INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

SCOPE, ADMISSIBILITY, AND CHALLENGES OF ELECTRONIC EVIDENCE

AUTHORED BY - PALLAMREDDY LASYA SRI
B.B.A LLB (9TH SEMESTER)
GITAM School Of Law
GITAM University, Visakhapatnam, Andhra Pradesh

INTRODUCTION:

In an increasingly digital world, electronic evidence has become fundamental to legal proceedings, impacting various fields, including criminal law, civil litigation, and corporate governance. In India, the Information Technology Act of 2000 and the Indian Evidence Act of 1872 have laid the groundwork for the recognition and admissibility of electronic evidence in court. Electronic evidence encompasses a wide range of digital data, such as emails, text messages, social media posts, digital recordings, and data stored in electronic devices, all of which can significantly influence the outcome of legal disputes.[1]

However, integrating electronic evidence into the judicial system presents several challenges. These include issues related to authenticity, integrity, and chain of custody. The rapid evolution of technology also raises questions about the methods used to collect, preserve, and present such evidence in court.[2] Furthermore, the need for uniformity in legal standards and the varying interpretations by courts can complicate the admissibility of electronic evidence, making it imperative for legal professionals to stay abreast of technological advancements and their implications for legal practice.

In India, the admissibility of electronic evidence is governed by specific provisions that require it to meet certain criteria, including relevance and reliability. Courts have established precedents highlighting the importance of proper documentation and verification of electronic

[1] *Marketing Team, Electronic Evidence and Its Admissibility in Court, SIGNATURIT (2023), https://www.signaturit.com/blog/electronic-evidence-and-its-admissibility-in-court/ (last visited Oct 9, 2024).*
[2] *Aditya Mehta Ghosh Arjun Sreenivas, Swagata, Section 65B of the Indian Evidence Act, 1872: Requirements for Admissibility of Electronic Evidence Revisited by the Supreme Court, INDIA CORPORATE LAW (2020), https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/ (last visited Oct 9, 2024).*

 ISSN: 2582-6433

evidence. As technology advances, ongoing legal reforms and judicial interpretations will be essential to address the emerging complexities surrounding electronic evidence, ensuring that it serves its intended purpose in pursuing justice.

WHAT IS ELECTRONIC EVIDENCE?

Electronic or digital evidence encompasses any information stored or transmitted in digital form that can be utilised in legal proceedings. This broad category includes various types of data, such as text-based information (emails, text messages, social media posts, documents, and chat logs), multimedia content (images, videos, audio recordings, and presentations), and metadata (details associated with electronic files like creation dates, modification dates, authorship, file sizes, and locations). Additionally, device data, including call logs, browsing history, GPS information, and app usage, plays a critical role in investigations.[3]

In today's digital landscape, myriad interactions and transactions generate significant electronic trails, making this evidence invaluable for proving or disproving claims and holding individuals or organisations accountable in court. Electronic evidence can be classified into direct evidence, which directly pertains to the facts at issue (such as a recorded confession or incriminating email); indirect evidence, which supports a claim circumstantially (like metadata indicating someone's location at a particular time); and meta-evidence, which provides information about the collection, handling, and analysis of electronic evidence itself.[4]

SCOPE OF ELECTRONIC EVIDENCE:

The scope of electronic evidence in India has evolved significantly due to the increasing reliance on digital communications and technology in everyday life. As society becomes more interconnected through digital platforms, the types of evidence available for legal scrutiny have broadened. This includes traditional forms of documentation and data generated through various digital interactions. For instance, electronic evidence now encompasses cloud-stored documents, online transaction records, and data from Internet of Things (IoT) devices, which can provide valuable insights into behaviour and transactions.[5] This growing electronic

[3] *Manupatra, ADMISSIBILITY OF ELECTRONIC EVIDENCE UNDER THE INDIAN EVIDENCE ACT, 1872, https://articles.manupatra.com/article-details?id=undefined&ifile=undefined (last visited Oct 9, 2024).*
[4] *Ghosh, supra note 2.*
[5] *The Complete Guide To Electronic Records & Evidence In Indian Law - Privacy Protection - Privacy - India, https://www.mondaq.com/india/privacy-protection/1470308/the-complete-guide-to-electronic-records-evidence-in-indian-law (last visited Oct 9, 2024).*

 ISSN: 2582-6433

information repository is vital for establishing facts in legal disputes, as it often serves as the primary source of evidence in cases involving digital interactions.

The legal framework governing electronic evidence in India is primarily defined by the Indian Evidence Act of 1872, particularly Section 65B, which lays down the criteria for admissibility. This section mandates that electronic records must be accompanied by a certificate of authenticity, ensuring that the data presented is relevant and reliable.[6] The framework has been further strengthened by the Information Technology Act of 2000, which recognises electronic documents and addresses cybersecurity and data protection issues. Together, these laws create a robust mechanism for incorporating electronic evidence in court, enabling judges and legal practitioners to navigate the complexities of digital data effectively. The practical implications of this scope are extensive, affecting various sectors such as criminal justice, civil litigation, and corporate governance. In criminal cases, electronic evidence is crucial for tracking activities and establishing timelines, particularly in cases of cybercrime or fraud.[7] Civil disputes can clarify contractual obligations or document interactions between parties. Furthermore, businesses increasingly rely on electronic evidence to comply with regulations and protect intellectual property. As technology advances, the scope of electronic evidence is expected to expand, prompting ongoing legal adaptations to ensure that the judiciary remains equipped to handle new forms of digital evidence effectively.[8]

ADMISSIBILITY OF ELECTRONIC EVIDENCE:

The admissibility of electronic evidence in India is anchored in a well-defined legal framework encompassing various statutes and judicial interpretations. The primary legal instruments governing this area are the Indian Evidence Act of 1872 and the Information Technology Act of 2000.

Indian Evidence Act, 1872

The Indian Evidence Act is the foundational legal document for evidence in Indian courts, establishing the rules for what constitutes admissible evidence. Key provisions related to

[6] *Supreme Court on the admissibility of electronic evidence under Section 65B of the Evidence Act. | India Corporate Law, https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/ (last visited Oct 9, 2024).*
[7] *Vaibhav Chadha & Janani Sivaraman, Critical Analysis of the Law on Admissibility of Electronic Evidence in India, 15 JINDAL GLOBAL LAW REVIEW 119 (2024).*
[8] *Team, supra note 1.*

 ISSN: 2582-6433

electronic evidence include:

Section 65B:

Before 2000, electronic evidence in India was classified as primary or secondary evidence based on Sections 61 to 65 of the Indian Evidence Act, 1872.[9] When the original document was presented in court, it was deemed primary evidence. When the original could not be produced, the procedure outlined in Section 65 had to be followed to introduce the electronic evidence.

After the enactment of the Information Technology Act in 2000, electronic evidence began to be governed by Sections 65A and 65B of the Indian Evidence Act.[10] These sections provided a more transparent framework for admitting electronic records. However, challenges arose regarding the certificate requirement when presenting electronic evidence, leading to conflicts and uncertainties in legal proceedings.

Section 65 of the Indian Evidence Act of 1872 significantly expands the scope of admissible evidence to include electronic records. This section stipulates that any information produced, recorded, and transferred using an electronic device capable of creating, storing, and transmitting such data is considered admissible as evidence in legal proceedings.[11] The provision recognises the critical role that electronic data plays in modern communication and transactions, thus treating it with the same legal validity as traditional documents.

According to this section, information recorded in electronic form qualifies as a document. This classification means that electronic records, such as those found on computers, mobile devices, and other digital platforms, are afforded the same evidentiary weight as paper documents, provided they meet specific requirements regarding authenticity and relevance.[12] This legal acknowledgement is crucial in an era where much of our daily interactions and transactions occur digitally, reflecting the need for the law to adapt to contemporary practices. Numerous examples illustrate the types of electronic records that fall under this ambit. For instance, cell phones can hold vital evidence through text messages, call logs, and multimedia

[9] *Manupatra, supra note 3.*
[10] *MODE OF PROOF OF ELECTRONIC EVIDENCE.*
[11] *Rachit Garg, Admissibility and Evidentiary Value of Electronic Records, IPLEADERS (Apr. 8, 2021), https://blog.ipleaders.in/admissibility-evidentiary-value-electronic-records/ (last visited Oct 9, 2024).*
[12] *Team, supra note 1.*

 ISSN: 2582-6433

content. Computers store digital files, including documents, emails, and software data, which can be pivotal in legal matters. Financial transactions recorded through ATM receipts, debit and credit card statements, and online banking records are also admissible as electronic evidence. Moreover, digital communications such as emails and SMS provide essential context in establishing timelines or intent between parties. Additionally, records like IP addresses and internet browsing history can help trace online activities, while CCTV footage is a critical visual record in criminal and civil cases.

Section 65B outlines the requirements related to electronic devices and the circumstances under which electronic evidence is recorded. It also specifies the conditions these devices must meet during the recording process.[13] Sub-Section 1 of Section 65B defines what constitutes computer output. When read in conjunction with Section 2 of the Information Technology Act of 2000, it can be inferred that any electronic device capable of storing, processing, and transmitting information, such as computers, mobile phones, tape recorders, or video recorders, can be categorised as an electronic device.[14] Collectively, these devices are referred to as "computer output."Additionally, the certificate should address other requirements as specified in Sub-Section 2 of Section 65B of the Act to ensure the admissibility of electronic evidence in legal proceedings.

Any information in an electronic record that is printed on paper, stored, recorded, or copied on optical or magnetic media generated by a computer is considered a document. These documents can be admitted as evidence without the need to produce the original, provided that the owner or the individual responsible for the computer issues a certificate under Section 65B (4) of the Indian Evidence Act of 1872. This certificate must confirm:[15]

- The operational condition of the computer at the time the evidence was recorded.
- The lawful usage of the computer by its owner or operator.
- An explanation of how the computer is typically utilised.
- If information is entered into another computer as part of standard activities, a description of this process.

[13] *Ghosh, supra note 2.*
[14] *Critical analysis of the law on admissibility of electronic evidence in India | Jindal Global Law Review, https://link.springer.com/article/10.1007/s41020-024-00219-1 (last visited Oct 9, 2024).*
[15] *Indian Evidence Act, 1872, §65B(4).*

 ISSN: 2582-6433

- The operational status of the computer throughout the entire period when the information was processed, created, or transferred.
- If multiple computers were used to generate or process the information, a description of all these computers could be treated as a single unit for this evidence.

In interpreting Section 65B, the court differentiates between using certificates in civil and criminal cases. In civil proceedings, if a party fails to provide a required certificate or presents a defective one despite a request to the relevant authority, the trial judge can summon the individuals involved and compel them to furnish the necessary certificate. This is crucial when electronic records are submitted as evidence without the appropriate certification.

According to Section 65B (4), in conjunction with Sections 207, 91, and 311 of the Criminal Procedure Code (CrPC), electronic evidence must be presented before the trial begins.[16] However, the court has the discretion to allow the submission of such evidence at a later stage, as long as it is before the conclusion of the trial.

Electronic records stored on CDs, VCDs, chips, and similar media must be accompanied by a certificate obtained when the evidence is collected, as stipulated by Section 65B.[17] Without this certificate, any secondary evidence related to the electronic record is deemed inadmissible in court.

Sections 61-90:[18]

These sections outline the general principles of evidence, including the requirements for relevance and hearsay prohibition. They also apply to electronic evidence, emphasising the necessity of establishing the authenticity and relevance of all evidence presented in court.

Information Technology Act, 2000:[19]

The Information Technology Act complements the Indian Evidence Act by providing specific legal recognition for electronic documents and transactions. Key aspects include;[20]

[16] *Admissibility of Electronic Record in India, https://articles.manupatra.com/article-details/Admissibility-of-Electronic-Record-in-India (last visited Oct 9, 2024).*
[17] *Chadha and Sivaraman, supra note 7.*
[18] *Indian Evidence Act, 1872*
[19] it_act_2000_updated.pdf, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last visited Oct 9, 2024).
[20] *Team, supra note 1.*

 ISSN: 2582-6433

- Legal Recognition of Electronic Records: The Act recognises electronic documents as legally valid, equating them with traditional paper documents. This is crucial for establishing the admissibility of digital evidence in legal proceedings.
- Digital Signatures: The Act also provides for the use of digital signatures, which can enhance the authenticity and integrity of electronic records. A valid digital signature can serve as proof of the origin and integrity of the document.
- Cybercrime and Data Protection: The Act addresses issues related to cybercrime and data protection, establishing legal protocols for handling electronic evidence in cases involving digital offences. This includes provisions for the secure storage and transmission of electronic data.

Authentication of Electronic Records:

Section 3 of the IT Act deals with the authentication of electronic records. It specifies that the originator can authenticate any electronic record using a digital signature. This provision ensures that electronic documents are verifiable and linked to the individual or entity that created them, enhancing the reliability and security of electronic communications. By requiring digital signatures, Section 3 helps prevent unauthorised modifications and fraud, fostering trust in electronic transactions.

Electronic Signature:

Section 3A specifically addresses electronic signatures. It defines what constitutes an electronic signature and emphasises that it has the same legal validity as traditional handwritten signatures. This section allows individuals and entities to use electronic signatures in transactions, streamlining processes and promoting digital methods for executing agreements and documents. By recognising electronic signatures as legally binding, Section 3A supports the growth of e-commerce and digital transactions.

Legal Recognition of Electronic Records:

Section 4 establishes that electronic records shall not be denied legal effect, validity, or enforceability merely because they are in electronic form. It lays the foundation for considering electronic documents on par with traditional paper documents, facilitating the acceptance of electronic evidence in legal proceedings.

 ISSN: 2582-6433

Legal Recognition of Electronic Signatures:

Section 5 asserts that electronic signatures (or digital signatures) shall be deemed valid and equivalent to handwritten signatures. This provision is crucial for establishing the authenticity of electronic records, ensuring that digital transactions are secure and legally binding. It encourages the use of digital signatures in various legal and commercial contexts.

Validity of Contracts:

This section confirms that contracts formed through electronic means are legally enforceable. Section 10A addresses concerns regarding the validity of online agreements, thereby promoting e-commerce and digital transactions. By affirming the legality of electronic contracts, this section enhances the acceptance of electronic evidence in contractual disputes.

Attribution of Electronic Records:

Section 11 discusses the attribution of electronic records, stating that the originator of an electronic record is the person who sends it. This section clarifies the liability and responsibilities associated with electronic communications, which is essential in cases where the authenticity of the evidence is questioned.

Use of Electronic Records:

Section 15 permits the use of electronic records in various situations, provided they comply with the relevant provisions of the Act. This flexibility encourages using digital formats in legal and commercial practices, thus promoting efficiency.

The rise of digital transactions in India, driven by initiatives like the Jan Dhan Yojana, the Digital India mission, direct benefit transfers, mobile banking, and various government e-services, underscores the need for robust legal frameworks concerning electronic records.[21] Given the increasing accuracy and reliance on electronic documents, it has become essential to formulate laws governing electronic signatures and related documentation to prevent fraudulent activities associated with these records. To address these concerns, the Information Technology Act of 2000 introduced Sections 65A and 65B into the Indian Evidence Act of 1872, specifically focusing on the admissibility of electronic evidence. These sections outline the legal framework for incorporating electronic records into judicial processes.

[21] *Supreme Court on the admissibility of electronic evidence under Section 65B of the Evidence Act. | India Corporate Law, supra note 6.*

 ISSN: 2582-6433

Definitions of key terms such as "electronic record," "computer," and "computer network" can be found in Section 2 of the Information Technology Act of 2000. The Act defines a computer system as a device or a collection of devices that includes input devices (like keyboards and mice), output devices (such as monitors and printers), and support devices.[22] These components work with external file formats (like MP3, MP4, Word, and PDF) to handle computer programs, electronic instructions, and input and output data. Additionally, any device capable of performing logical operations, arithmetic functions, data storage and retrieval, communication control, and other relevant tasks falls under the definition of a computer. Thus, Sections 65A and 65B can be effectively interpreted within the broader context of the Information Technology Act, providing a comprehensive understanding of electronic evidence in India.

JUDICIAL INTERPRETATION:

Indian courts have played a pivotal role in interpreting the provisions of the Indian Evidence Act and the Information Technology Act concerning electronic evidence. Landmark judgments have clarified critical aspects of admissibility:

Anvar P.V vs P.K. Basheer[23]

The case centres around allegations of corrupt practices during an election by the winning candidate. The complainant sought to invalidate the election results and submitted CDs containing speeches, songs, and announcements as evidence to support his claims. However, he failed to obtain the necessary certificate required under Section 65B (4) of the Indian Evidence Act for the admissibility of electronic records.

In this case, a three-judge bench of the Supreme Court examined the provisions of Section 65B (4) to determine the admissibility of the electronic evidence presented. The section outlines specific conditions for introducing electronic records in court. These conditions include the necessity of a certificate affirming the electronic record's authenticity, a description of how the electronic record was obtained, details about the device used to produce the record, compliance with the requirements outlined in Section 65B (2) of the Evidence Act; and the signature of an individual holding a responsible official position related to the operation of the relevant device.

[22] *Admissibility and evidentiary value of electronic records - iPleaders, https://blog.ipleaders.in/admissibility-evidentiary-value-electronic-records/ (last visited Oct 9, 2024).*
[23] *2014 10 SCC 473*

 ISSN: 2582-6433

The court acknowledged the inherent risks of electronic evidence, noting that it can easily be tampered with or altered. Therefore, it emphasised the importance of taking necessary safeguards when the outcome of a trial relies on electronic records. The ruling underscored that a certificate is essential for electronic evidence, and it must clearly state that the information is accurate to the best of the presenter's knowledge and belief. This approach was adopted to ensure the authenticity and reliability of the electronic records presented in court.

The court determined that for the admissibility of CDs, VCDs, and electronic chips as evidence, a certificate under Section 65B of the Indian Evidence Act must be submitted. With this certificate, electronic evidence can be accepted by the court. The reliability of electronic evidence presented in CDs, VCDs, or electronic chips is contingent upon proper certification of the secondary evidence by the court.[24]

Sections 65A and 65B specifically govern the admissibility of secondary evidence through electronic records, meaning that the provisions of Sections 63 and 65 are not applicable in this context. The court held that Sections 65A and 65B create a "complete code" regarding the admissibility of information in electronic records. Until the conditions specified in Section 65B are met, electronic records presented as secondary evidence should not be accepted unless accompanied by a written certificate under Section 65B (4). The court further clarified that the Evidence Act does not allow for the proof of an electronic record through oral testimony if the requirements of Section 65B are not satisfied.[25] However, if an electronic record is utilised as primary evidence under Section 62, it can be admitted without adhering to the conditions outlined in Section 65B.

Tomaso Bruno & Anr vs State Of Uttar Pradesh[26]

In this case, the Supreme Court emphasised that "with the advancement of information technology, a scientific approach must permeate investigative methods at both individual and institutional levels." The increasing reliance on electronic evidence reflects the growing influence of technology in daily life, making electronic documents recognised as material evidence in legal proceedings.

[24] *Critical analysis of the law on admissibility of electronic evidence in India | Jindal Global Law Review, supra note 14.*
[25] *Ghosh, supra note 2.*
[26] *(2015) 7 SCC 178.*

 ISSN: 2582-6433

The apex court noted that if electronic records are proven by the stipulations of Section 65B of the Evidence Act, and if the conditions outlined in sub-section (2) of that section are satisfied, computer-generated electronic records can be accepted as evidence in trials. The judgment correctly establishes this legal principle. However, when the court stated that secondary evidence regarding the contents of a document could also be admitted under Section 65 of the Evidence Act, it contradicted the provisions of Section 65B and needed to be revised.[27] In the case context, the electronic records, such as CCTV footage and call records, were not submitted or relied upon.

Shafhi Mohammad vs. State of Himachal Pradesh[28]

In this case, the Supreme Court addressed whether video graphic evidence from a crime scene or recovery site is crucial for establishing the credibility of collected evidence. To answer this question, the court interpreted Section 65B(4) of the Evidence Act, 1872, which outlines the procedural requirements for the admissibility and certification of digital evidence.

The Supreme Court acknowledged the benefits of modern methods of evidence collection, citing precedents from cases such as Ram Singh and Ors. v. Col. Ram Singh[29] and English judgments in R. v. Maqsud Ali and R. v. Robson. These cases emphasised that disregarding the advantages of electronic records would undermine the legitimacy of evidence. While caution must be exercised in evaluating evidence, the court noted that relevant electronic evidence should not be excluded from admissibility.[30]

The court clarified that Sections 65A and 65B are procedural provisions, and the acceptance of evidence ultimately depends on the case's specific facts and whether the individual presenting the evidence can provide the necessary certificate under Section 65B (4). It also highlighted that these sections should be viewed as partial regarding the admissibility of electronic evidence. Definitions of 'document' from Section 3 of the Evidence Act and electronic records from Section 2(1)(t) and 2(1)(o) of the Information Technology Act, 2000 are considered to understand the nature of electronic evidence better.

---

[27] *ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT PROCEEDINGS, https://www.taxmanagementindia.com/visitor/detail_article.asp?ArticleID=11092 (last visited Oct 9, 2024).*
[28] *(2018) 2 SCC 801.*
[29] *AIR 1986 3 SCR SUPL. (2) 399*
[30] *Critical analysis of the law on admissibility of electronic evidence in India | Jindal Global Law Review, supra note 14.*

 ISSN: 2582-6433

Furthermore, the court noted that while the certificate under Section 65B (4) is not always mandatory, it is procedural. A person not possessing the device from which the document is produced cannot be compelled to provide a certificate.[31] The court asserted that the requirements of Sections 63 and 65 remain applicable if the individual does not possess the device used to produce the electronic evidence.

Arjun Pandit Rao v. Kailash Kushanrao[32]

Facts:

The case involved a dispute over the legitimacy of electronic records submitted as evidence in a civil suit concerning a property transaction. The appellant, Arjun Pandit Rao, challenged the validity of certain documents produced by the respondent, Kailash Kushanrao, which included email communications and electronic signatures related to the property sale agreement. The main contention was whether these electronic documents met the requirements under Section 65B of the Indian Evidence Act for admissibility in court. The appellant argued that the respondent must provide a proper certificate under Section 65B (4) for electronic records to be accepted as evidence.

Issues:

1. Whether the electronic documents submitted by the respondent were admissible under the Evidence Act without a certificate as required by Section 65B (4).
2. The interpretation of the procedural requirements for the admissibility of electronic evidence.
3. The impact of technological advancements on the admissibility and evaluation of electronic evidence in legal proceedings.

Judgment:

The Supreme Court ruled in favour of the respondent, holding that the electronic documents in question were admissible. The court emphasised that while Section 65B provides a procedural framework for the admissibility of electronic evidence, it should not be interpreted in a manner that excludes relevant and authentic evidence due to procedural lapses. The court observed that:

[31] ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT PROCEEDINGS, *supra* note 27.
[32] *AIR 2020 SC 4908*

 ISSN: 2582-6433

- The requirement for a certificate under Section 65B (4) should not be seen as an absolute barrier to admitting electronic evidence. If the authenticity of the electronic record can be established through other means, its admissibility may still be upheld.
- The court recognised the importance of adapting legal standards to accommodate the realities of modern technology and the growing prevalence of electronic communications in legal matters.
- It highlighted that strict adherence to procedural requirements should uphold the pursuit of justice, especially when relevant evidence is available.

The court ultimately directed that the electronic records submitted by the respondent, including the emails and signatures, should be admitted as evidence, setting a precedent for the flexibility required in evaluating electronic proof in light of technological advancement. This case is significant for its interpretation of the admissibility of electronic evidence under the Indian Evidence Act, particularly regarding Section 65B. It underscores the necessity of balancing procedural requirements with ensuring that relevant and authentic evidence is not excluded merely due to technicalities. The ruling highlights the court's recognition of the evolving nature of evidence in the digital age and its implications for legal proceedings.

ELECTRONIC EVIDENCE AND BHARATIYA SAKSHYA ADHINIYAM, 2023:

The Indian Evidence Act, 1872 (IEA) has been replaced by the Bharatiya Sakshya Adhiniyam, 2023 (BSA), marking a significant step toward modernising India's judicial system. This new legislation seeks to update, streamline, and simplify how courts present and interpret evidence.[33] However, the fundamental principles regarding evidentiary standards remain intact despite these changes. The integrity, chain of custody, and impartiality of evidence remain paramount, as the Hon'ble Supreme Court has frequently highlighted concerns over how easily electronic records can be altered.

Recognising these concerns, the BSA incorporates safeguards to ensure the reliability of digital evidence while embracing modern technology. It also retains the core legal principles of the IEA. One fundamental change is the expanded definition of "evidence" under the BSA's Section 2(e). This now includes "statements given electronically," in addition to those made by

[33] *Bhartiya Sakshya Adhiniyam, 2023 - A Dynamic Shift to the Digital Era - ELP Law, ECONOMIC LAWS PRACTICE, https://elplaw.in/leadership/bhartiya-sakshya-adhiniyam-2023-a-dynamic-shift-to-the-digital-era/ (last visited Oct 9, 2024).*

 ISSN: 2582-6433

witnesses about matters under inquiry, as defined in Section 2(e)(i). Such statements are now categorised as oral evidence under the new law.[34]

This differs from Section 3(1) of the IEA, which defined oral evidence solely as statements made by witnesses that the court permits or requires about matters under inquiry. The inclusion of "statements given electronically" under Section 2(e)(i) aligns with broader changes introduced by the Bhartiya Nyaya Sanhita, 2023 (BNSS), which now allows various legal processes such as the issuance, service, and execution of summons and warrants, witness examination, recording of evidence, and appellate proceedings to be conducted electronically through audio-visual means or other electronic communication methods.

The definition of documentary evidence under the Bharatiya Sakshya Adhiniyam, 2023 (BSA) has been expanded to include digital and electronic records. The term "document" has also been redefined to encompass these records. An illustrative example has been added to clarify that electronic records, such as emails, server logs, documents stored on computers, laptops, smartphones, messages, websites, locational data, and voice mail messages saved on digital devices, are now considered documents under the law.[35]

These changes have been made in response to the corresponding amendments in the Bhartiya Nyaya Sanhita, 2023 (BNSS), which now requires audio-video recordings in specific circumstances, including:

- Videography during evidence collection at crime scenes for offences punishable by seven years or more;
- Videography during search and seizure operations;
- In cases involving victims of sexual offences, particularly when the victim has a physical or mental disability.

To facilitate the admission of electronic and digital records into evidence, Section 57 of the BSA has been revised to include several clarifications regarding primary evidence:[36]

- When an electronic or digital record is created or stored across multiple files (simultaneously or sequentially), each is considered primary evidence.

[34] *Electronic Evidence under Bhartiya Sakshya Adhiniyam, 2023,* DRISHTI JUDICIARY, *https://www.drishtijudiciary.com/to-the-point/bharatiya-sakshya-adhiniyam-&-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023 (last visited Oct 9, 2024).*
[35] *Id.*
[36] *Id.*

 ISSN: 2582-6433

- If an electronic or digital record is produced from proper custody, it will be regarded as primary evidence unless its authenticity is contested.
- When a video recording is stored electronically and transmitted, broadcast, or transferred elsewhere, each copy is treated as primary evidence.
- In the case of electronic or digital records stored across multiple locations or in automated temporary files on a computer resource, each storage instance qualifies as primary evidence.

These provisions clarify what constitutes primary evidence in the context of electronic and digital records.

Section 57 further states that an electronic or digital record from proper custody qualifies as primary evidence. Additionally, Section 80 of the BSA presumes the authenticity of certain official documents, such as those purporting to be the Official Gazette, newspapers, journals, or any document required by law to be kept, provided it is kept in the form mandated by law and comes from proper custody.

Section 61 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) states that electronic or digital records cannot be deemed inadmissible as evidence, provided that the conditions outlined in Section 63 are satisfied. One of the critical requirements introduced under sub-section 4 of Section 63 is the need for expert certification. This provision adds a layer of accountability, ensuring that statements made electronically, audio or video, are subject to scrutiny before being admitted as evidence. This certification process strengthens the reliability of electronic records and enhances their credibility in legal proceedings.

CHALLENGES:

Electronic evidence presents several challenges in legal contexts, impacting its collection, preservation, and admissibility.[37] Here are some key challenges:

1. Authentication and Integrity: Establishing the authenticity of electronic evidence can be difficult. Digital files can be easily altered or tampered with, raising questions about their integrity. Courts require robust mechanisms to verify that the evidence presented is genuine and has not been modified.

[37] Chadha and Sivaraman, *supra* note 7.

 ISSN: 2582-6433

2. Compliance with Legal Standards: The requirements for the admissibility of electronic evidence, such as those outlined in Section 65B of the Indian Evidence Act, can be complex. Parties may need help to meet the procedural requirements, including the need for certificates confirming the authenticity of electronic records.
3. Data Privacy and Confidentiality: The collection of electronic evidence often involves sensitive personal or proprietary information. Balancing the need for evidence with privacy concerns can lead to legal dilemmas, especially in jurisdictions with strict data protection laws.
4. Chain of Custody: Maintaining a transparent chain of custody is crucial for the admissibility of electronic evidence. Any break in the chain, such as improper handling, storage, or transfer, can undermine the evidence's credibility.
5. Technical Expertise: Judges, lawyers, and juries may need more technical knowledge to understand electronic evidence fully. This gap can lead to misinterpretation or undervaluation of such evidence in legal proceedings.
6. Interoperability and Compatibility: Different devices, software, and formats can complicate the retrieval and presentation of electronic evidence. Ensuring compatibility among various technologies is essential for effective evidence management.
7. Evolving Technology: Rapid technological advancements can outpace existing legal frameworks, leading to uncertainties about how new types of electronic evidence (such as social media content or cloud storage data) are treated in court.
8. Cost and Resource Constraints: The collection, preservation, and analysis of electronic evidence can be resource-intensive. Smaller firms or individuals may need help in affording the necessary technology and expertise to handle electronic evidence effectively.
9. Jurisdictional Issues: Electronic evidence often crosses geographical boundaries, leading to jurisdictional challenges. Different laws governing electronic evidence in various jurisdictions can complicate cases involving international elements.
10. Volume and Complexity: The sheer volume of electronic data can be overwhelming. Identifying, extracting, and analysing relevant evidence can be complex and time-consuming in cases involving extensive digital communication or large datasets.
11. Data Loss and Corruption: Electronic evidence can be susceptible to data loss due to hardware failure, accidental deletion, or corruption. This risk makes implementing effective backup and preservation strategies to safeguard proof crucial.

 ISSN: 2582-6433

12. Social media and Digital Footprints: Evidence collected from social media and online interactions poses unique challenges. Issues of authenticity, context, and user privacy can complicate the use of such evidence in court.
13. Ethical Considerations: The methods used to collect electronic evidence can raise ethical concerns, especially if they involve invasive techniques or violate privacy rights. Legal practitioners must navigate these ethical dilemmas carefully.

CONCLUSION:

The scope of electronic evidence has transformed the legal landscape, opening new avenues for establishing facts and enhancing the efficiency of judicial proceedings. However, this evolution is accompanied by significant challenges that demand careful consideration. Issues of authentication, integrity, and compliance with legal standards pose critical hurdles that legal professionals must navigate to ensure that electronic evidence is reliable and admissible.

As technology advances, the legal framework must evolve in tandem, adapting to the complexities of digital data while safeguarding individual rights and maintaining the integrity of the judicial process. By fostering a robust understanding of the admissibility requirements and addressing the inherent challenges, the legal system can leverage electronic evidence to uphold justice effectively.

A collaborative effort among lawmakers, legal practitioners, and technology experts is essential in this dynamic environment. By embracing innovation and promoting continuous education, we can harness the full potential of electronic evidence, ensuring that it serves as a powerful tool for truth and accountability. Ultimately, adapting to these changes will strengthen the legal system and enhance public trust in its capacity to deliver justice in the digital age.

BIBLIOGRAPHY:

Websites:

- https://www.mondaq.com/india/privacy-protection/1470308/the-complete-guide-to-electronic-records-evidence-in-indian-law
- https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/

 ISSN: 2582-6433

- https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/
- https://ijcrt.org/papers/IJCRT2205188.pdf
- electronic_records_article.pdf (tn.gov.in)
- https://www.drishtijudiciary.com/to-the-point/bharatiya-sakshya-adhiniyam-&-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023
- https://www.signaturit.com/blog/electronic-evidence-and-its-admissibility-in-court/
- https://doi.org/10.1007/s41020-024-00219-1
- https://elplaw.in/leadership/bhartiya-sakshya-adhiniyam-2023-a-dynamic-shift-to-the-digital-era/
- https://articles.manupatra.com/article-details?id=undefined&ifile=undefined
- https://www.taxmanagementindia.com/visitor/detail_article.asp?ArticleID=11092
- https://blog.ipleaders.in/admissibility-evidentiary-value-electronic-records/