Digital Evidence and Legal Challenges of Admissibility in Court

Govind Bahadur Singh
Assistant Professor, Janhit College of Law

***Abstract*- In the digital age, the collection, preservation, and presentation of digital evidence in legal proceedings have gained prominence in India. Digital evidence refers to any information stored or transmitted in digital form, including data from computers, smartphones, emails, social media, and sound storage. While digital evidence plays a crucial role in modern investigations, its admissibility in court poses significant legal challenges, primarily around its authenticity, chain of custody, and relevance. A key issue is the need for digital evidence to be presented in a way that ensures it is unaltered and reliable. Unlike physical evidence, digital data can be easily manipulated, raising concerns about the integrity of evidence during collection and transmission. The legal system must establish robust protocols for preserving and documenting the evidence to prevent tampering or alteration. Moreover, the existing legal framework in India, such as the Bharatiya sakshya sanhita, is not fully equipped to handle the complexities of digital evidence. While the Information Technology Act, 2000 has made some strides in addressing digital issues, its implementation is often unclear, especially in the context of the courts. Another challenge is the lack of specialized knowledge among legal professionals and law enforcement officers in handling digital evidence, which may hinder its proper use in trials. Additionally, issues related to privacy rights, data protection, and cybercrimes create further complexities when presenting digital evidence. Balancing the need for justice with the protection of individual rights remains a contentious issue. As technology evolves, Indian laws must be continuously updated to address emerging issues related to digital evidence.**

***Index Terms*- Digital evidence, admissibility, authenticity, chain of custody, Indian Evidence Act, Information Technology Act, legal challenges, data protection, cybercrimes.**

I. INTRODUCTION

Digital evidence refers to any information stored or transmitted in electronic form that can be used in a legal context to support or refute saims in a case. It can encompass a wide variety of data, such as emails, text messages, documents, audio/video recordings, photographs, and metadata—essentially, any data that is stored or communicated digitally. Digital evidence is crucial in a wide array of cases, ranging from cybercrime and fraud to intellectual property theft and family disputes.[1]

The evidence laws have been modernised, streamlined, and made simpler by the "Bharatiya Sakshya Adhiniyam, 2023", replacing the "Indian Evidence Act of 1872".Although many of the provisions of the IEA are still included in the BSA, they have been updated and improved.The amendment was introduced to add Section 65A & 65B to the act, keeping the concerns regarding the authenticity of electronic records intact and to ensure their adaptability in courtrooms

The usage of digital and electronic evidence in court proceedings is expanding quickly but dealing with the many categories of electronic evidence such as CDs, DVDs and computer-generated documents brings a unique set of problems and difficulties for suitable authentication. But now the changes have been introduced and BSA has allowed digital or electronic records to be accepted as evidence and stipulates that they must have the same legal weight, validity, and enforceability as paper records. The updated definition of 'document ' clearly includes digital and electronic records[2]

II. DEFINITION OF DIGITAL EVIDENCE

Electronic evidence is regarded by the BSA as documentary evidence. Documentary evidence is defined as "evidence" under S. 2(1)(e)[3] to include documents that include electronic or digital records that are produced for the Court's scrutiny.

As compared to IEA, which defines "electronic evidence" as documentary evidence in the interpretation clause under Sec 3 whereas BSA defines

the term "electronic evidence" more broadly, encompassing digital information and electronic equipment.[4]

Significance of Digital Evidence

As the use of digital platforms has exploded, so too has the role of digital evidence in both criminal and civil cases. For example, in cybercrime cases, digital evidence is often the core piece of evidence that links the defendant to a crime, while in family law, digital records such as text messages or social media interactions can be vital to resolving disputes. The widespread adoption of the internet and mobile technology has made digital evidence a cornerstone of modern legal practice in India.

Legal Challenges in the Admissibility of Digital Evidence

The most significant challenge in the legal context concerning digital evidence is ensuring its admissibility in court. Digital evidence faces unique challenges compared to traditional forms of evidence, such as physical documents or witnesses. Issues related to authenticity, tampering, preservation, and privacy concerns make it difficult for courts to accept digital evidence without careful scrutiny. The Indian legal framework, particularly the Bharatiya Nyaya Sanhita 2023 and the Information Technology Act, 2000, provide some guidelines but also face significant challenges in addressing these issues effectively. This paper aims to explore these challenges and propose solutions to ensure that digital evidence is appropriately managed and accepted in Indian courts.[5]

III. UNDERSTANDING DIGITAL EVIDENCE IN THE INDIAN CONTEXT

Types of Digital Evidence

Digital evidence can take various forms, each with its own set of challenges in terms of collection, preservation, and presentation in court.

1. **Electronic Documents:** This category includes emails, text messages, and other types of correspondence that are stored or transmitted digitally. These are commonly used in cases involving fraud, defamation, and cybercrimes.
2. **Data from Social Media and Messaging Platforms:** Evidence gathered from platforms such as Facebook, WhatsApp, Twitter, and Instagram has become essential in cases involving cyberbullying, online harassment, and defamation. However, the authenticity of such evidence is often questioned due to the ease with which posts and messages can be manipulated or deleted.
3. **Forensic Data:**Digital forensics involves the recovery of deleted files, logs, and data from computers, smartphones, and storage devices. This form of evidence is often used in criminal cases but requires specialized skills and tools for extraction and analysis.
4. **Metadata**: Metadata refers to data that provides information about other data, such as the creation date of a file, the author of an email, or the location a photo was taken. Metadata can be crucial for establishing timelines and verifying the authenticity of digital evidence.
5. **Audio/Visual Evidence:** Digital recordings, including audio files, surveillance footage, and video recordings, are becoming more common in both criminal and civil cases. Such evidence is vital in corroborating witness testimony and supporting claims made by the parties involved.

Role of Digital Evidence in Indian Courts

Digital evidence has been instrumental in various high-profile cases in India. In cybercrimes, fraud cases, and even terrorism-related cases, digital evidence can play a pivotal role in establishing guilt or innocence. Courts increasingly rely on digital records, such as emails, call logs, and chat histories, to establish a chain of events. However, due to the complex nature of digital evidence and its vulnerability to tampering, it requires rigorous procedures for authentication and handling.[6]

IV. LEGAL FRAMEWORK GOVERNING DIGITAL EVIDENCE IN INDIA

The Legal Realism school of legal jurisprudence succinctly stated that the law is always of approaching nature. The Parliament legislates law penalizing certain act and categorizing it as an offence only once it comes to light. Examples can be a law on mob lynching. The freshly legislated Criminal Law Legislations, one of them being Bhartiya Nyaya Sanhita, 2023, now includes mob lynching as an offence. The same is the case with technological advancements. A recent attempt is made through

enacting Bhartaiya Sakshya Adhiniyam, 2023 (hereinafter referred to as "BSA") to exhaustively provide for technological advancements as a means of evidence having admissibility and relevancy in the Courts of Criminal Justice in India. However, still concerns with respect to lack of proper safeguards, digital ignorance and likelihood of privacy breaches were raised.[7] BSA was also criticized by various experts on the ground that the changes brought into effect would have also been made by amending the Indian Evidence Act, 1872. To which, Senior Advocate and Former Additional Solicitor General, Pinky Anand stated: "*Whenever you change the law, some allegation of the other is always made. The point of bringing a new law is that if you amend a law it tends to have various possible contradictions, some ethos that you don't want to repeat. You want to have a law with lesser colonial deference, so that we have our own laws. So, the concept of amendment is a gone concept*[8]*."*

V. BHARATIYA NYAYA SANHITA 2023

Bharatiya Nyaya Sanhita,2023 is the new statute which replace the Indian Evidence Act,1872 governing the admissibility of evidence in Indian courts. However, the Indian Evidence act,1872 was drafted long before the advent of digital technology, which has led to several challenges in applying its provisions to digital evidence. The Act does not specifically address the issue of digital records or the methods for verifying their authenticity, making the handling of digital evidence in court complex

. THE INDIAN EVIDENCE ACT, 1872 – LIMITATIONS

Before discussing the correlation between BSA and the recent technological developments, it is necessary to discuss where the existing colonial-era Indian Evidence Act, 1872 lacked with respect to technology. An amendment was made and put into effect on Nov. 20, 2022 by the Parliament to include digital records and electronic records as means of evidence. The said amendment also made forensic evidence admissible under Sections 3(3), 45, 73B and 89A of the Indian Evidence Act, 1872. However, it is quite surprising to note that even before this amendment brought into effect, the Courts of Criminal Justice through 'judge-made law' were already giving primacy to digital records and electronic records as means of evidence. In the case of *State v. Qamrul Islam & Ors 2017*[9]the Hon'ble Court stated that 'video footage' can be considered as a 'document' under the meaning of 'document' provided under Section 02 of the said 1872 Act. In the case of *Rifat Murder Case (2020)*[10], the CCTV footage was considered as evidence under the Act.

Furthermore, apart from digital and electronic records, the forensic evidence is also used to be utilised by the Courts as means of evidence prior to this amendment. DNA, blood samples, fingerprint, etc. were considered as admissible form of forensic evidence by the Courts despite the Evidence Act, 1872 fail to mention the same. However, the said amendment restricted the definition of 'forensic evidence' to blood, semen, hair, organs, DNA, fingerprints, eye impression. This definition restricted the inclusion of new technology leading to forensic evidence through proteomics, molecular profiling. The said 'digital amendment' made to the Indian Evidence Act, 1872 was though broadened the contours of the legislation as well as lessened the confusion and disputes arising with respect to the definitions of 'digital records,' 'electronic records' and 'forensic evidence,' failed to encompass the needs of the hour.[11]

Apart from the said amendment, hardly amendments were introduced to include technological advancements as means of evidence. The said amendment was the only major amendment made to the said Act in order to include the technological means which can facilitate in determining relevancy and admissibility of the evidence.

THE BHARTIYA SAKSHYA ADHINIYAM, 2023 AND TECHNOLOGY – CORRELATION

The BSA first brought changes to the definition of 'document' under Section 2(d)[12] of the Act, including digital records and electronic records as a part of document. The said section further encapsulates the illustrations defining what are electronic records. Furthermore, Section 61[13] of the BSA provides that both kind of evidence, electronic or digital evidence and documentary evidence shall be treated equally with respect to their legal effect, validity, and enforceability.

Furthermore, amendments to the definition of "evidence," as stated in Section 2(e), is made in order to establish facts under investigation. Electronic evidence in the form of a witness statement is now permitted as per the said definition. This also implies that under Section 2(e)(i), witnesses may now virtually

appear before the Court and provide testimony, greatly streamlining and simplifying the process of delivering justice.

The Primary Evidence definition provided under Section 62 of the 1872 Act is now further enhanced providing that the original documents produced for the inspection to be done by the Court to support four new explanations about electronic and digital evidence. i.e.,

1. Creation and storage in multiple files;
2. Production from proper custody;
3. Video recordings storage and simultaneous transmission, broadcast or transfer to another;
4. Multiple storage spaces and temporary files

Implications of the changes to the provisions pertaining to the admissibility of electronic evidence under the Bharatiya Sakshya Sanhita 2023.

Similar to s.65B IEA, S.63[14] BSA provides a specific procedure for the admissibility of electronic records. However, it introduces the following changes to the other provisions relating to primary and secondary evidence, that would impact the evidentiary nature and admissibility of electronic records:

1. S.2(c) BSA which replaces s.3 IEA, defines documents to also include 'electronic or digital records'. Accordingly, separate references to electronic records have been deleted in certain provisions.[1]
2. S.57 BSA[15], which replaces s.62 IEA, introduces explanations 4 to 7, which expand the meaning of primary evidence to include electronic or digital records.

These explanations introduce the following changes:

1. Any electronic file which is created, or stored simultaneously or sequentially in multiple files (which would include copies) would be primary evidence.
2. If the proper chain of custody of electronic or digital records is produced, then it would be primary evidence.
3. Any video recording which is transmitted, broadcasted or stored in another device would be primary evidence.
4. If an electronic record is stored in multiple storage spaces in a computer, then each automated storage, including the temporary files, would be primary evidence.
5. S.62 BSA, which replaces s.65A IEA, states that electronic records must be proved as primary evidence, unless mentioned.
6. Newly introduced S.61 BSA, prescribes that the admissibility of electronic records cannot be denied on the basis of their nature as electronic records and their legal effect, validity and enforceability shall be at par with paper records.

Notably, S.63(4) BSA introduces the stage at which the certificate regarding the electronic record must be submitted. Further, it proposes changes to the authorship of such certificates, which may include the person in charge of the computer or communication device and an expert that retrieves the electronic record. Lastly, it also introduces a format for a two-part certificate to be submitted. Part A of the certificate should be filled by the party, who owns, manages or maintains the computer device from which the electronic record is retrieved. Part B of the certificate should be filled by the expert who retrieves the electronic record from the device. Currently, due to a lack of format for a certificate under s.65B IEA, there is no uniformity in the information that may be present in such certificates.[16]

. **Uncertainty regarding the procedure for Admissibility of Electronic Evidence**

The explanations 4 to 7 to S.57 BSA, consider both originals and copies of electronic records as primary evidence. Therefore, it is uncertain whether copies of electronic records would be governed by the special conditions specified in S.63 BSA or would be directly admissible as primary evidence under S.57 BSA.

a. Option 1: special procedure may continue to govern Admissibility

In view of the non-obstante clause ('notwithstanding anything contained in this Adhiniyam') in S.63(1) BSA, the ratio *of Arjun Panditrao Khotkar* may continue to be good law. Therefore, the procedure prescribed in S.63(1) BSA would continue to govern the admissibility of copies, irrespective of whether they come within the purview of primary evidence as per explanations 4 – 7 to S.57 BSA.

b. Option 2: general provisions regarding Admissibility of Documentary Evidence may be applicable to Electronic Records

Unlike s.65A IEA which specified that contents of electronic records would be proved in accordance with special provisions under s.65B; S.62 BSA marks a

significant shift as it prescribes that electronic records may be proved in a similar manner to other documentary evidence under S.59 BSA. Further, S.61 BSA, which also begins with a non-obstante sause, mandates that the admissibility of electronic records shall be at par with paper records.[17]

These changes may be interpreted to mean that copies of electronic records within the purview of explanations 4 to 7 to S.57 BSA, may be proved as primary evidence, without following the special procedure in S.63 BSA. This may resurrect the view taken by the Supreme Court in Navjot Sandhu and Shafhi Mohammad, that the general provisions governing the admissibility of documents may also apply to electronic records. In these judgments, the Supreme Court held that the special procedure in s.65B IEA is not mandatory, and can be relaxed, for instance if the electronic record is produced by a party not in possession of the device.

Changes to the conditions specified in S.63 BSA-

S.63 BSA makes three broad changes to the conditions specified in s.65B IEA for the admissibility of electronic records.

Firstly, the definition of computer output in S.63(1) BSA has been expanded to insude output from any communication device. It also adds that information in an electronic record may be 'stored, recorded or copied in any electronic form' to be covered within this provision. Similarly, S.63(3) BSA provides that computer output may be produced by computers or communication devices working standalone or in any system or network, including those managed by an intermediary such as telecom service providers, social media services etc.

Secondly, unlike s.65B(4) IEA, which does not clarify the stage at which the certificate must be submitted,[6] S.63(4) BSA mandates that such a certificate shall be submitted along with the electronic record for admission. This is a positive change as it may ensure more meaningful compliance with the admissibility requirements under S.63 BSA.

Thirdly, S.63(4)(c) provides that the certificate shall be signed by 'a person in charge of the computer or communication device and an expert (whichever is appropriate)' as per the format specified in the schedule. This marks a change from the position under s.65B(4) IEA which specified that the certificate may be signed by a person in an official position in relation to the operation of the device or in the management of relevant activities. The proposed changes under S.63(4)(c) may help ensure only those persons directly in control of the device, irrespective of their official position or designation, who may be better suited to certify the operability of the computer and the authenticity of the electronic record are permitted.

However, the use of the terms 'whichever is appropriate' creates uncertainty regarding whether the certificate should be issued by both the person in charge of the device and an expert or whether it merely indicates the type of expert that may issue the certificate. [18]This interpretation would be significant since Part A of the prescribed format of the certificate, which must be filled by the person in charge of the device, varies from Part B which has to be filled by the expert. Only Part B of the certificate carries the requirement to state that the computer device was operating properly and to specify the hash value of the file, which is essential for authenticating the electronic record. Therefore, in case submission of Part A of the certificate filled by the person in charge of the computer or communication device is sufficient, then the proper operation of the device and the hash value of the file may not be specified.

VI. THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000, was enacted to deal with issues arising from the use of computers and digital platforms. The Act governs issues related to electronic records, digital signatures, and cybersecurity, and serves as the foundational law governing digital transactions and communications in India.

Chain of Custody

Maintaining a proper chain of custody is crucial for ensuring that digital evidence is not tampered with. In the case of physical evidence, the process of documenting who handled the evidence and when it was accessed is relatively straightforward. However, for digital evidence, the chain of custody can be complex, especially when data is transferred between multiple parties or stored across different systems. Any break in the chain of custody can lead to questions about the integrity of the evidence, which can result in its inadmissibility.

Privacy Concerns

Digital evidence often involves personal information, and its collection and use raise significant privacy

concerns. In many cases, the evidence may come from private communication platforms, personal files, or social media posts. There is a need to balance the right to privacy with the need for justice. The rapid advancement of digital surveillance and data collection has led to debates regarding the extent to which privacy should be sacrificed in criminal investigations.

International Jurisdiction Issues

In cases involving digital evidence stored outside of India (e.g., on servers located in foreign countries), international jurisdiction issues arise. Indian courts may face challenges in obtaining evidence from foreign platforms like Google, Facebook, or Twitter, especially if these companies are governed by foreign laws. Additionally, cross-border legal frameworks for data sharing are still developing, creating complications for law enforcement agencies in India.[20]

VII. LANDMARK CASES INVOLVING DIGITAL EVIDENCE IN INDIA

Taking note of technological advances, the Supreme Court had observed *in R.M. Malkani v. State of Maharashtra* [20] that tape-recorded conversation is admissible in evidence provided that the conversation is relevant to the matters in issue; that there is identification of the voice and that the accuracy of the conversation is proved by eliminating the possibility of erasing the tape-recorded version. A contemporaneous tape record of a relevant conversation is a relevant fact and is admissible under section 7 of the IEA . In *State vs. Mohd. Afzal And Ort*[21] the court held that Computer generated electronic records is evidence, admissible at a trial if proved in the manner specified by Section65BoftheEvidenceAct.

In *State vs. Navjyot Sandhu* [22] the court held that merely because a certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely Sections 63 & 65.

The Supreme Court's finding in Navjot Sandhu case raised uncomfortable questions about the integrity of prosecution evidence, especially in trials related to national security or in high-profile cases of political importance. The state's investigation of the Parliament Attacks was shoddy with respect to the interception of telephone calls. The Supreme Court's judgment notes in prs. 148, 153, and 154 that the law and procedure of wiretaps was violated in several ways.

In Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke, [8]in this case the offence of demanding bribe was sought to be proved by producing a tape-recorded conversation which the Supreme Court found to be inadmissible. In fact, the Directorate of Forensic Science Laboratories, State of Maharashtra had stated in its report that the conversation is not in audible condition and, hence, the same was not considered for spectrographic analysis.[23] The learned counsel for the respondents submitted that the conversation had been translated and the same had been verified by the panch witnesses. Admittedly, the panch witnesses had not heard the conversation, since they were not present in the room. The Supreme Court held that as the voice recorder was itself not subjected to analysis, there was no point in placing reliance on the translated version, having no source for authenticity of the translation. Handling and the subsequent product of decoded evidence is significant to ensure admissibility in the court, it must establish in a reliable and cogent manner the statements produced and must be in accordance with the provisions mentioned in the Evidence and the Information Technology Act.

Anoop Kumar Case[24]

This case involved the admissibility of SMS messages in a criminal case. The court held that digital evidence, including text messages, could be accepted under Section 65B, provided the certification of authenticity was obtained. This landmark case affirmed the legal recognition of digital evidence but highlighted the importance of following the correct procedural requirements.

State of Maharashtra v. Bharat Shanti Lal Shah (2008)[25]

In this case, the Bombay High Court emphasized the need for certification under Section 65B of the Evidence Act. The court ruled that without the appropriate certification, digital evidence such as phone records and SMS messages would not be admissible in court.

The "***Yahoo" Case (2010)***[26]

In this case, the court ordered Yahoo to provide information related to a cybercrime investigation. This case highlighted the challenges of obtaining digital

evidence from international platforms and dealing with data privacy laws in different jurisdictions.

The "***Facebook" Case (2017)***[27]

This case revolved around the admissibility of digital evidence from social media platforms. The court ruled that screenshots and social media posts could be used as evidence if they were appropriately certified, paving the way for social media evidence to be considered in court.

Proposed Solutions for Improving the Handling and Admissibility of Digital Evidence in India:

Strengthening Certification Processes-

To improve the admissibility of digital evidence, there needs to be searer guidelines for the certification process under Section 65B of the Indian Evidence Act. Courts should ensure that digital evidence is accompanied by a detailed and reliable certificate of authenticity. Additionally, training legal professionals and law enforcement personnel in digital forensics and certification requirements is essential.[28]

Establishing Digital Forensic Infrastructure:

India should invest in developing specialized digital forensic labs and training forensic experts. These experts can ensure that digital evidence is properly handled, preserved, and analyzed, thus preserving its integrity and making it admissible in court.

Developing Sear Guidelines for Social Media Evidence

Given the growing importance of social media evidence, sear guidelines need to be established for handling and presenting such evidence in court. Courts must develop protocols for the collection, preservation, and authentication of digital content from social media platforms.

Updating the Legal Framework

Bharatiya sakshya adhiniyam, and the Information Technology Act, 2000, must be updated to more explicitly address the challenges of digital evidence. clear provisions on chain of custody, data privacy, and international jurisdiction would provide a stronger legal foundation for the use of digital evidence in courts.

VIII. CONCLUSION

Digital evidence plays a pivotal role in modern legal proceedings, but its admissibility in Indian courts is hindered by several challenges. By reforming existing laws, strengthening certification processes, investing in digital forensic infrastructure, and ensuring privacy protections, India can address these challenges. The legal framework must evolve to keep pace with the advancements in digital technology, ensuring that digital evidence is effectively used to uphold justice while safeguarding individual rights. As we are gradually moving towards the virtual world, which is an extended version of the real world, every activity involves the generation of an electronic record. In today‘s era, electronic records have become the most crucial piece of evidence in every crime. Therefore, the position of admissibility of such piece of evidence must not remain in ambiguity. Indian Courts have clarified this position from time to time, that the original electronic record, and the computer output, can be produced before the Court as evidence. Whereas, in the case of the computer output, a certificate must be accompanied by it. Opposition can always rebut the same on the ground of genuineness. In such instances, the resort can be made to an examiner of electronic records.

REFERENCES

[1]. Leroux, Olivier. "Legal admissibility of electronic evidence." *International Review of Law, Computers & Technology* 18.2 (2004): 193-220.

[2]. Granja, Fernando Molina, and Glen D. Rodríguez Rafael. "The preservation of digital evidence and its admissibility in the court." *International Journal of Electronic Security and Digital Forensics* 9.1 (2017): 1-18.

[3]. BSA s.2(1)(e) "evidence" means and includes—
(i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence;
(ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence;

[4]. Yeboah-Ofori, Abel, and Akoto Derick Brown. "Digital forensics investigation jurisprudence: issues of admissibility of digital evidence." *Journal of Forensic, Legal & Investigative Sciences* 6.1 (2020): 1-8.

[5]. Thomson, Lucy L. "Mobile devices: New challenges for admissibility of electronic evidence." *SciTech Lawyer* 9.3 (2013): 32.

[6]. Kasper, Agnes, and Eneli Laurits. "Challenges in collecting digital evidence: a legal perspective." *The future of law and eTechnologies* (2016): 195-233.

[7]. OBAMANU, GV. "Legal issues and challenges in the admissibility of digital forensic evidence in courts in Nigeria." *AJIEEL* 8.01 (2023): 96-109.

[8]. https://www.google.com/amp/s/www.businesstoday.in/amp/latest/in-focus/story/new-criminal-law-reform-bills-reflect-new-tech-realities-says-senior-advocate-pinky-anand-410565-2023-12-22

[9]. https://www.dhakalawreview.org/blog/2020/02/admissibility-of-electronic-evidence-drawback-of-an-outdated-evidence-act-4570

[10]. https://www.thedailystar.net/country/barguna-rifat-sharif-murder-key-accused-rifat-farazi-arrested-1766023

[11]. Antwi-Boasiako, Albert, and Hein Venter. "A model for digital evidence admissibility assessment." *Advances in Digital Forensics XIII: 13th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 30-February 1, 2017, Revised Selected Papers 13*. Springer International Publishing, 2017.

[12]. (d) "document" means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records.

[13]. BSA s.61. Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document.

[14]. Admissibility of electronic records. s.63. (1) Notwithstanding anything contained in this Adhiniyam, any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

[15]. Section 57. Primary evidence.
Primary evidence means the document itself produced for the inspection of the Court.
Explanation 1.--Where a document is executed in several parts, each part is primary evidence of the document.
Explanation 2.--Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, each counterpart is primary evidence as against the parties executing it
Explanation 3.--Where a number of documents are all made by one uniform process, as in the case of printing, lithography or photography, each is primary evidence of the contents of the rest; but, where they are all copies of a common original, they are not primary evidence of the contents of the original.
Explanation 4.--Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.
Explanation 5.--Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed.
Explanation 6.--Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence.
Explanation 7.--Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.

[16]. Edward, Elizabeth Ozioma, and Joseph A. Ojeniyi. "A systematic literature review on digital evidence admissibility: methodologies, challenges and research directions." *2019 15th International Conference on Electronics,*

Computer and Computation (ICECCO). IEEE, 2019.

[17]. Vasuki, Prajwal. "A Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence in Criminal Cases." *Part 1 Indian J. Integrated Rsch. L.* 2 (2022): 1.

[18]. Bharati, Rahul, et al. "Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings." *Int J Sci Res Sci & Technol. Jan-Feb-2024* 11.16 (2024): 24-35.

[19]. Edward, Elizabeth Ozioma, and Joseph A. Ojeniyi. "A systematic literature review on digital evidence admissibility: methodologies, challenges and research directions." *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*. IEEE, 2019.

[20]. 1973 1 SCC 471

[21]. 2003 (71) DRJ 178

[22]. AIR 2005 SC 3820

[23]. Harvey, David John. "Digital Evidence Admissibility: Some Issues." *Available at SSRN 3505611* (2019).

[24]. 2019:AHC:75390

[25]. 2008] 12 S.C.R. 1083

[26]. https://indiankanoon.org/doc/626315/

[27]. Meredith, Sam (April 10, 2018). "Facebook-Cambridge Analytica: A timeline of the data hijacking scandal". CNBC. Archived from the original on October 19, 2018

[28]. Vasuki, Prajwal. "A Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence in Criminal Cases." *Part 1 Indian J. Integrated Rsch. L.* 2 (2022): 1.