

Digital Evidence – its Applications in Court Proceedings

Krishna Karthik. L. R¹, Lakshmi Aishwarya R², Ramakrishna. L³

¹BALLB (Hons) Scholar, MKPM RV Institute of Legal Studies, KSLU, Bengaluru

²MBA Scholar, Dayananda Sagar College of Engineering, Bengaluru

³Superintending Survey Officer, Geological Survey Officer, Ministry of Mines, Bengaluru

Abstract—In the saga of advanced and modern technological evolutions in India, the Application of Digital evidence forms an important form of an Investigation. The Digital Evidence being used more and more with an objective to make the investigation faster and authenticated in solving the complicated crimes and legal proceedings. The Digital Evidence also known as Electric Evidence is used as reliable in comparison with the traditional evidence. The Government of India, recognised the importance of digital evidence and made necessary enactments in the Parliament of India for admissibility in the new Bharatiya Sakhsya Bill, 2023. The Bill is regarded the Digital Evidence as a Primary Evidence for the reasons that the evidence collected is safe and unchanged by way of safeguarding with strong passwords and digital security adoptions. The Digital Evidence has its own challenges such as software privacy, cyber hacking, cyber fraud, cyber theft, etc., and hence there is need for the updating of legislation and provision of clear guidelines to secure and create awareness on safety of the evidence. Here, the authors are making an attempt to study the aspects on the Digital Evidence and on the legal provisions, thereof.

Index Terms—Digital Evidence, Cyber Crime, Legal Provision and information technology.

I. INTRODUCTION

Application of Digital Evidence in Court Proceedings in India has become an important part of civil and criminal litigation in India. It includes information created, stored, transmitted or received in digital form, such as emails, WhatsApp messages, SMS, call-detail records, CCTV footage, photographs, videos, social-media posts, GPS/location data, computer files, server logs, cloud data and digital documents. The legal framework has undergone a major change because, from 1 July 2024, the

Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaced the Indian Evidence Act, 1872. The BSA specifically deals with electronic and digital records. 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 are (i) Communications through text messages, emails, instant messaging, and other electronic messaging platforms can be used as digital evidence; (ii) 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; (iii) Digital documents, spreadsheets, presentations, and other file types are also forms of digital evidence. Metadata within these files may also provide important information; (iv) Digital photos and videos can be powerful evidence. Metadata, such as timestamps, and geolocation data, can be crucial in order to establish authenticity and context of media files; (v) Logs that record computer and internet activities, including browsing history, file access and system logs, can be analysed as digital evidence; (vi) Mobile devices and some digital cameras record GPS and location data, and are also considered as digital evidence; (vii) Records of phone calls, including call logs, durations and time stamps, can be treated as digital evidence; (viii) 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; (ix) Fingerprints, facial recognition data, and recording of unique voice characteristics may be used as digital evidence; (x) Information related to network traffic, IP addresses, and connection logs can be important for

cybersecurity and digital forensics; (xi) Information that is related to software usage, application logs and system configurations can be treated as digital evidence; (xii) Data which is stored in cloud services such as Google Drive, Dropbox, or One drive, can be used as evidence; (xiii) 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; and (xiv) Cryptocurrencies, and blockchain transactions, can also serve as digital evidence.

II. IMPORTANCE OF DIGITAL EVIDENCE

Digital evidence is collected using specialised tools and techniques. Forensic experts use methods such as imaging hard drives, analysing network traffic and extracting data from various devices. In India, the use of digital evidence is not limited to particular cases. It can be used in a wide range of cases including cybercrime, fraud, intellectual property theft, child exploitation and even in traditional criminal investigations where electronic devices are involved. Digital evidence can be used to establish facts in both criminal and civil proceedings such as (i) WhatsApp or SMS messages may establish communication between parties; (ii) Emails may establish contractual negotiations or admissions; (iii) CCTV footage may establish the presence of a person at a particular location; (iv) Call-detail records may help establish communication between individuals; (v) GPS data may establish the location or movement of a person or vehicle; (vi) Digital photographs and videos may establish the occurrence of an event; (vii) Computer or server logs may establish access, transactions or other activities; and (viii) Social-media posts may constitute evidence of statements, conduct or publication. The principal advantage of digital evidence is that it can preserve information that may otherwise be difficult to establish through oral testimony. At the same time, courts must consider questions of authenticity, integrity, reliability, relevance and manner of proof.

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: (i) 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; (ii) 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; (iii) 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; (vi) Digital evidence helps to establish intellectual property theft, copyright infringement, or violation of digital rights by providing a clear record of data through different digitised methods. It helps to establish ownership and provides proof of unauthorized use or distribution of digital assets; (v) Digital evidence plays a crucial role in establishing facts in concern with the cybercrimes, which have been occurring more recently. In order to combat cybercrimes like cyber harassment, online bullying, online fraud and other related offences, digital proof is essential to establish real facts; (vi) 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.; (vii) 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; (viii) 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 cybercriminals by finding out where attacks 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; (ix) The matter deals with border issues, digital evidence is very essential. The digital technology is used to monitor border security issues. In order to analyse and monitor activities related to potential threats, it plays a role in verifying identities, tracking the movement of individuals, and preventing illegal activities across borders; (x) Digital evidence is essential for establishing the facts concerned with public safety. Police and security teams use digital information to monitor online activities and, they can investigate as early as possible; and (xi) In the healthcare sector, the adoption of digital technology is important to make sure that information about the patient is kept private and secret. It helps in checking if someone is misusing medical records or doing something wrong with the patient's information. It can be used as digital evidence if any issues arise in future.

III. 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), in 2019 there was a significant rise of 63.5 percent in cybercrime cases reported in India. The reported cases increased from 28248 to 45546 cases in 2019. In those cases, a total 60.4 percent involved fraud as the primary motive, while 5.1 percent are related to sexual exploitation. Karnataka had the highest number of registered cyber crimes cases 12020, in Uttar Pradesh 11416, in Maharashtra 4867, and in Assam as 2231 cases. Among the union territories Delhi alone accounted for 78 percent of cyber crimes. By the end of 2022, there were a total of 65000 cyber related cases registered in India. 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, cyberstalking, and credit card fraud. Digital evidence is important in finding cybercrimes and proving them in court. The use of digital devices assists in uncovering the evidence related to proof of cybercrimes, data leaks, hackings, and other digital problems. Indian authorities are incorporating various

licensed equipment. That equipment are specialised in software and advanced algorithms for their investigations. This helps to combat cybercrimes effectively. In this regard, tools like X-ways, WinHex, Rifliuti, Pasco, Galleta / Cookies, Nmap, ethereal BinText, and more are helpful in investigation purposes. Rifuti helps to recover deleted documents and Pasco gathers records of internet activities on a targeted computer.

IV. SIGNIFICANCE AS 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 authorised 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 unauthorised 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: (i) 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; and (ii) Digital certificates are used to verify the identity of a person or any organisation. 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.

V. 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 criticised 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 from a satellite phone, Direct Inward Dialing (DID) facilities, GPS equipment and the tracking of emails/IP addresses. Even before this incident, there were worries about the use of digital devices in attacks in India. Pakistani hacker groups had been targeting Indian websites and tried to hack government official pages and an atomic research facility.

VI. INDIAN EVIDENCE ACT, 1872

The Indian Evidence Act, of 1872 is one of the foundational legislations 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. This document 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 such as (i) 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; (ii) During this regular use, the kind of information in the electronic record was regularly input into the computer as part of the usual activities; (iii) 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; and (vi) 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 (2014), 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 emphasised that this certificate ensures the source and authenticity of the electronic record. However, in the case of Shafhi Mohammad v/s State of Himachal Pradesh (2018), 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.

VII. BHARATIYA SAKSHYA ADHINIYAM, 2023

The principal legislation governing the admissibility of digital evidence is now the Bharatiya Sakshya Adhiniyam, 2023. Its provisions concerning electronic evidence are principally found in Sections 61–63. Section 61 provides that an electronic or digital record cannot be denied admissibility merely because it is electronic or digital. Subject to Section 63, it has the same legal effect, validity and enforceability as other documents. Thus, the law recognises the basic principle that a digital document is not inferior to a paper document merely because of its electronic form. Section 62 provides that the contents of electronic records may be proved in accordance with Section 63. Therefore, Section 62 must generally be read together with Section 63 when electronic evidence is sought to be introduced in court. Section 63 is particularly important. It deals with the admissibility of electronic records produced from computers and communication devices and lays down conditions under which such electronic records can be admitted as evidence. An important requirement is the certificate contemplated by Section 63(4). Where an electronic record is sought to be admitted under this provision, the certificate must identify the electronic record, describe how it was produced, provide relevant particulars of the device involved and address the conditions relating to the computer/device. It is to be signed by the appropriate person and an expert, in accordance with the statutory requirements. This provision is the successor to the former Section 65B of the Indian Evidence Act, 1872. Before 1 July 2024, electronic evidence was principally governed by Sections 65A and 65B of the Indian Evidence Act, 1872. Section 65A provided the special framework for proving electronic records, while Section 65B dealt with the admissibility of computer output. The Supreme Court's interpretation of Section 65B remains highly important because the new Section 63 substantially carries forward the earlier framework. In Arjun

Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), the Supreme Court held that the certificate required under Section 65B(4) was a condition precedent for admissibility of secondary electronic evidence. The Court reaffirmed the earlier decision in Anvar P.V. v. P.K. Basheer.

VIII. PRIMARY AND SECONDARY DIGITAL EVIDENCE

An important distinction is between the original electronic record/device and a copy or computer output. For example, Producing the original device containing the relevant data may raise different evidentiary considerations from Producing a printout, copied file, extracted data or other computer output. The BSA's provisions on primary and secondary evidence, read with Sections 61–63, determine how the electronic material should be proved. The BSA also expressly deals with electronic/digital records within its provisions on primary evidence. Consequently, merely printing a WhatsApp conversation or taking a screenshot does not automatically resolve all questions of admissibility. The party producing it must establish it in accordance with the applicable evidentiary requirements.

IX. ROLE OF THE CERTIFICATE

The certificate is particularly important where electronic evidence is being produced in the form contemplated by Section 63. A proper certificate helps establish (i) what electronic record is being produced; (ii) how it was generated or extracted; (iii) which computer, mobile phone, server or other device was involved; (iv) the relevant circumstances concerning the functioning of the device; (v) the identity/role of the person responsible for the device or relevant activities; and (vi) the expert's certification as required by the statutory scheme. The statutory certificate is therefore intended to provide the court with assurance concerning the source and reliability of the electronic record. Section 63(4) specifically requires the certificate to accompany the electronic record at each instance when it is submitted for admission. Other important legislation include Digital evidence in Indian courts is not governed by the BSA alone.

X. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 remains important because the BSA itself uses concepts and terminology connected with the IT Act. The IT Act provides the broader legal framework for electronic records, electronic signatures and various cyber activities.

XI. BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) governs criminal procedure. It expressly recognises the use of audio-video electronic means, including video conferencing and electronic recording/transmission in various procedural contexts. This is significant because digital evidence is not merely something that can be produced at trial; electronic technology is also increasingly incorporated into investigation, search and seizure, identification and court proceedings.

XII. BHARATIYA NYAYA SANHITA, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS) contains offences involving conduct connected with documents and electronic records. For example, it addresses failure to produce a document or electronic record where a person is legally bound to do so.

XIII. APPLICATION IN CRIMINAL & CIVIL PROCEEDINGS

Digital evidence can play a crucial role at several stages of a criminal case: Investigation → seizure/acquisition → forensic examination → charge-sheet → admission in evidence → examination/cross-examination → appreciation by court. For example, in a cybercrime case, investigators may obtain a mobile phone or computer, create a forensic copy, examine relevant files and metadata, and subsequently produce the relevant electronic record before the court. Similarly, CCTV footage may be used to establish the movement of an accused, while call records can be used to establish communication between individuals. The prosecution must nevertheless

establish the relevance and evidentiary reliability of the material; the mere existence of a digital file does not automatically prove the truth of everything contained in it.

Digital evidence is also increasingly important in civil litigation. Examples include: (i) Electronic contracts and emails in contractual disputes; (ii) Banking records in financial disputes; (iii) WhatsApp conversations in commercial or family litigation; (iv) Digital photographs in property or damage claims; (v) GPS records in transportation disputes; (vi) Website records in intellectual-property disputes; and (vii) Electronic accounting records in commercial litigation. The court must determine whether the electronic record is relevant and whether it has been properly proved under the BSA.

Indian courts generally examine digital evidence carefully because electronic information can potentially be altered, copied, manipulated or fabricated. The Supreme Court's decision in *Anvar P.V. v. P.K. Basheer* established the importance of compliance with the statutory requirements for secondary electronic evidence. Arjun Panditrao Khotkar subsequently reaffirmed and clarified the position, particularly regarding the certificate requirement under Section 65B. The transition to the BSA does not eliminate the importance of these principles. Section 63 now occupies the central statutory position concerning admissibility of electronic records.

A party seeking to rely on digital evidence should generally pay attention to (i) Relevance – The evidence must relate to a fact in issue or relevant fact, (ii) Authenticity – The source and identity of the electronic record should be capable of being established; (iii) Integrity – There should be no unexplained alteration or manipulation; (iv) Proper acquisition – Investigators or parties should preserve the evidence appropriately; (v) Chain of custody – Particularly in criminal cases, the handling and transfer of digital evidence should be properly documented; (vi) Forensic examination – Where necessary, an expert may examine the device or data; (vii) Section 63 compliance – Where applicable, the statutory requirements and certificate must be satisfied; and (viii) Presentation before court – The original device, forensic copy, printout, extracted data or other form of evidence should be produced in the legally appropriate manner.

XIV. SUGGESTIONS

- 1) Providing training and education for legal professionals and law enforcement officials is very important. The training and education with regard to the digital methods and its applications will enhance the proper usage of different digital methods, it will help to collect more accurate information about the cases involving such evidence. It will enhance the credibility and admissibility of such evidence before the court.
- 2) There is a need for clarity regarding the rules of digital evidence in its collections, storage, and presentation. This includes making guidelines for using forensic tools, setting procedures for handling digital evidence correctly, and having protocols in place.
- 3) It is important for different groups like the police, lawyers, and tech experts to work together. They can share the many ways to do things, create new technologies and agree on common rules. It will help to deal with the challenges of handling digital evidence because when people from different groups work together, they often have the opportunity to learn about each other's work, details of evidence, and the rules for collecting and presenting it in court.
- 4) Using strong and unique passwords for all accounts is essential to reduce the risk of unauthorised access.
- 5) Implementation of two factor authentication will add an extra layer of security. It provides users with a second form of verification such as a code sent to their mobile device. Two factor authentication is a security process that requires users to provide two different authentication factors to verify their identity.
- 6) Keeping all software, operating systems and applications up-to-date will help to mitigate cybercrimes. When a software is updated regularly, it will protect the system from unauthorised usage or illegal hacking. Regular updates ensure that the system has the latest security measures in place.
- 7) Encryption tools will help to protect sensitive data. It can be used both in transactions and when such data is stored. This adds a layer of security from cyber hacks.

- 8) Activating a backup system can save a lot of information. It will help in the event of a cyber-attack and it allows for the recovery of necessary information.
- 9) Applying firewalls and intrusion detection systems will help to monitor and control network traffic. This will help to mitigate unauthorised access.
- 10) Digital evidence is sensitive and easily changed so it is important to collect volatile evidence. This evidence refers to digital data that is temporary and can be easily altered or lost. This type of evidence is usually stored in collective memory such as RAM and can be quickly affected by actions like powering off a device. Accordingly, collecting the most sensitive data first and least sensitive at last. It is very important to collect the correct order of volatility of evidence.

XV. CONCLUSION

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. Digital evidence has become an essential component of modern judicial proceedings in India. The Bharatiya Sakshya Adhiniyam, 2023, particularly Sections 61, 62 and 63, provides the present statutory framework for electronic and digital records. Section 61 recognises their legal status, Section 62 directs proof of their contents according to the special procedure, and Section 63 establishes the principal admissibility framework, including the certificate requirement. The earlier jurisprudence under Sections 65A and 65B of the Indian Evidence Act—especially Anvar P.V. and Arjun Panditrao Khotkar—remains important for understanding the principles behind the present law. The BNSS, IT Act and BNS complement the evidentiary framework by addressing electronic procedures, electronic records and technology-related

offences. In short, digital evidence is admissible in Indian courts, but its evidentiary value depends upon relevance, authenticity, integrity and compliance with the statutory requirements governing its proof. The deleted data be recovered as digital evidence. In many cases, deleted data can be recovered through forensic tools such as autopsy, and recuva that can be reconstructed and analysed in storage media. Digital evidence is presented in court through the testimony of digital forensic experts with required certificates as mentioned under Section 64B(4) of the Act. Digital evidence is typically stored in secure digital formats. It may use hash values or metadata to verify the integrity of the stored evidence over time. 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. The ICC also provided legal recognition to digital evidence in admitting such evidence in many cases. When use of technology increases, the information stored on digital devices also increases. This may lead to the misuse of technology often tends to 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. Here, the authors have made an attempt to summarise the importance of Digital Evidence and to create awareness on the application of Digital Evidence in Court proceedings.

REFERENCES

- [1] Anvar P. V. and Arjun Panditrao Khotkar.
- [2] Government of India, The Bharatiya Sakshya Adhiniyam, 2023.
- [3] Government of India, The Bharatiya Nagarik Suraksha Sanhita, 2023.
- [4] Government of India, The Indian Evidence Act, 1872.
- [5] Government of India, The Bharatiya Sakshya Bill, 2023.
- [6] Government of India, The Information Technology Act, 2000.
- [7] Government of India, The Bankers' Books Evidence Act, 1891.
- [8] Intellectual Property Rights (IPR).
- [9] State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru, (2005).
- [10] Manu Sharma v. State (NCT of Delhi), (2010).
- [11] Unnikrishnan @ Unni v. State by Inspector of Police, (2011).
- [12] Konnadan Abdul Gafoor v. State of Kerala, (2012).
- [13] Anvar P. V. v. P. K. Basheer & Ors., (2014).
- [14] Tomaso Bruno & Anr. v. State of Uttar Pradesh, (2015).
- [15] Shafhi Mohammad v. State of Himachal Pradesh, (2018).
- [16] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020).
- [17] PRS Legislative Research, "The Bharatiya Sakshya Bill, 2023." Available: <https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023>
- [18] Law Times Journal, "Digital Forensics in India: An Overview." Available: <https://lawtimesjournal.in/digital-forensics-in-india-an-overview/>
- [19] ScienceDirect, "Digital Evidence and Related Research." Available: <https://www.sciencedirect.com/science/article/abs/pii/S1742287612000187>
- [20] Financial Express, "Cybercrime and Digital Evidence." Available: <https://www.financialexpress.com/business/defence-cybercrime-and-digital-evidence-2632164/>
- [21] LatestLaws, "Importance of Protecting Intellectual Property Rights in Digital Age." Available: <https://www.latestlaws.com/articles/importance-of-protecting-intellectual-property-rights-in-digital-age-180377/>
- [22] Cyril Amarchand Mangaldas, "Supreme Court on the Admissibility of Electronic Evidence under Section 65B of the Evidence Act." Available: <https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/>

- [23] SCC Online, “Electronic Evidence.” Available:
<https://www.scconline.com/blog/post/2021/03/13/electronic-evidence/>
- [24] Murarijha Legal, “Digital Evidence in Indian Law: Investigating Challenges and Legal & Ethical Considerations.” Available:
<https://medium.com/@murarijhalegal/digital-evidence-in-indian-law-investigating-challenges-and-legal-ethical-considerations-6ef913052254>
- [25] Legal Desire, “Challenges Faced by Digital Forensics.” Available:
<https://legaldesire.com/challenges-faced-by-digital-forensics/>
- [26] Jackson Kelly, “Admissibility of Electronic Evidence.” Available:
<https://www.jacksonkelly.com/anticipation-litigation-advisor-blog/admissibility-of-electronic-evidence>
- [27] Australian Law Reform Commission, “Reliability and Accuracy of Computer-Produced Evidence.” Available:
<https://www.alrc.gov.au/publication/uniform-evidence-law-alrc-report-102/6-documentary-evidence/reliability-and-accuracy-of-computer-produced-evidence/>