A COMPREHENSIVE ANALYSIS OF ADMISSIBILITY OF DIGITAL EVIDENCE IN THE INDIAN LEGAL SYSTEM

Prity Kumari Suman[1]

Introduction

Human civilizations have kept progressing consistently, and their consistent efforts have led to consequent discoveries and innovations. With the passage of time, humans have invented fire to get into space; one of them is information technology and the Internet, which connects people worldwide through the web. In science and technological development, the cyberspace, which is one of the results of the development of information technology, is also not free from the threat of being misused. Being the fastest medium and having a diversity of contents to spread, it is closer to the risk of misuse and a threat to society.[2]

In the contemporary world of advanced technology, not only India but the entire world is fascinated by cyberspace. Technology has provided an upgraded version to each and every sector because of its availability with just a swipe of the fingertips. As per the increasing dependence on the internet, there has been an increase in the tendency to use electronic means for communication, online business, transactions, and the storage of data in a computerized structure. Online data storage and cyberspace have called up the necessity of transforming the rules of admissibility of electronic evidence in the legal field of India.

The number of cyber cases is increasing day by day, and the best part is that they are also getting registered, but for an effective investigation of these cases and for further prosecution, primary evidence is extracted from the computers and cyberspaces. These evidences are in computerized structure and are termed digital evidence, and their proper collection is a herculean task that requires actual expertise in cyber technology. Digital evidence does not only mean the evidence found in computers; it also includes the evidence shared with computerized gadgets.[3] It extends to the visual and sound devices. Every shared audio and

[1] Prity Kumari Suman, B.A.LL.B. (Hons), School of Law & Governance, Central University of South Bihar
[2]Lallie, H.S., 2012. An overview of the digital forensic investigation infrastructure of India. *Digital Investigation*, *9*(1), pp.3-7.
[3] Janaki, M.C., 2016. Digitalization of investigation and detection of crime. *Digital India: Rhetoric Versus Reality*, pp.130-143.

visual message, email, photo, ATM transaction log, history of UPI transactions, archives, posts, word processing, and text narratives. Digital audio and video recordings, Web program history, saved documents, spread sheets, documents related to accounts, GPS tracking, computer memory contents, and printouts.

In the context of digital evidence and cyberspace, cyber forensics is also one of the sub-branches of digital evidence that is significant in criminal cases. The art and science of collecting computerized structured evidence are very significant as an aid in all kinds of cases but have also raised multiple legal issues in India. In this paper, we will understand the admissibility of digital evidence in courts.

Historical Background of Digital Evidence in India

The history of digital evidence can be traced back to the 20th century; it started with the rapid increase in digital technologies. It was equivalently proportional to the proliferation of digitization, so as per the increasing reliance on computers and cyberspace, the legal system also needs to address the challenges arising with the digital age and the admission of digital evidence.[4]

If we get into the historical development of legislation for the admissibility of digital evidence, the first legislation that laid the foundation of digital evidence was the Information Technology Act, 2000 (India). It was recognizing the digital evidence and tackling the offenses related to cybercrime. In 2002, the Indian Evidence Act, 1872, was amended. In this amendment, two sections were introduced to deal with digital evidence specifically. Sections 65A and 65B are the two sections that deal with digital evidence. Section 65A of the Indian Evidence Act deals with special provisions for considering digital evidence as evidence, and Section 65B deals with the admissibility of digital evidence through deeming fiction.

Further, in 2023, under the Bharatiya Sakshya Bill (BSB), the Indian Evidence Act, 1872 (IEA) will be replaced. It retains most provisions of the Indian Evidence Act; one of them is electronic evidence. Section 61 of Bharatiya Sakshya Adhiniyam deals with the admissibility of digital evidence. It also says that digital records and such records shall be subject to Section 63, and all these documents have the same legal effect, validity, and enforceability as other legal

[4] Karia, T., Anand, A. and Dhawan, B., 2015. The Supreme Court of India re-defines admissibility of electronic evidence in India. *Digital Evidence & Elec. Signature L. Rev.*, *12*, p.33.

documents. Section 62 supporting it states that all the contents of electronic records may be proved according to the provisions of Section 63. Moving further, Section 63 outlines that any information contained in an electronic record that is printed on paper, stored, recorded, or copied in optical or magnetic media or semiconductor memory that is produced by a computer or any communication device or otherwise stored, recorded, or copied in any electronic form (here it is referred to as the computer output). Above mentioned all shall be deemed to be a document as other documents.[5] For an electronic record to be directly admissible, it needs to satisfy the conditions mentioned in this section. Such documents do not require proof of the original, as evidence, or any contents of the original of the computer in question. We will understand those conditions further.

Literature Review

The book by Powell (et al. 2018)[6] offers a comprehensive overview of the legal framework governing digital evidence in India, specifically addressing its implications for corruption cases. The author meticulously examines the provisions of the BSA and the Information Technology Act, emphasizing how these laws have evolved to accommodate the rise of digital communication. The author illustrates various case studies to demonstrate the practical challenges faced by law enforcement agencies in collecting and preserving digital evidence. This book serves as a foundational text, highlighting both the potential of digital evidence to uncover corrupt practices and the need for legal reforms to address existing procedural shortcomings.

The book by Katsh (et al. 2017)[7] delves into the intersection of technology and corruption, providing an in-depth analysis of how digital tools can both facilitate and combat corrupt practices. The author discusses the role of digital evidence in enhancing transparency and accountability in governance, particularly in politically sensitive environments like India. By exploring empirical case studies, the book illustrates how digital evidence can be instrumental in prosecuting corruption cases, while also highlighting the ethical and legal dilemmas that arise in its use. This work offers a balanced perspective on the advantages and challenges posed

[5] Popova, E.I., 2023. Impact of Digital Technologies on Criminal Procedure in Russia and India: Comparative Legal Aspect. *Int'l JL Changing World*, *2*, p.52.
[6] Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. Routledge.
[7] Katsh, E., & Rabinovich-Einy, O. (2017). *Digital justice: technology and the internet of disputes*. Oxford University Press.

by digital evidence in the realm of political corruption.

The paper by Jain (et al. 2020)[8] investigates the legal challenges associated with the admissibility of digital evidence in Indian courts. The author analyzes various judicial precedents to assess how the courts have interpreted the provisions of the BSA, particularly Section 63. The paper highlights the discrepancies between legal theory and practice, demonstrating how inconsistent application of legal standards can impact the prosecution of political corruption cases. The findings underscore the need for clearer guidelines and training for legal practitioners to ensure that digital evidence is effectively utilized in court.

The research paper by Granja (et al. 2017)[9] focuses on the procedural challenges faced by law enforcement agencies when collecting digital evidence. The author discusses the technical complexities involved in accessing and preserving electronic records, emphasizing the lack of resources and training within investigative bodies. By presenting case studies of political corruption investigations, the paper illustrates how procedural lapses can lead to the inadmissibility of crucial evidence, ultimately hindering justice. The author advocates for the development of specialized units within law enforcement agencies to enhance their capacity to handle digital evidence.

The paper by Losavio (2018)[10] explores the ethical implications of using digital evidence in corruption cases, particularly concerning privacy rights and data protection. The author examines the balance between the necessity of investigating corrupt practices and the protection of individual rights, highlighting the potential for misuse of digital evidence in politically charged environments. The paper calls for a more nuanced approach to digital evidence, advocating for legislative reforms that address privacy concerns while enabling effective investigations into corruption.

Research Questions

1. What are the legal frameworks governing the admissibility of digital evidence in India?

[8] Jain, N., & Srinivas Reddy, S. (2020). Admissibility of Electronic Evidence in India: An Overview. *Nyaayshastra L. Rev.*, *1*, 1.
[9] Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1-18.
[10] Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and Privacy*, *1*(3), e23.

2. What procedural challenges do law enforcement agencies face in the collection and preservation of digital evidence?

3. How have judicial interpretations influenced the use of digital evidence in India?

4. What ethical considerations arise from the use of digital evidence in investigations of cases?

Hypothesis

The hypothesis of this research posits that while digital evidence is a valuable tool in combating political corruption in India, significant legal and procedural challenges hinder its effective use in court. The hypothesis will be partially proven, as the research will highlight existing challenges and identify areas for improvement while acknowledging instances where digital evidence has successfully contributed to the prosecution of corruption cases.

Research Methods

This study will adopt a doctrinal research approach, focusing on analyzing legal texts, case law, and scholarly articles related to the use of digital evidence in political corruption cases. The research will involve a comprehensive review of the BSA and the Information Technology Act, examining relevant provisions that govern the admissibility and handling of digital evidence.

Additionally, a case law analysis will be conducted to assess how courts in India have interpreted and applied these legal frameworks in political corruption cases. This will include reviewing landmark judgments to identify trends in judicial reasoning and the implications for law enforcement practices.

Qualitative research methods, including interviews with legal practitioners, law enforcement officials, and experts in digital forensics, may also be employed to gather insights into the practical challenges and ethical considerations faced in the field. By synthesizing these sources, the research aims to provide a holistic understanding of the role of digital evidence in political corruption cases and propose recommendations for legal reform and improved practices

Analysis

Understanding Digital Evidence

To understand Evidence, we need to dive into the various conceptions regarding the word Evidence. A very general concept to be considered is that it is derived from the Latin word "Evidentia" which means clear evident, plain or at the stage of being evident. It is also argued that it means to prove or to make clear and plain, as it is derived from evident evidere. If we refer to the Oxford English Dictionary to understand the concept of Evidence it is "the available body of facts or information indicating whether a belief or proposition is true or valid".

Delving further into the concepts of this paper, we will look at what is digital evidence and how it is defined. In this modern-techno world, we are all over surrounded with devices and digital gadgets and these are the sources of digital evidences. When we talk about digital evidence, peoples in general thinks that information carried and shared through cell phones, computers or via internet shared contents are only digital evidence, but in reality it is very wide. For an example, if an automated Vaccum cleaner have the capacity to transfer and exchange messages then any information shared through it is considered as digital evidence. If any illegal message or image is shared through it then it will be also regulated as per Bharatiya Sakshya Adhiniyam, 2021.

According to Section 57 of Bharatiya Sakshya Adhiniyam, 2021 Digital and Electronic records is wide and it includes how digital records are treated as primary evidence. This new Act allows the use of digital records in document and it widely covers the digital document, emails, maps, text messages, server logs, files which are stored in any devices, contents from websites, data related to location, etc.

Digital evidence is also understood as information and data of value to an investigation that is stored on, received or transmitted by an electronic device.

Legal Framework Governing Digital Evidence in India

The legal framework governing digital evidence in India is primarily anchored in the Bharatiya Sakshya Adhiniyam (2023), which has been enacted to incorporate provisions relevant to electronic records. This framework is essential for ensuring that digital evidence is treated with the same rigor and scrutiny as traditional forms of evidence, particularly in the context of

political corruption cases.

Section 63 of the **BSA** outlines the conditions under which electronic records can be admissible in court. It specifies that to qualify as admissible evidence, electronic records must meet certain criteria, including being produced directly from the device used to generate or store the data. This section serves as a crucial safeguard against the introduction of manipulated or unreliable digital evidence. To establish authenticity, the person who produces the electronic record must provide a certificate, outlining the details of the record's generation and storage, which aids in maintaining the integrity of the evidence.[11]

In addition to the BSA, the Information Technology Act, 2000, plays a significant role in regulating digital evidence. This Act provides the legal recognition of electronic documents, digital signatures, and secure electronic transactions. It also establishes the legal framework for cybercrime, which is particularly relevant in corruption cases where digital evidence may involve unlawful access, data breaches, or forgery. The IT Act's provisions aim to create a secure environment for digital transactions, thereby enhancing the reliability of digital evidence.

Furthermore, various judicial pronouncements have shaped the interpretation of digital evidence in Indian courts. Courts have increasingly recognized the importance of digital evidence in addressing issues of corruption and malpractice, reinforcing its admissibility and relevance. Landmark cases have set precedents for how digital evidence is collected, preserved, and presented in court, ensuring that the legal standards are upheld. [12]

Despite the robust legal framework, challenges persist in the effective application of these laws. Law enforcement agencies often grapple with issues related to the technical expertise required for collecting and analyzing digital evidence. Additionally, the rapidly evolving nature of technology presents challenges in keeping the legal framework current and effective. Ensuring that legal provisions can adapt to new forms of digital communication and storage is critical for maintaining the integrity of the justice system.

In conclusion, the legal framework governing digital evidence in India is multifaceted,

[11] Bhardwaj, S. (2020). Admissibility of Electronic Evidence under the BSA, 2023. *International Journal of Management and Humanities*, *4*(7), 15-20.
[12] Karia, T., Anand, A., & Dhawan, B. (2015). The Supreme Court of India re-defines admissibility of electronic evidence in India. *Digital Evidence & Elec. Signature L. Rev.*, *12*, 33.

comprising the BSA and the Information Technology Act, along with judicial interpretations. Understanding this framework is crucial for effectively utilizing digital evidence in political corruption cases, ensuring that it serves as a reliable tool for justice in India.

Procedural Challenges in the Collection and Preservation of Digital Evidence

The collection and preservation of digital evidence in political corruption cases present unique procedural challenges that must be addressed to ensure the integrity and admissibility of such evidence in court. Unlike traditional forms of evidence, digital evidence is inherently vulnerable to manipulation, alteration, or loss. As such, law enforcement agencies and legal practitioners must adhere to stringent protocols to mitigate these risks.

One of the primary challenges in the collection of digital evidence is ensuring proper authorization and adherence to legal protocols. The process typically begins with obtaining warrants or court orders to access electronic records, which may include emails, text messages, and financial transactions.[13] In political corruption cases, the sensitive nature of the information often necessitates expedited procedures to prevent potential tampering or destruction of evidence. However, the urgency may lead to lapses in following established protocols, which can compromise the evidence's integrity and lead to legal challenges regarding its admissibility.

Once digital evidence is collected, preserving its authenticity becomes paramount. Maintaining a proper chain of custody is essential to establish that the evidence has not been altered or tampered with since its collection.[14] This involves documenting every step of the evidence handling process, from the initial collection to storage and eventual presentation in court. Failure to maintain an unbroken chain of custody can result in challenges to the evidence's reliability, potentially jeopardizing the prosecution's case.

Moreover, the technical expertise required to handle digital evidence is another significant challenge. Many law enforcement agencies lack specialized training and resources to effectively collect and analyze digital data. This can lead to improper collection methods, such as using unauthorized tools or failing to create proper backups, which can jeopardize the

[13] Verma, R., Govindaraj, J., & Gupta, G. (2016). Data privacy perceptions about digital forensic investigations in India. In *Advances in Digital Forensics XII: 12th IFIP WG 11.9 International Conference, New Delhi, January 4-6, 2016, Revised Selected Papers 12* (pp. 25-45). Springer International Publishing.
[14] Dubey, V. (2017). Admissibility of electronic evidence: an Indian perspective. *Forensic Research and Criminology International Journal*, *4*(2), 58-63.

evidence's integrity. Additionally, as technology rapidly evolves, legal practitioners and investigators must continuously update their skills and knowledge to keep pace with new forms of digital communication and storage.[15]

Another procedural challenge arises from the potential for data encryption and privacy laws. In political corruption cases, investigators may encounter encrypted data that is difficult to access without proper decryption methods. Additionally, privacy concerns and regulations surrounding personal data can complicate the collection of digital evidence, particularly when it involves public officials or politically sensitive information.

Judicial Interpretation and Case Analysis in Political Corruption Cases

Judicial interpretation plays a pivotal role in shaping the legal landscape surrounding the use of digital evidence in political corruption cases. Courts in India have increasingly recognized the significance of digital evidence in revealing corrupt practices and ensuring accountability among public officials. By analyzing landmark judgments and recent cases, one can gain insight into how judicial bodies approach the admissibility and reliability of digital evidence in political corruption scenarios. One notable aspect of judicial interpretation is the courts' emphasis on the principles of fairness and justice when assessing the admissibility of digital evidence.[16] In several cases, judges have underscored the necessity of upholding constitutional rights while ensuring that the integrity of the investigative process is not compromised. This balanced approach reflects a commitment to the rule of law and highlights the judiciary's role as a guardian of civil liberties in the context of political corruption.[17]

A key focus of judicial analysis has been on the procedural aspects of collecting and presenting digital evidence. Courts have scrutinized whether law enforcement agencies adhered to legal protocols and maintained the proper chain of custody. In instances where evidence was deemed to be collected improperly, judges have ruled it inadmissible, reinforcing the importance of following established procedures. Such rulings emphasize the necessity for law enforcement to equip themselves with the requisite technical skills and legal knowledge to handle digital

[15] Dholam, S. (2015). Electronic evidence and its challenges. *URL: http://mja. gov. in/Site/Upload/GR/Title% 20NO*, *12*(9).
[16] Sharma, N., & Vadhera, S. (2021). Case Commentary: State of India vs Suhas Katti. *Available at SSRN 3776961*.
[17] Bhattathiripad, P. V., & Behera, L. (2019). Electronic evidence in the Indian courts: A set of forensic guidelines for the police officers in India. *Indian Police Journal*, *66*(4), 1.

evidence effectively.

Moreover, case analysis reveals how judges interpret the provisions of the BSA and the Information Technology Act in the context of digital evidence. Courts have consistently upheld the notion that electronic records, when properly authenticated, hold the same weight as traditional evidence. This judicial stance reinforces the growing recognition of digital evidence's significance in contemporary investigations and prosecutions.

Additionally, landmark cases have illustrated the judiciary's proactive role in addressing issues related to digital evidence, including challenges posed by data encryption and privacy concerns. Courts have navigated the complexities of balancing investigative needs with individual rights, setting precedents for how future cases involving digital evidence will be handled.[18]

In conclusion, judicial interpretation and case analysis in political corruption cases in India demonstrate the judiciary's pivotal role in shaping the legal framework surrounding digital evidence. By emphasizing procedural fairness, adhering to legal standards, and addressing contemporary challenges, the courts contribute to the effective use of digital evidence in the fight against corruption. As the landscape of political corruption evolves, the judiciary will continue to play a critical role in ensuring that justice is served while safeguarding individual rights.

Conclusion

The use of digital evidence in political corruption cases in India presents a complex interplay of legal, procedural, and ethical challenges. As this research has demonstrated, while digital evidence offers significant potential for uncovering corrupt practices and enhancing accountability, various hurdles must be addressed to ensure its effective application in judicial proceedings. The legal frameworks governing digital evidence, particularly the BSA and the Information Technology Act, require ongoing evaluation and reform to adapt to the rapidly evolving technological landscape. Additionally, the challenges faced by law enforcement in collecting and preserving digital evidence highlight the necessity for specialized training and resources to safeguard the integrity of investigations. Ethical considerations surrounding data

[18] Ekanandanayaka, S. (2023). An Analysis on the Admission and Confession in the BSA. *Issue 4 Int'l JL Mgmt. & Human.*, *6*, 1472.

privacy further complicate the landscape, necessitating a careful balance between effective investigation and the protection of individual rights. To enhance the fight against political corruption in India, it is imperative to create a cohesive strategy that incorporates legal reforms, procedural improvements, and ethical guidelines. Such an approach will not only facilitate the admissibility of digital evidence but also bolster public confidence in the integrity of political processes and the justice system as a whole.

Bibliography

Books

1. Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: Crime and justice in digital society. Routledge.

2. Katsh, E., & Rabinovich-Einy, O. (2017). Digital justice: technology and the internet of disputes. Oxford University Press.

Journal Papers

a) Jain, N., & Srinivas Reddy, S. (2020). Admissibility of Electronic Evidence in India: An Overview. Nyaayshastra L. Rev., 1, 1.

b) Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), 1-18.

c) Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3), e23.

d) Bhardwaj, S. (2020). Admissibility of Electronic Evidence under the BSA, 2023. International Journal of Management and Humanities, 4(7), 15-20.

e) Karia, T., Anand, A., & Dhawan, B. (2015). The Supreme Court of India re-defines admissibility of electronic evidence in India. Digital Evidence & Elec. Signature L. Rev., 12, 33.

f) Verma, R., Govindaraj, J., & Gupta, G. (2016). Data privacy perceptions about digital forensic investigations in India. In Advances in Digital Forensics XII: 12th IFIP WG 11.9 International Conference, New Delhi, January 4-6, 2016, Revised Selected Papers 12 (pp. 25-45). Springer International Publishing.

g) Dubey, V. (2017). Admissibility of electronic evidence: an Indian perspective. Forensic Research and Criminology International Journal, 4(2), 58-63.

h) Dholam, S. (2015). Electronic evidence and its challenges. URL: http://mja. gov. in/Site/Upload/GR/Title% 20NO, 12(9).

i) Sharma, N., & Vadhera, S. (2021). Case Commentary: State of India vs Suhas Katti. Available at SSRN 3776961.