IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE SHIFTING PARADIGM OF CRIME AND INDISPENSABLE ROLE OF SCIENTIFIC DIGITAL EVIDENCE IN UNFOLDING SUCH CRIMES

Mansi Bajpai, LLM 1 year, Faculty of Juridical Sciences, Rama University, Kanpur

Mr. Rahul Singh, Assistant Professor, Faculty of Juridical Sciences, Rama University, Kanpur

ABSTRACT:

In the contemporary era, the proliferation of technology has not only revolutionized communication and commerce but has also paved the way for a new breed of criminal activity. This paper delves into the pivotal role played by digital evidence in addressing and untangling the complexities inherent in modern-day criminal activities. Drawing upon an amalgamation of scholarly insights, empirical investigations, and practical case illustrations, this study investigates the multifaceted facets of digital evidence and its indispensability in the investigation, prosecution, and resolution of diverse forms of crime. Ranging from cybercrimes such as hacking, identity theft, and online fraud to conventional offenses like homicide and financial malfeasance, digital evidence serves as a cornerstone in reconstructing the narrative of criminal occurrences. Furthermore, this paper scrutinizes the challenges and intricacies associated with the procurement, preservation, and analysis of digital evidence, encompassing concerns pertaining to privacy, veracity, and jurisdictional limitations. Additionally, it scrutinizes the evolving legal paradigms and technological innovations that influence the domain of digital forensics, emphasizing the necessity for adaptive methodologies and interdisciplinary cooperation to effectively counter emerging threats.

INTRODUCTION

In the contemporary digital era, the landscape of criminal activity has undergone a profound transformation, largely due to the widespread integration of technology into every aspect of daily life. This shift has given rise to a myriad of new criminal behaviours that exploit the vulnerabilities of digital infrastructure. From cybercrimes like hacking and online fraud to more traditional offenses facilitated by digital means such as

financial malfeasance and identity theft, criminal activity in the digital realm has become increasingly sophisticated and prevalent.

Central to understanding and combating this new wave of crime is the critical role played by digital evidence. Digital evidence encompasses a wide array of data extracted from electronic devices, networks, and online platforms, offering crucial insights into the methods, motives, and identities of perpetrators. In the realm of law enforcement and criminal justice, digital evidence serves as a cornerstone in the investigation, prosecution, and adjudication of criminal cases, providing investigators with a digital trail that can unravel the complex web of criminal activities.

However, effectively harnessing digital evidence presents significant challenges. From the technical complexities of data acquisition and analysis to the legal and ethical considerations surrounding privacy and data protection, navigating the landscape of digital forensics requires specialized expertise, resources, and collaboration across various disciplines. Furthermore, the rapid pace of technological advancement continually reshapes the digital landscape, introducing new forms of crime and rendering existing forensic methodologies obsolete.

This paper aims to explore the multifaceted role of digital evidence in addressing and unraveling the evolving nature of criminal activities in the digital age. By examining the significance of digital evidence across different types of crime, discussing the challenges and complexities associated with its collection and utilization, and highlighting emerging trends and advancements in digital forensics, this study seeks to provide a comprehensive understanding of the pivotal role digital evidence plays in contemporary law enforcement and criminal justice efforts. Through an analysis of scholarly research, empirical evidence, and practical insights, this paper aims to underscore the importance of leveraging digital evidence to confront the challenges posed by the ever-changing landscape of crime in the digital era.

MEANING, NATURE AND SCOPE OF DIGITAL EVIDENCE IN CRIMINAL CASES

The term ‘Electronic Evidence’ signifies a piece of evidence generated by some mechanical or electronic processes which is often relevant in proving or disproving a fact or fact at issue, the information that constitutes evidence before the court[1]. Electronic Evidence is commonly known as Digital evidence. Digital evidence in cybercrime cases refers to information transmitted, stored, or retrieved on digital devices and networks, represented in the binary language of ones and zeros.

Digital evidence refers to electronic data that holds legal significance and can be utilized in legal proceedings. It encompasses a wide array of electronic information, such as emails, documents, images, videos, social media content, computer files, and metadata. This evidence is crucial in verifying or disproving claims made by parties involved in legal matters and serves as supporting documentation.

[1] "Electronic Evidence and the Law" by Stephen Mason (2nd Edition, 2012)

The nature of digital evidence lies in its electronic form, making it susceptible to alteration or deletion if not properly preserved. Additionally, digital evidence often contains metadata, which provides valuable information about its creation, modification, and transmission. Its volatile nature means it can change or be lost if not promptly collected and preserved.

In terms of its scope, digital evidence is extensively utilized in criminal investigations, particularly in cybercrimes, fraud, hacking, identity theft, and cases involving child exploitation. It also plays a significant role in civil litigation, regulatory investigations, internal organizational inquiries, and electronic discovery processes.

To ensure the integrity of digital evidence, proper handling, preservation, and analysis are essential. Adhering to established protocols and employing digital forensic techniques help maintain the admissibility and reliability of digital evidence in legal proceedings.

TYPES OF DIGITAL EVIDENCE

Digital evidence encompasses a wide range of electronic data that can be collected and analyzed for its relevance in legal proceedings. Understanding the different types of digital evidence is essential for effective investigation and presentation in court. Some common types of digital evidence include:

1. **Emails and Electronic Communications**: Emails, instant messages, and other electronic communications are frequently used as evidence in legal cases. These communications can provide insights into conversations, agreements, and intentions of individuals involved in a case.
2. **Documents and Files**: Digital documents, such as Word files, PDFs, spreadsheets, and presentations, are often submitted as evidence. These documents may contain critical information related to contracts, agreements, financial records, and other relevant data.
3. **Social Media Content**: With the widespread use of social media platforms, content posted on sites like Facebook, Twitter, Instagram, and LinkedIn has become valuable digital evidence. Posts, comments, messages, photos, and videos shared on social media can offer insights into a person's activities, relationships, and behavior.
4. **Computer Forensic Evidence**: This category includes data retrieved from computers, laptops, tablets, smartphones, and other digital devices. Computer forensic evidence may consist of files, browsing history, deleted data, metadata, and system logs, which can provide valuable clues in investigations involving cybercrimes, hacking, intellectual property theft, and more.
5. **Internet and Network Data**: Evidence obtained from internet activities and network traffic analysis can be crucial in cybercrime investigations. This includes website visit logs, IP addresses, server logs, DNS records, and other network-related data that can help trace online activities and identify perpetrators.

6. **GPS and Location Data**: GPS data from mobile devices, vehicle navigation systems, and other location-tracking technologies can be used as evidence to establish a person's whereabouts at specific times. This type of evidence is commonly utilized in criminal investigations, personal injury cases, and disputes involving property rights.

7. **Digital Multimedia**: Photos, videos, audio recordings, and other multimedia files are frequently used as evidence in legal proceedings. Digital multimedia evidence can provide visual or auditory documentation of events, incidents, or behaviors relevant to a case.

8. **Metadata**: Metadata refers to hidden data embedded within digital files, providing information about their creation, modification, and distribution. Metadata can offer valuable context and authenticity to digital evidence, helping to establish its credibility and relevance in court.

Understanding the different types of digital evidence and their potential relevance to a case is essential for legal professionals involved in investigations, litigation, and dispute resolution processes. Proper collection, preservation, and analysis of digital evidence are critical to ensuring its admissibility and reliability in court.

COLLECTION OF DIGITAL EVIDENCE

The process of collecting digital evidence is not an easy task. Further, it is very crucial in ensuring its admissibility, integrity, and reliability in legal proceedings. It requires following essentials for its collection:

1. **Preparation and Planning**:
    - Identify the scope and objectives of the investigation.
    - Determine the types of digital evidence likely to be relevant to the case.
    - Obtain necessary legal permissions and warrants for accessing and collecting digital evidence.
    - Assemble the appropriate tools and resources for digital evidence collection, including hardware and software for forensic analysis.
2. **Identification of Sources**:
    - Identify the sources of potential digital evidence, including computers, mobile devices, servers, cloud storage, and network infrastructure.
    - Determine the locations where relevant data may be stored, such as file systems, databases, emails, social media accounts, and communication logs.
3. **Preservation and Documentation**:
    - Document the scene where digital evidence is located, including the physical environment and the state of any electronic devices.
    - Take photographs or videos to record the condition of the evidence and its surroundings.

- Use write-blocking hardware or software to prevent alteration or contamination of digital evidence during collection.
- Create a detailed chain of custody log to track the handling and transfer of digital evidence from collection to analysis and presentation in court.

4. **Collection Techniques**:
   - Use forensically sound methods to collect digital evidence, ensuring that data integrity is preserved throughout the process.
   - Make exact copies (forensic images) of storage media using specialized forensic tools to preserve the original evidence while allowing analysis to be conducted on duplicate copies.
   - For live systems, use specialized forensic software to collect volatile data, such as running processes, open network connections, and system logs, without altering the state of the system.
5. **Data Acquisition**:
   - Collect digital evidence in a systematic and organized manner, following established protocols and procedures.
   - Gather relevant data from identified sources, including files, emails, documents, logs, metadata, and communication records.
   - Ensure that data is collected in a forensically sound manner to maintain its integrity and admissibility in court.
6. **Verification and Validation**:
   - Verify the integrity of collected digital evidence by comparing hash values or checksums of original and duplicate copies.
   - Validate the accuracy and completeness of collected evidence by cross-referencing with other sources and conducting preliminary analysis.
7. **Packaging and Transport**:
   - Package digital evidence securely to prevent tampering, damage, or loss during transport.
   - Use tamper-evident seals and secure containers to protect storage media and documentation.
   - Transport digital evidence in accordance with legal requirements and chain of custody procedures, ensuring that it is securely transferred to the forensic laboratory or analysis facility.

8. **Documentation and Reporting**:
    - Document the collection process thoroughly, including the date, time, location, and personnel involved in each step.
    - Prepare detailed reports describing the collected digital evidence, the methods used for collection, and any observations or findings during the process.
    - Maintain accurate records of all documentation, reports, and chain of custody logs for future reference and legal proceedings.

By following a structured process for collecting digital evidence, investigators can ensure the integrity, authenticity, and admissibility of evidence in legal proceedings while adhering to ethical and legal standards.

CHALLENGES ASSOCIATED WITH COLLECTION AND USE OF DIGITAL EVIDENCES IN CRIMINAL TRIAL

The collection and use of digital evidence in criminal trials present several challenges, which can impact the integrity, admissibility, and reliability of the evidence. Some of the key challenges associated with digital evidence in criminal trials include:

1. **Complexity and Volume**: Digital evidence often involves vast amounts of data stored across multiple devices and platforms, including computers, mobile phones, cloud services, and social media accounts. Managing and analyzing large volumes of digital evidence can be time-consuming and resource-intensive for investigators and prosecutors.
2. **Authentication and Chain of Custody**: Establishing the authenticity and integrity of digital evidence is crucial for its admissibility in court. Challenges may arise in proving the chain of custody, ensuring that the evidence has not been tampered with or altered during collection, storage, or analysis.
3. **Privacy and Data Protection**: Digital evidence collection must comply with legal and privacy regulations governing the protection of personal data and electronic communications. Obtaining warrants, consent, or legal authorization for accessing and collecting digital evidence while respecting individuals' privacy rights can be challenging.
4. **Technological Complexity**: Digital evidence often involves complex technologies, encryption, and security mechanisms, which may require specialized tools and expertise to access, extract, and interpret data. Keeping pace with rapid technological advancements and evolving digital platforms presents ongoing challenges for investigators and forensic experts.
5. **Anti-Forensic Techniques**: Perpetrators may employ anti-forensic techniques to hide, delete, or alter digital evidence, making it more challenging for investigators to collect and preserve data effectively. Detecting and countering these techniques requires advanced forensic analysis and expertise.

6. **Cross-Border Jurisdictional Issues**: Digital evidence collection in cases involving multinational crimes or online activities may raise jurisdictional challenges, particularly when data is stored or transmitted across international borders. Coordinating investigations and obtaining evidence from foreign jurisdictions can be complex and time-consuming.

7. **Expert Testimony and Interpretation**: Presenting digital evidence in court often requires expert testimony to explain technical concepts, methodologies, and findings to judges and juries. Communicating complex technical information in a clear and understandable manner can be challenging for both prosecutors and defense attorneys.

8. **Legal Admissibility and Standards**: Digital evidence must meet legal standards for admissibility, relevance, and reliability in court. Challenges may arise in establishing the probative value of digital evidence, addressing objections from opposing counsel, and navigating evolving legal precedents and rules of evidence.

Addressing these challenges requires collaboration among law enforcement agencies, forensic experts, legal professionals, and technology providers to develop best practices, standards, and protocols for collecting, analyzing, and presenting digital evidence in criminal trials. Ongoing training, education, and interdisciplinary cooperation are essential to ensure the effective use of digital evidence in the pursuit of justice.

LAW RELATING TO ADMISSIBILITY AND RELIABILITY OF DIGITAL EVIDENCE IN INDIA

Ensuring the admissibility and reliability of digital evidence poses significant challenges for legal systems worldwide. The admissibility of the electronic evidence rest on two hallmarks of credibility and authenticity. Various legal developments have taken to ensure that authentic digital evidences can aid the criminal justice system in dispensation of justice.

In India, the legal landscape concerning digital evidence is multifaceted and constantly evolving due to technological advancements and legal precedents. Digital evidence's admissibility hinges on relevance, authenticity, and reliability. Courts assess whether the evidence is what it claims to be and if it was obtained legally.

The legal framework governing the relevance and admissibility of digital evidence in India is delineated within several Indian statutes. The Information Technology Act of 2000 serves as the primary legislation concerning electronic records and electronic evidence. This act has spurred amendments in various statutes related to evidence, expanding their scope to encompass not just oral or documentary evidence but also electronic evidence. The Indian Evidence Act of 1872 stands as the principal law overseeing the pertinence and admissibility of electronic evidence in legal proceedings across the country.

Additionally, amendments to the Indian Penal Code of 1860 have been made to encompass electronic records, extending beyond traditional written documents, as means through which offenses are committed.

Furthermore, to facilitate the presentation of electronic evidence in court, the Code of Criminal Procedure of 1973 provides specific provisions for proving digital evidence through government scientific experts.

Information Technology Act, 2000

The Information Technology Act of 2000 plays a pivotal role in providing legal recognition to electronic records and electronic signatures in India. This legislation establishes the legal framework necessary to facilitate electronic transactions and communications, ensuring their validity and enforceability. Key provisions of the IT Act [2]include:

1. Legal Recognition: Section 4 and Section 5 of The IT Act grants electronic records and electronic signatures the same legal validity and recognition as traditional paper-based records and handwritten signatures. This recognition is crucial for fostering trust and confidence in electronic transactions and communications.

2. Electronic Signatures: Chapter 2 and Chapter 3 of the IT Act provides a legal framework for the use of electronic signatures, allowing individuals, businesses and Government Agencies to authenticate electronic documents and transactions securely by way of asymmetric crypto system. Electronic signatures are deemed equivalent to handwritten signatures under the Act.

3. Cybercrime Provisions: Chapter 11 of the IT Act includes provisions aimed at combating cybercrime and safeguarding electronic transactions and data. It criminalizes various cyber offenses such as hacking, identity theft, cyber terrorism, publishing or transmitting obscene material and unauthorized access to computer systems.

4. Data Protection and Privacy: The legislation also includes clauses concerning data protection and privacy, which delineate rules for gathering, retaining, and handling individuals' personal data within the realm of electronic transactions. It sets forth measures to shield sensitive personal information from unauthorized use and access. Furthermore, it grants the Central Government authority to safeguard vital digital infrastructure and manage cyber incident responses by designating computer systems as protected systems under section 70 of the Act. Additionally, it mandates the estay evidences blishment of a Nodal Agency under section 70 A and the Indian Computer Emergency Response Team (CERT-In) as the national agency under section 70 B for handling such incidents.

5. Jurisdiction and Enforcement: The IT Act defines the jurisdiction of Indian authorities in handling cybercrime cases and outlines procedures for investigation, prosecution, and adjudication of offenses under the Act. It empowers law enforcement agencies to take necessary measures to combat cyber threats effectively.

Overall, the IT Act of 2000 plays a crucial role in promoting the use of electronic records and signatures, while also providing legal mechanisms to address cybercrime and ensure the security and integrity of electronic transactions and communications in India.

[2] The information Technology Act, 2000

Indian Evidence Act, 1872

The Indian Evidence Act, 1872 establishes a legal framework for determining the relevance and admissibility of electronic evidence through its various provisions. Section 3 of the Act [3]acknowledges electronic records as valid evidence alongside oral and documentary evidence. It defines "Evidence" to include ***all documents, including electronic records***, presented for court inspection, which are referred to as documentary evidence.

Chapter 2 of the Act delineates the relevance of electronic evidence through its provisions. Section 45 of the Act holds significant importance concerning electronic evidence. It renders expert forensic evidence admissible, playing a crucial role in determining the admissibility and utilization of electronic evidence in criminal trials.

The Indian Evidence Act, 1872, prescribes guidelines for admitting electronic evidence, which are delineated in various sections, notably Sections 136, 65A, and 65B.

Section 136 of the Act addresses the admission of evidence, establishing the principle that evidence can only be provided regarding relevant facts in a court of law. It renders all types of evidence admissible if they pertain to the relevant facts outlined in Sections 6-55 of the Act.

Sections 65A and 65B provide specific provisions regarding the admissibility of electronic evidence.

Section 65A declares that the contents of electronic records may be proved in accordance with the provisions of section 65B.

Section 65B is a non obstante clause that sets out the requirements for the admissibility of electronic evidence. It stipulates that any information contained in an electronic record must be presented in court in the form of a certified electronic record. The certification must be provided by a person in charge of the operation of the relevant device or computer, and it must confirm the conditions under which the electronic record was produced, stored, or transmitted. Failure to adhere to these requirements may render the electronic evidence inadmissible. The certificate must relate to the following matters:

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;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) of Section 65 B of the ACT relate. It relates to the following :

- the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

[3] Indian Evidence Act, 1872

- during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
- throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
- the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

Overall, these sections of the Indian Evidence Act establish a legal framework for determining the admissibility of electronic evidence, ensuring that such evidence meets certain standards of authenticity and reliability before being accepted in court. However there has been a long standing controversy as to requirement of certificate in relation to the admissibility of electronic evidences. It was set to rest recently by the judgement of constitutional bench in the case of Arjun Pandit Rao Khotkar V. Kailash Kushan Rao Khotkar.[4]

In case of NCT of Delhi v. Navjot Sandhu [5]the Supreme Court held regardless of whether Section 65B's standards regarding the admissibility of electronic data are met, there is no restriction on the admission of secondary evidence under the other provisions of the Evidence Act, notably Sections 63 and 65. This opened the room for admissibility of electronic evidence without producing certificate in term of sub section 4 of section 65 B of the Act.

However this judgement was overturned in the case of Anvar PV v. PK Basheer [6]where court held that "Proof of electronic record is a special provision introduced by the IT Act amending various provisions under the Evidence Act. The very caption of Section 65A of the Evidence Act, read with Sections 59 and 65B is sufficient to hold that the special provisions on evidence relating to electronic record shall be governed by the procedure prescribed under Section 65B of the Evidence Act. That is a complete code in itself. Being a special law, the general law under Sections 63 and 65 has to yield[7]." Thus, in nutshell it emphasized the fact that Section 65 A and 65 B being a separate code in itself has to be strictly and mandatorily complied with in case of admissibility of electronic evidences.

Thereafter in case of Shafhi Mohd. V. State of Himachal Pradesh the court stated "that it can be safely held that electronic evidence is admissible and provisions under Sections 65A and 65B of the Evidence Act are by way of a **clarification and are procedural provisions**. If the electronic evidence is authentic and relevant the same can certainly be admitted subject to the Court being satisfied about its authenticity and procedure for its admissibility may depend on fact situation such as whether the person producing such evidence is in a

[4] Arjun Pandit Rao Khotkar v. Kailash Kushan Rao Gorantyal[(2020) 7 SCC 571]
[5] NCT of Delhi v. Navjot Sandhu [(2005) 11 SCC 600]

[7] Anvar PV v. PK Basheer [(2014) 10 SCC 473]

position to furnish certificate under Section 65B(h)"[8] Thus it held that compliance of Sec 65 A and Section 65 B is not mandatory in every case. Where Certificate cannot be obtained the electronic evidence is admissible if found to be authentic and credible.

The controversy was finally set to rest by Arjun Pandit Rao Khotkar v. Kailash Kushan Rao Gorantyal in which the ratio of the Supreme Court can be briefly summarised as following:

1. Section 65A and 65B together form a comprehensive legal framework. A certificate mandated by Section 65B(4) is essential for the admissibility of any secondary electronic record.
2. Where primary evidence itself has been produced, no certificate under Section 65B would be necessary.
3. The certificate mandated by Section 65-B can be presented at a later stage under any circumstances if it was not obtained alongside the electronic record, or if it was not submitted to the court with the charge-sheet, or if it was submitted but in an improper format. Such omission is considered a curable irregularity.
4. The necessary certificate does not have to be provided during the presentation of evidence but can be furnished at a later stage in the proceedings.
5. In case person having original electronic record, refuses to provide certificate, the trial Courts may secure Certificate under Section 65B in respect of any Secondary electronic record from such person by using its inquisitorial powers under Sections 91, 311,173(8),231 of the Code of Criminal Procedure, 1973 [9]and Section 165 of the Indian Evidence Act,1872
6. It issued general directives to cellular companies and internet service providers regarding the preservation of Call Detail Records (CDRs) and other pertinent records for the specified duration. These directions mandate the maintenance of CDRs and other records in a segregated and secure manner if they are seized during investigations within the mentioned period. These directives are applicable to criminal trials until appropriate instructions are issued under relevant licenses or under Section 67C of the Information Technology Act, 2000. Furthermore, the judgment establishes a procedure for concerned parties to summon such CDRs and other records during the presentation of defence evidence or during the cross-examination of a specific witness.

CONCLUSION

The rapid advancement of technology has transformed the landscape of criminal activities, giving rise to new forms of offenses that exploit digital infrastructure. In response to these challenges, the role of digital evidence has become indispensable in unraveling the complexities of modern-day crimes. This research delves into the multifaceted facets of digital evidence, exploring its significance in investigating, prosecuting, and resolving various forms of criminal activity.

[8] Shafhi Mohd. V. State of Himachal Pradesh [**(2018) 5 SCC 311**]
[9] Code of Criminal Procedure, 1973

Through an analysis of legal frameworks, case studies, and empirical investigations, this study highlights the critical role of digital evidence in reconstructing the narrative of criminal occurrences, from cybercrimes to conventional offenses facilitated by digital means. It underscores the importance of proper handling, preservation, and analysis of digital evidence to ensure its admissibility and reliability in legal proceedings.

Despite the invaluable insights provided by digital evidence, its collection and utilization pose significant challenges. From technical complexities to legal and ethical considerations, navigating the landscape of digital forensics requires specialized expertise, resources, and interdisciplinary cooperation.

Furthermore, this research examines the evolving legal paradigms and technological innovations shaping the domain of digital forensics, emphasizing the necessity for adaptive methodologies and collaboration to effectively counter emerging threats.

By shedding light on the pivotal role of digital evidence in contemporary law enforcement and criminal justice efforts, this study aims to enlighten policymakers, law enforcement entities, and practitioners regarding the imperative of leveraging technological advancements and forensic acumen to contend with the complexities engendered by the shifting landscape of crime in the digital era.

REFERENCES:

1. Mishra, A., & Gupta, S. (2021). Digital evidence in the age of cybercrime: Challenges and opportunities. International Journal of Cyber Criminology, 15(1), 78-94.
2. Singh, R., & Kaur, A. (2020). Role of digital evidence in criminal investigations: A comprehensive review. Journal of Forensic Science & Criminology, 8(3), 120-135.
3. Sharma, P., & Saxena, V. (2019). Digital evidence: Legal perspectives and challenges. International Journal of Law and Legal Jurisprudence Studies, 6(2), 267-282.
4. Gupta, R., & Verma, A. (2018). Admissibility of electronic evidence in India: An analytical study. Journal of Legal Analysis & Research, 5(2), 189-205.
5. Choudhury, A., & Das, S. (2017). Digital evidence and its admissibility: A critical analysis. Indian Journal of Legal Studies, 5(1), 45-62.
6. Pandey, S., & Sharma, N. (2016). Evolution of legal framework for digital evidence in India. Journal of Cyber Law & Policy, 14(2), 201-218.
7. Indian Evidence Act, 1872.(1872).Government of India
8. Information Technology (IT) Act, 2000. (2000). Government of India.
9. Arjun Pandit Rao Khotkar v. Kailash Kushan Rao Gorantyal [(2020) 7 SCC 571]
10. NCT of Delhi v. Navjot Sandhu [(2005) 11 SCC 600]
11. Anvar PV v. PK Basheer [(2014) 10 SCC 473]
12. Shafhi Mohd. V. State of Himachal Pradesh [(2018) 5 SCC 311]

BIBLIOGRAPHY

1. **Friedman Nemecek& Long LLC**.(blog)
   URL: https://www.iannfriedman.com
2. www.livelaw.in.columns
   URL:https://www.livelaw.in/columns/arjun-panditrao-decision-the-time-to-revisit-s65b-of-indian-evidence-act-a-scientific-legal-analysis-162590?from-login=927983
3. www.scconline.com.(blog)
   URL:https://www.scconline.com/blog/post/2020/07/14/sc-clarifies-law-on-admissibility-of-electronic-evidence-without-certificate-under-section-65b-of-evidence-act-1872/
4. www.legalserviceindia.com.article
   URL:**https://www.legalserviceindia.com/legal/article-14633-the-admissibility-and-challenges-digital-evidence-in-court.html#google_vignette**