in the digital age. However, an important point was raised regarding the admissibility of digital photographs. The Madras High Court had given recognition to the digital photograph as relevant evidence. It interpreted that the digital photograph must meet the conditions that are specified in section 65B of the Indian evidence act. Section 65B(2) of the act states the requirements for the admissibility of electronic evidence. Section 65B(4) includes the need for a certificate confirming its authenticity and integrity. Thus, the court asserted that in cases involving digital photography, the photograph itself is primary evidence. There is no necessity of submitting negatives for its admissibility in legal proceedings.

10.4. Konnadan Abdul Gafoor vs. The State of Kerala (2015) SCC OnLine Ker 35800

In this case, the issue was raised regarding the admissibility of electronic evidence. The petitioner, Konnadan Abdul Gafoor, was the fourth accused in multiple crimes including illegal and fraudulent activities. The accused individuals were allegedly engaged in activities that cheated telecoms service providers, and tampered with the telecommunication network. Further, it was alleged that he caused substantial monetary losses to the government and service providers and installed parallel telephone exchanges in Kozhikode. The mode of operation included the use of multiple broadband connections,

illegal call routing Gateway devices, and the insertion of pre-activated SIM cards without the owner's knowledge and consent.

- The issue in this case was whether the electronic device met the requirements of Section 65B of the Indian Evidence Act or not.
- Secondly, whether such evidence is required to be accompanied by the necessary certificate under Section 65B(4) of the Act in order to confirm its authenticity.

The High Court of Kerala ruled that electronic evidence in the form of probative information is stored in digital form in a Court. However, the court has recognized the delicate and easily manipulable nature of digital evidence. Digital evidence such as electronic files or data which can be easily altered, damaged or destroyed. Hence, there must be special care needed to protect such information. To address these concerns for the admissibility of such evidence in court, the court had ruled that electronic evidence must meet certain specific requirements, which are outlined in Section 65B of the Indian Evidence Act. The court upheld the significance of digital evidence in this case. However, it interpreted that such evidence needs to fulfill the condition specified under Section 65B of the Act.

10.5. Anver P.V vs. P.K Basheer & Ors AIR 2015 SC 180

The Honourable Supreme Court in this decision had ruled regarding the evidentiary admissibility of the electronic record. The appellant contested in an election as an independent candidate with alleged support from the Left Democratic Front. The respondent emerged as the victor in the 034 Eranad Legislative Assembly Constituency. The issue was related to an election dispute where the appellant alleged corrupt practices during the election campaign. The main issue involved in this case was about the admissibility of the electronic evidence. The evidence specifically included CDs and the publication of a leaflet. It allegedly contained false statements to influence the election outcome. The appellant failed to give a certificate for certain CDs which is required under Section 65B(4) of the Act. It led to questions about the admissibility of the electronic records as secondary evidence. Additionally, the case represented the claims related to the publication of the contentious leaflet (Exhibit- P1). Such claims constituted a corrupt practice under Section 123(4) of the Representation of the People Act (1951).

The court in its judgment ruled that the electronic record in question was inadmissible as evidence. The evidence had not met the requirements of Section 65B of the Indian Evidence Act. The court clarified that the Section exclusively governs the admissibility of electronic records as secondary evidence. Specifically, the court has highlighted that a person is required to declare in the certificate that the information in CDs, VCDs and chips is to the best of their knowledge and belief. This decision underscores the mandatory nature of Section 65B for admitting electronic evidence as secondary evidence in legal proceedings. The court also held that without submitting the certificate as mentioned under section 65B of the Act, CDs are not admissible as relevant evidence. The decision of the court declared that strict adherence to the conditions outlined in Section 65B is important for the admissibility of electronic records. This decision provided clarity for the admissibility of electronic evidence in legal proceedings. It is considered one of the landmark cases in the admissibility of digital evidence.

10.6. Tomaso Bruno & Anr vs. State of U.P (2015) 7 SCC 178

In this case, the Honourable Supreme Court declared that Section 65B of the Indian Evidence Act was not a complete code, but it didn't refer to the earlier decision held in Anvar vs Basheer case, which is considered a precedent for upcoming cases. In this case, previous judgment appellants were convicted for the alleged murder of Francesco Montis an Italian tourist who resided in Varanasi. The prosecution claimed that the appellants were responsible for his death.

Meanwhile, the court said that the evidence like security camera footage and electronic proof were not properly shown during the trial. The judges pointed out that the investigation had big mistakes, and the trial court didn't take them seriously. The decision stressed the importance of having strong evidence in criminal trials. Because necessary proof was missing or not good enough, hence the court acquitted the accused. The court further held that though there is legal recognition of electronic evidence in the Indian Evidence Act, such evidence can be proved beyond a reasonable doubt. The court held that the law prefers to give the benefit of the doubt to the accused when evidence is not clear. However, the judgment is not made clear as to the consideration of the digital evidence.

10.7. Shafhi Mahommad vs. The State of Himachal Pradesh (2018) 2 SCC 801

In this case, the Honourable Supreme Court of India addressed the issue of the admissibility of electronic evidence. Issue specifically addressed that the party presenting the evidence is not in possession of the device that generated the electronic document. The court discussed the applicability of Section 65B(4) of the Evidence Act. The Section requires a certificate for the admissibility of electronic evidence. The court held that the requirement of such a certificate is not compulsory when electronic evidence is produced by a party who is not in possession of the device. The court had replaced the procedural requirement of the certificate under Section 65B(4) of the Indian Evidence Act instead allowing electronic evidence without the certificate.

10.8. Arjun Panditrao Khotkar vs. Kailash Kishanrao (2020) 3 SCC 216

In this case, the Honourable Supreme Court of India dealt with the main issue that revolved around the admissibility of electronic records as secondary evidence in court proceedings. Arjun Pnaditrao Khotkar challenged the election of Kailash Kushanro Gorantyal under Section 80 and Section 81 of the Representation of the People Act 1951. The court has interpreted the Section 65B(4) of the Indian Evidence Act, of 1872. The court further held that a certificate is compulsory for the admissibility of electronic records in court. The purpose of this compulsory requirement is to ensure the source and genuineness of electronic records. Because these evidences are more susceptible to tampering or any modifications.

The court further clarified that the person providing the certificate, such person, needs to state that it is to the best of their knowledge and belief. This certificate must accompany electronic records. That includes computer printouts, CDs, VCDs, pen drives, and some other records when presented as evidence. These safeguards aim to maintain the integrity of electronic records. It prevents potential injustices in trials based on such evidence. The judgment highlighted that if the original document itself is produced, then the certificate Section 65B(4) is not necessary. The owner of a device such as a laptop, tablet, or mobile phone, can enter the witness box to prove ownership and operation of the device where the original information is stored. However, if the computer is part of a larger system network, it's not possible to physically bring it to court. In such circumstances, Section 65(B) and requirements of obtaining the certification under Section 65B(4) become essential. It is

required to prove information contained in electronic records. Further courts specifically addressed the Anvar P.V. case and upheld the judgment in this case. The court interpreted that electronic records used as primary evidence do not necessarily adhere to Section 62 of the Evidence Act. This is because Section 65B is considered the complete code for dealing with electronic records.

10.9. Overruling of Judicial Decisions

The Honourable Supreme Court of India overruled the decisions of the Tomaso Bruno case and the Shafhi Mohammad case while deciding the Arjun Panditrao Khotkar vs the Kailash Kishanrao case. The court stated that Tomaso Bruno's case stated that Section 65B was not a complete code. Thereby, the court ignored the earlier decision in the Anver vs Basheer case. The court in the Arjun Panditrao Khotkar vs Kailash case held that Section 65B is a complete code for electronic records. Justice Nariman criticized Shafi Mohammad's case interpretation that Section 65B is merely procedural, and the certificate requirement can be waived when the electronic device is inaccessible. The court further emphasized that difficulties in obtaining the certificate are not a valid reason for admitting the electronic evidence. Further the court has considered the legal provisions such as Section 165 of the Evidence Act, Order XVI of Civil Procedure Code, Sections 91, and 349 of the Criminal Procedure Code 1973 which allow the court to order the production of any document, including electronic evidence too. Thus, if unable to obtain the certificate a person can request the court's order for document production. Similarly, the court ruled that section 65B(4) is mandatory, not optional. It is a prerequisite before admitting secondary copies of electronic records. It clarified that electronic evidence must be present before the trial begins, and the court can order the certificate's production at any stage before trial completion.

11. Benefits of Digital Evidence in Legal Proceedings

The digital evidence plays an important role in establishing the facts in legal proceedings. Earlier it was stuck to physical evidence. As a result of rapidly growing technology, various transactions are carried out in digital mode. Digital evidence has many benefits, some of the important merits are as follows:

- Digital evidence can be sourced from a variety of formats and devices. Devices like laptops, mobiles, hard disks, software and documents like PDF,

JPG, image, and audio formats like mp3, mp4, and many others. These formats and devices can easily be carried in legal proceedings. Thus, it will help to widen the scope of investigations.

- Digital evidence is stored or transmitted in binary form. The binary form refers to it as a way of representing data using only 0s and 1s. In computing, it's the fundamental language of electronic devices. Each digit is called a "bit". This system forms the basis for encoding and processing information inclined every text, image, audio, and video. Digital evidence is the binary nature of data that allows the accurate, reliable representation. This will add more value to the evidence before the court.
- Digital Evidence can be more secure as it prescribes certain passwords and security reluctantly, there is less chance of violating private information with strong passwords.
- The Digital data can be easily found, organized and shown in court. This evidence is like information on computers or phones and is helpful in court because it is easily found in different documents, easily copy- pasted and executed in legal proceedings. The digital files not only contain the main information but also keep the record of when it was created, modified and viewed. The digital evidence often comes with metadata. Metadata helps to prove that digital evidence is more organized and more truthful evidence in legal proceedings. In cases where in legal proceedings any money matters are involved, digital evidence is very important. It serves as a document, showing how money moves around. This proof is helpful in situations of fraud, or any financial wrongdoing.
- Digital technologies such as encryption, digital signatures, blockchain technology timestamps and logging technology help to maintain the originality and authenticity of the data. Thus, it will be considered as more reliable in court.
- Digital technology will provide real-time information. This will help lawyers and other legal experts to have access to the most recent and relevant information when dealing with ongoing cases in the court.
- Instead of dealing with lots of paperwork, storing physical documents, and handling everything manually, digital evidence allows, to do things more efficiently. This means with less printing, less physical storage space and less manual work. It makes the whole legal process more cost-effective.

- The digital clues like metadata, timestamps, and other digital footprints help the experts to investigate more accurately. It provides structured information to get a better and complete picture of the case. This helps to understand the sequence of events and gather more information related to the case.
- Extra details contained in the digital evidence help to verify facts. This might include information like geological data, device identification and user authentication details. These additional details make the evidence more reliable.

12. Challenges in handling digital evidence in India

Though there are immense benefits of using digital evidence, there are many challenges associated in handling digital evidence in India. In India, digital evidence got prominence after the amendment made in the year 2000 to the Indian Evidence Act 1872. But, even today there are numerous complexities in managing electronic evidence. The major challenges are as follows:

12.1. Legal framework

Initially, digital evidence did not bear any legal recognition before the court. However, amendment of the Indian Evidence Act in 2000 has given legal recognition to the digital evidence as admissible before the court. However, this Act does not consider electronic evidence as primary evidence, though it is admissible as evidence before the Court. The digital evidence is considered as the secondary evidence as per the Indian Evidence Act 1872. The major issue is as a secondary evidence it may affect its credibility in court. Primary evidence is considered as more reliable and has more evidentiary value compared to secondary evidence. The classification of digital evidence as secondary evidence could impact on the outcome of cases. Moreover, treating digital evidence as secondary evidence will place an extra burden on the person to establish their claims. In the legal concept, the burden of proof is something which dictates that the party making a claim must provide relevant and sufficient evidence in order to support their claim. While electronic evidence is admissible before the court as per the Evidence Act it needs to be provided with authenticated certificate to make that evidence admissible before the court. Thus, parties need to overcome additional hurdles for establishing the authenticity of the digital records. In order to combat these issues later some changes were made in the new Act

called Bharatiya Sakshya Adhiniyam 2023. The Act has treated digital evidence as the primary evidence.

- The Act is lacking in sufficient safeguards to prevent tampering or contamination of electronic records during investigations. This will raise questions about the integrity of digital evidence in legal proceedings. The Act requires the need for an expert's certificate to authenticate specific electronic evidence. While this certification is indeed to ensure the accuracy of digital evidence, it may pose a challenge in terms of the ease of producing such evidence in court.
- Further, electronic evidence is bifurcated as both primary and secondary evidence. This will often create confusion in court proceedings. This confusion could affect while interpreting the digital evidence. This may impact the outcome of the cases.

12.2. Data protection and privacy

Digital evidence can have both positive and negative impacts. Digital evidence is very important for the investigation of Cyber crimes. However, it can also cause threats to people's privacy rights. Such rights are protected under Article 21 of the Constitution that states that every individual has the right to life and liberty. The same contention was upheld in Justice K.S Puttaswamy vs Union of India case.

For instance, digital evidence is like a detective tool that will be used in order to catch online criminals. It has the capacity to track and analyze activities on the internet. However, this can be misused to the rights of the individual. Because tracking their online movement without their permission is a clear way of violation of privacy. Furthermore, digital evidence can go beyond just identifying criminal activities. It has the power to reveal personal information about individuals. During the investigation if these information are not handled properly this may lead to potential harm to one's own privacy. In order to balance these concerns, it is essential to use digital evidence in an ethical manner. The methods used to collect digital evidence must respect the individual privacy rights. There are so many methods to protect the privacy of the person. Using effective methods like encryption, that act like a secret code to secure data and makes it difficult for unauthorized individuals to access it. There are privacy enhancing technologies such as virtual private networks, block chain technology, and encrypted messaging apps that will inform individuals to control what

personal information is collected about them. The implementation of these tools will safeguard the privacy rights and investigation can be carried in an ethical border.

12.3. Search, Seizure and Search Authority

The court will admit the digital evidence if the methods used to obtain digital evidence are in line with legal procedures. The challenge arises when digital evidence is obtained without proper authority. If the evidence is obtained without a valid search warrant is also one of the challenges. In such cases, where the procedural requirements stated in the Code of Criminal Procedure or BNSS are not met, the defence has the right to challenge the admissibility of such evidence. If there is a failure to follow the correct protocols like maintaining a properly documented record of evidence handling, it can lead to challenges regarding the reliability of the evidence.

For instance, law enforcement searches a suspect's computer, without following specific guidelines in the CrPC or BNSS or not getting a valid search warrant. It raises a big question about the legality of the search. The defence can take the point that any digital evidence obtained by the unauthorized search, will not be allowed as evidence before the court. The court will closely determine the legitimacy of the search process in order to maintain a fair investigation.

12.4. Ethical issues

An ethical issue is like a problem where people have to decide what's right or wrong based on what they believe is good or fair. It's a situation where people may have different perspectives on what actions should be taken because ethical issues involve values and morals. The digital evidence must be in accordance with the ethical concerns. The evidence collected is affecting the privacy and the rights of the person, it may lead to ethical issues. In ethical issues, primary consideration is the respect for individuals privacy rights. This must be maintained through the collection and utilization of digital evidence. Digital evidence can cause unfair treatment if it is not handled fairly. If only some information is looked at, or if people's ideas or unfair attitudes affect how the evidence is understood. It can lead to treating individuals in legal cases unfairly. The important ethical rule here is that digital evidence should be looked at in a fair way to make sure everyone is treated equally.

For instance, in some workplaces, employers may use digital surveillance tools like computer monitoring software or CCTV cameras to monitor employees' activities. While the intention is to ensure productivity and security, ethical concerns arise when this surveillance extends beyond professional activities to invade employees' privacy. Likewise, if an employer installs monitoring software on company computers without informing employees and tracks their personal online activities. Such as private emails, and social media use during breaks, it can be seen as an ethical issue. This collection of digital evidence may raise concern about the right to privacy in the work place.

12.5. Forensic Challenges

Digital evidence often undergoes forensic examination in order to determine its authenticity. However, challenges can arise due to the rapidly growing technology. Outdated forensic tools present a challenge during the examination, potentially impacting the court's confidence in the accuracy of digital evidence. Digital forensics experts must stay updated to address these challenges and ensure that forensic procedures align with legal standards for the admissibility of evidence. The digital forensic challenges fall into three main categories that includes:

Technical Challenges - means issues like anti-forensic techniques, cloud operations, skill gaps and stenography.

Legal Challenges - involve presenting digital evidence, lack of proper guidelines, and inadequate electronic evidence collection and acquisition.

Resource Challenges - include the power required for collecting digital evidence and analyzing a running computer.

In order to maintain the integrity and admissibility of digital evidence in legal proceedings, there is a need to overcome these challenges.

12.6. Cross Border Issues

In the interconnected world, the movement of digital evidence between countries is continuously increasing. It will lead to a lot of issues related to legal jurisdiction, international agreements, and recognition of foreign digital evidence in legal proceedings. When it is used as evidence in Indian courts, things can get more complicated. It will raise questions about who has authority and how such evidence can be accepted.

For instance, if evidence comes from a server outside India, it raises questions about whether Indian courts have the authority over that data. These situations can get tricky because different countries have different rules about how evidence can be shared and used. The legal issues are not always straightforward, as they expand on the unique details of each case.

12.7. Technological Advancement

The evolving technology has posed many challenges for defining and controlling digital technologies like artificial intelligence, blockchain, and other internet things. Because of this progress, courts have to get used to dealing with proof or information that comes from these very advanced technologies. It's like they need to learn and understand these new technologies to make fair decisions when such evidence is involved in legal cases. For instance, the court faces issues while getting to accept evidence as created by an artificial intelligence system. Because difficulty may arise because those artificial intelligence generated evidence are more often seen as black boxes. That means it implies lack of transparency and accuracy in how the system processes information and arrives at its conclusions. This complicates determining whether such evidence is preceded by such systems as reliable or not.

13. Conclusion

Digital evidence is very important in today's investigation. Due to the rapid growth in technology, the scope of digital evidence is increasing. The Indian judiciary has given legal recognition to digital evidence by adopting digital evidence in many cases. Digital evidence or electronic evidence is used in various cases. In cases like Cyber crime or fraud digital evidence is more reliable than traditional evidence. After knowing the importance of digital evidence Parliament made necessary enactment with regard to digital evidence admissibility in Bharatiya Sakshya Adhinyam 2023. The Act considered digital evidence as primary evidence. On the other hand, digital evidence has its own set of challenges. It is important to keep this evidence safe and unchanged by including strong passwords and some digital security measures. Digital evidence faces some challenges like software privacy, Cyber hacking, Cyber fraud, and Cyber theft. To address these challenges legal systems need to continually update legislation. The Government had to provide clear guidelines for securing and creating awareness regarding this evidence. Digital evidence is getting legal recognition in different countries. When

use of technology increases, the information stored on digital devices also increases. This may lead to the misuse of technology often tends to be crimes. Everyone involved in the legal system, such as lawyers, and judges, need to understand how to handle and use this digital evidence properly. Working together is needed to make sure that this kind of evidence is used correctly, by meeting the ethics of law and justice is served properly.

*****