THE ADMISSIBILITY OF DIGITAL EVIDENCE IN MODERN LEGAL SYSTEMS: CHALLENGES AND SOLUTIONS

Prakriti Dutta, BA LLB (H), Symbiosis Law School, Pune

INTRODUCTION:

"Evidence is the bedrock of Justice; without it, the truth remains elusive, and justice is compromised."[1] Justice V.R. Krishna Iyer's Pronouncement emphasizes the crucial role that evidence plays in the judicial system around the world. In light of the Indian context, the law of evidence was previously guided by the Indian Evidence Act of 1872[2]; however, in order to incorporate technological and contemporary advancement and societal changes, it has been revised and renamed as the Bharatiya Shakshya Adhiniyam 2023.[3] One of the key factors in the revised version, along with the removal of the colonial era reference, is the inclusion of Digital Evidence. **Section 61** of the Bharatiya sakhsya Adhiniyam states that *"**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**"*[4]. If we focus on the words **"Nothing in this Adhiniyam**," the scope of admissibility of digital evidence will be expanded.

Research Question

- Have recent technological advancements impacted the standards for the admissibility of digital evidence?
- Whether the Bharatiya Sakshya Adhiniyam copiously addresses the challenges and practical solutions associated with digital evidence?
- Whether the role of digital forensics is acknowledged in determining the admissibility of digital evidence, and how are the results assessed in court?

[1] The Judicial Philosophy of Justice V.R Krishna Iyer, Bar and Bench, People's Philosophy edition column 2022
[2] Indian Evidence Act, No. 1 of 1872, (India).
[3] Bharatiya Sakshya Adhiniyam, No. 11, Acts of Parliament, 2023 (India).
[4] Bharatiya Sakshya Adhiniyam, No. 11 § 61, Acts of Parliament, 2023 (India).

Research Objectives

- To analyze the Indian Evidence Act, 1872, and the Bharatiya Sakshya Adhiniyam, 2023, regarding digital evidence's admission and evidentiary value in Indian courts.
- The objective is to formulate and provide strategic suggestions to tackle the difficulties related to digital evidence in India, with the goal of assuring its efficient and trustworthy use in judicial processes.
- To carry out a comparison between Indian admissibility and management of digital evidence and foreign norms and practices
- The objective is to examine the advantages provided by digital evidence in judicial procedures and the difficulties faced in its management within the Indian legal system.

Research Methodology

The research methodology involves a descriptive and analytical approach. Secondary sources such as research papers, landmark judgments, and books are used to draw a conclusion. The research uses purposive sampling to pick important sources, qualitative and comparative analysis to uncover significant themes and trends, and cross-verification and consistent standards to assure validity and dependability.

Literature Review

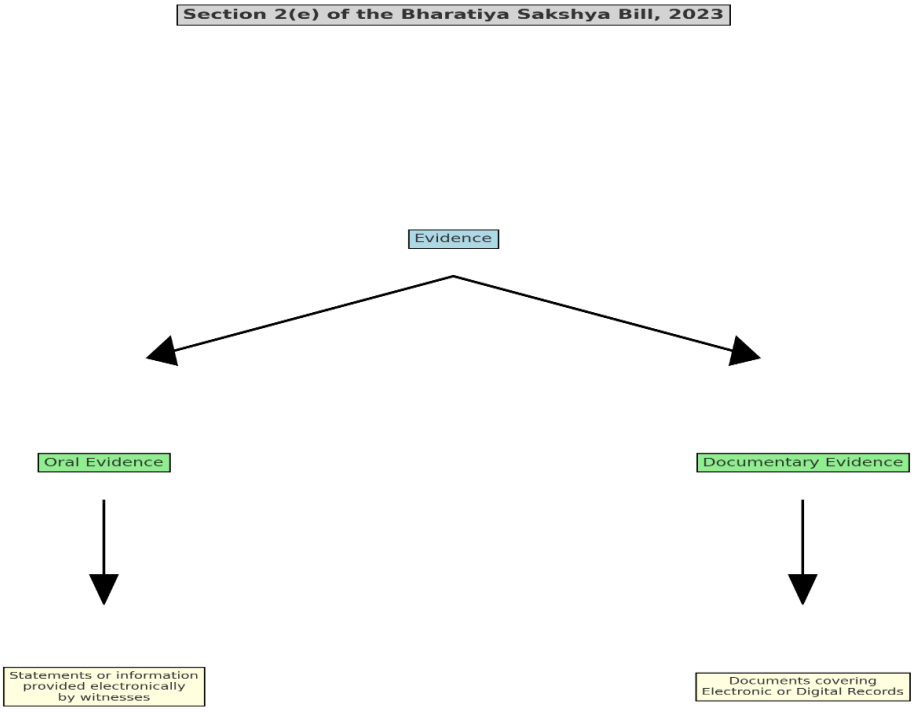
Paper name	***Literature review***
Admissibility of electronic evidence: an Indian perspective-Vivek Dubey. [*Paper citation: Vivek Dubey, Dr. H.S.Gour Vishwavidyalaya Sagar University, India, Forensic Research & Criminology International Journal, Volume 4 Issue 2 – 2017*]	This paper examines the admissibility of digital evidence in the Indian context and its critical aspect. The Indian Evidence Act and the cases it regulates were comprehensively reviewed by the author. Nevertheless, it does not provide a comprehensive examination of the impact of the landmark cases on the application of section 65(B) of the Evidence Act. Additionally, the paper neglects to consider the technological obstacle associated with managing electronic devices.

A Review on the Changing Dimensions of Digital Forensics in Criminal Investigations [*Paper citation: Dr. K.V.K. Santhy & Abhishek Sharma Padmanabhan, Sardar Vallabhbhai Patel National Police Academy Journal Vol. LXXI, No. 1-2, 160-183*]	Digital forensics is examined in this paper in the context of criminal investigations. It emphasises the pivotal role of digital evidence in the contemporary criminal justice system. The author meticulously examines the process of scientific validation in digital forensics. At the same time, the paper fails to verify the extent to which these technologies influence the collection and validation of digital evidence. Furthermore, the subject of privacy is not addressed.

DEFINING DIGITAL EVIDENCE IN THE MODERN LEGAL FRAMEWORK

We consider something that furnishes proof as evidence, and this proof generally needs to be in the form of records or any information relevant to the case at hand. The Information Technology Act of 2008[5] defines electronic evidence as "*Any information with values that is stored or transmitted electronically, and it includes evidence such as computer data, digital audio, digital video, cell phones, and digital fax machines*."

Section 2(e) of the Bharatiya Sakshya Adhiniyam [6]provided us with the legal framework for the admissibility of the digital evidence. The below pictorial representation ***(fig.1)*** showcases the provision under this section.



[5] The Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2008 (India).
[6] Bharatiya Sakshya Adhiniyam, No. 11 § 2(e), Acts of Parliament, 2023 (India).

(fig.1)

Section 32 of the Bharatiya Sakshya Addhiniyam[7] also talks about electronic evidence in reference to the laws of the other country. The table below ***(fig.2)*** gives an overview of the changes regarding digital and electronic evidence under the Indian Evidence Act and Bharatiya Sakshya Adhiniyam to get a better understanding of the same.

Aspect	Indian Evidence Act, 1872	Bharatiya Sakshya Bill, 2023
Admissibility of Digital Evidence	Considered as Secondary Evidence (Section 65B)	Considered as Primary Evidence (Section 57)
Definition of Primary Evidence	Documents presented for examination (Section 62)	Digital records created/stored simultaneously considered primary evidence
Treatment of Digital Records	Not explicitly recognized as primary evidence	Explicitly recognizes digital records as primary evidence
Specific Provisions for Digital Evidence	Limited provisions, mainly under Section 65B	Detailed provisions under Section 5

(fig.2)

EVALUATING THE SCOPE AND ESSENTIALITY OF DIGITAL EVIDENCE IN CONTEMPORARY JURISPRUDENCE

If we closely look into the technological advancement of this fast-flowing world, we see the scope of digital evidence, which is of utmost importance. Digital evidence plays a crucial role in this digital world, namely forensic analysis and investigation, corporate investigation, the growing aspect of intellectual property, cyber security, and, needless to say, criminal investigation.[8] Presently, in the 21st century, cyberbullying is one of the most frequent forms of offense; therefore, to deal with cyber crimes such as cyber harassment and fraudulent activities

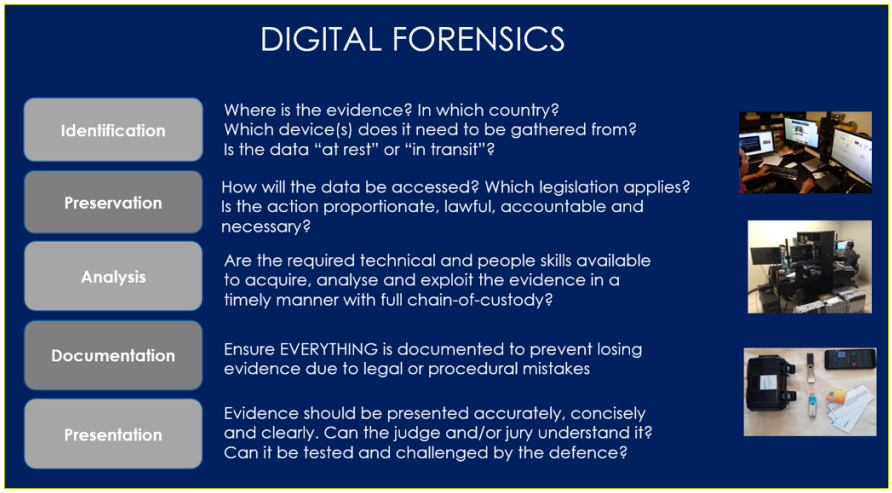
[7] Bharatiya Sakshya Adhiniyam, No. 11 of 2023, § 32 (India).
[8] Karia, Tejas D. "Digital Evidence: An Indian Perspective." *Digital Evidence & Elec. Signature L. Rev.* 5 (2008): 214.

that occur online, digital proof becomes of paramount noteworthiness. [9]

The growth in the digital world is unparalleled to this date, and almost every business organization, be it retail or e-commerce, is pertaining towards e-contracts. In situations such as this, digital proof becomes essential to exhibit the relevance and reliability of such documents.[10]

THE DIGITAL REVOLUTION IN FORENSICS: UNVEILING THE IMPORTANCE OF ELECTRONIC EVIDENCE

Forensic investigation involves the scientific method of investigation, and specific scientific tools and techniques are used to examine physical evidence for criminal or civil legal proceedings. This physical evidence mainly includes **fingerprints, DNA, blood stains**, analysis of weapons, autopsy reports, post-mortem reports, and other related evidence. **Now, the general question might arise as to how digital evidence can help in forensic investigation?** Typically, the digital forensics method also bestows a substantial character in forensic investigation; this comes in handy specifically when dealing with information stored electrically, retrieving, retaining, and analyzing electronic data that may be beneficial in criminal investigations. This encompasses data from mobile phones, hard drives, computers, and other data storage devices.[11] In India, digital forensics is still in a nascent stage.

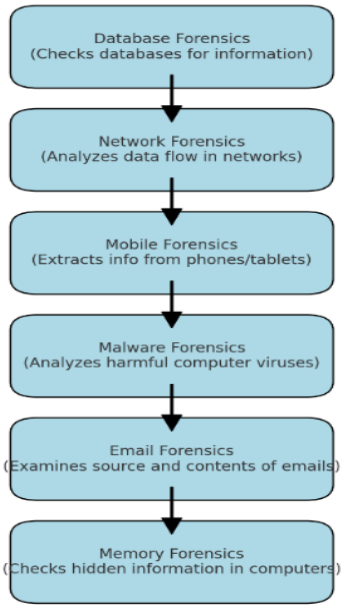


[9] Dubey, V., 2017. Admissibility of electronic evidence: an Indian perspective. *Forensic Research and Criminology International Journal*, *4*(2), pp.58-63.
[10] Karia, Tejas D. "Digital Evidence: An Indian Perspective." *Digital Evidence & Elec. Signature L. Rev.* 5 (2008): 214.
[11] Lallie, Harjinder Singh. "An overview of the digital forensic investigation infrastructure of India." *Digital Investigation* 9, no. 1 (2012): 3-7.

Identification of suspects and victims through various data points such as communication records and social media profile can be enhanced through the admissibility of digital evidence furthermore reconstructing crime scenes , GPS data from smartphones, CCTV Footage can help to establish timelines and prove or disproving alibi claims furthermore, it helps in corroborating physical evidence[12]. If we try to categorise digital forensics we can categorise into 6 basic parts. The below flowchart represents the same (fig.3)

TYES OF DIGITAL FORENSICS

(fig.3)



If we look into some of the major cases dealing with these a better understanding and clarity of the same can be concluded. In 2021, **Bharat Jadav Vs State of Madhya Pradesh**,[13] the importance of technology in forensic sciences was highlighted by the honourable high court of Madhya Pradesh. The case at hand was regarding the grant of parole under section 439 of CRPC. The court underscored the scope of forensic science is not just limited to DNA reports and blood samples. The executive body and judiciary must take in to account the subject and instruments of digital forensic methods.

The Mumbai train bombing of 2006 shows us how much digital forensics comes of paramount interest. The nonstate actors used very sophisticated technology. [14]This included

[12] Yadav, D., Mishra, M., & Prakash, S. (2013, September). Mobile Forensics challenges and admissibility of electronic evidence in India. In *2013 5th International Conference and Computational Intelligence and Communication Networks* (pp. 237-242).
[13] Bharat Jatav v. State of Madhya Pradesh, MCRC NO.17346 of 2021, decided on 02-09-2021.
[14] Mumbai train blasts: Death for five for 2006 bombings, BBC News (30 September 2015).

proxy services and concealing their IP address to hide the trace of their communication. After this incident it was recommended that India's Information Technology be safeguarded from the potential damage by strengthening the cyber forensics and cyber security professionals.

The 2008 Mumbai attacks, popularly known as 26/11, were a series of coordinated attacks that took place in November 2008. Ten members **of Lashkar-e-taiba** carried out 12 coordinated shooting and bombing attacks lasting four days across Mumbai. Apparently, The US warned us about the possible terror attack with the help of digital information; **however, India missed those warnings due to the inability to decode that digital information**. [15]Following the attack, the Indian government generated a report that underscored the importance of digital devices after the investigators discovered that digital evidence played a crucial role in the planning and execution of these terror attacks.

JUDICIAL PRONOUNCEMENT SURROUNDING DIGITAL EVIDENCE

State (N.C.T of Delhi) v. Navjot Sandhu (2005) [The Parliament Attack Case][16]

The Supreme Court determined a vital issue regarding electronic record admission in court in this case. This lawsuit included the 2001 Indian Parliament terrorist attack. The plot was alleged against former Punjab Pradesh Congress Politician President Navjot Sandhu. The prosecution requested phone records as proof. However, the defense objected because the records lacked the certificate needed by Section 65B(4) of the Indian Evidence Act. [17]Indian Supreme Court rendered a significant verdict in this matter. However, it was overruled in 2015 in Anver P.V. V PK Basheer and others.

- Electronic documents might be admissible without a certificate under Section 65B(4) of the Indian Evidence Act. After this case, electronic record admission regulations were relaxed.

- Parties might present an original record as the main evidence in court. Under Section 65B (4) of the Evidence Act, they might use a copy of the original record with a

[15] Monahan, T., & Stainbrook, M. (2013). Learning from the lessons of the 2008 Mumbai terrorist attacks. *The Police Chief*, *78*, 24-32.
[16] State (N.C.T of Delhi) v. Navjot Sandhu @ Afsan Guru, 2005 11 SCC 600.
[17] Indian Evidence Act, No. 1 of 1872, § 65B (India).

certificate.

Anver P.V v. P.K Basheer & Ors (2014)[18]

This Supreme Court decision addressed electronic record evidentiary admissibility. An independent candidate, the appellant claimed Left Democratic Front support. The responder won the 034 Eranad Legislative Assembly Constituency. In an electoral dispute, the appellant claimed campaign corruption. Electronic evidence admissibility was the major issue in this case. ***CDs and a pamphlet were evidence***. It purportedly contains lies to sway the election. The appellant failed to certify several CDs as required by Section 65B(4) of the Act. Electronic records' secondary evidence admissibility was questioned. The lawsuit also included accusations about ***the controversial booklet (Exhibit-P1)***. Section 123(4) of the Representation of the People Act (1951)[19] considered such allegations corrupt.

- Section 65B requires judicial processes to incorporate electronic evidence as supplementary evidence, as this ruling shows. CDs are inadmissible as evidence without the certificate required under section 65B of the Act, the court ruled.

- The court ruled that electronic records must meet Section 65B requirements to be admissible.

In this case, the Supreme Court ruled that Section 65B of the Indian Evidence Act was not a comprehensive code but did not refer to the precedent set in Anvar vs. Basheer. In the previous judgment, appellants were convicted of murdering Varanasi visitor Francesco Montis. The prosecution claimed that the appellants killed him.

Security camera video and technological documentation were not correctly displayed throughout the trial, the judge concluded. The courts said the trial court ignored the investigation's significant errors. Criminal trials need compelling evidence, the judgment said. The court acquitted the accused due to insufficient evidence. The Indian Evidence Act recognizes electronic evidence, but it can be proven beyond a reasonable doubt, the court said. In unclear cases, the law favors the accused. The ruling doesn't specify how digital evidence is

[18] Anvar PV v. PK Basheer & Ors (2014 10 SCC 473)
[19] Representation of the People Act, 1951, § 123(4) (India).
[20] Tomaso Bruno & Anr. Versus State of U.P. (2015) 3 SCC (Cri) 54.

considered.

Shafhi Mahommad v. The State of Himachal Pradesh (2018)[21]

This case included the examination of the admissibility of electronic evidence by the Supreme Court of India. The problem arose from the fact that the party presenting the evidence does not own the electronic document-generating device. The judge examined the applicability of Section 65B (4) of the Evidence Act.[22] The Section mandates the submission of an electronic proof certificate. The court said that electronic evidence produced by an individual who does not have possession of the equipment does not need a certificate. Pursuant to Section 65B(4) of the Indian Evidence Act, the court admitted electronic evidence even in the absence of a certificate.

LAW COMMISSION REPORT

The 185th Law Commission report suggested the amendment to the Indian Evidence Act 1872 to incorporate digital evidence. This report indicated the inclusion of 65B, which specifies conditions under which digital evidence can be admissible or not. It also highlighted that proper preservation methods of digital proof must be present**.**

The 221st Law Commission report showcases the growing importance of digital evidence. It also highlights the possible challenges, such as the potential for tampering. It also addressed the importance of authenticating digital signatures under the IT Act 2000.

A COMPARATIVE ANALYSIS OF DIGITAL EVIDENCE ADMISSIBILITY ACROSS JURISDICTIONS

UNITED STATES OF AMERICA

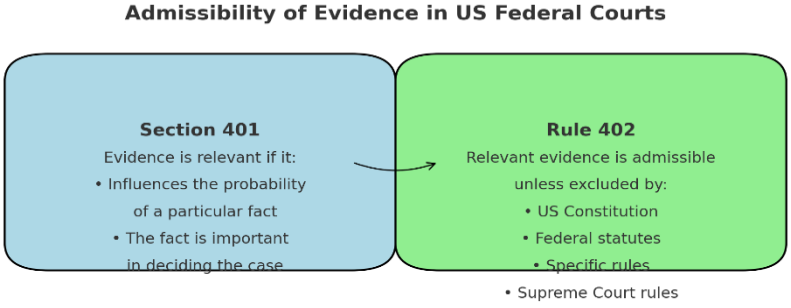
The Federal Rules of Evidence 1975[23] govern the evidence law in the United States, these rules also cover the aspect of digital evidence. There are three-fold criteria that must be met in order to give digital evidence its due credit:

[21] Shafhi Mahommad v. The State of Himachal Pradesh (2018) (2015) 7 SCC 178.
[22] Indian Evidence Act, No. 1 of 1872, § 65B (India).
[23] Fed. R. Evid. (1975).

- Firstly, the evidence provided should be relevant to the matter in issue
- Secondly, the evidence must be authentic; such authentication may be done through expert opinions, public reports, official records, and certified data.
- Thirdly, such evidence must be sourced from Federal Rules of Evidence Rule 401[24] and Rule 402.[25]

The diagrammatic representation below(fig.4) will show the essentials for coming under rules 401 and 402

(fig.4)



The major obstacle in the American legal system regarding digital evidence is the presence of a hearsay rule. The federal rule of evidence, Rules 801 [26]and 802[27] highlights the fact that us courts need to analyze whether the evidence presented is either a statement made by the individual or is being offered to substantiate the truth of a claim. If the evidence adheres to these categories, it may be classified as hearsay.

AUSTRALIA

The Uniform Evidence Act,1955,[28] sections 146[29] and 147 are responsible for governing the admissibility of electronic evidence in Australia.[30]

The debate on DP 69, inspired by South Australia's evidence laws, has raised questions about the adequacy of the rules to simplify computer-generated evidence in court. To ensure data

[24] Fed. R. Evid. Rule 401 (1975).
[25] Fed. R. Evid. Rule 402 (1975).
[26] Fed. R. Evid. Rule 801 (1975).
[27] Fed. R. Evid. Rule 802 (1975).
[28] Uniform Evidence Act 1955 (Australia).
[29] Uniform Evidence Act 1955, § 146 (Australia).
[30] Uniform Evidence Act 1955, § 147 (Australia).

accuracy, ***DP 69 introduced something known as "the redundancy test,"*** which required extra computer system tests. These added precautions were expected to improve computer-generated evidence dependability by ***redundancy test supporters***. However, the same proposal was rejected by the officers of the director of public prosecution. The chart given below (Fig. 5) summarises the debate regarding DP-69.[31]

Aspect	Details
Initial Goal	To simplify the use of computer-generated evidence in court.
Opposition to DP 69	Officers of the Director of Public Prosecutions opposed the proposal.
Support for Presumption Rules	The Commonwealth Director of Public Prosecutions (CDPP) supported the existing presumption rules.
Lawyers' Opinions	Some lawyers argued that presumption rules facilitate the admission of documents and records from computer data.
Concerns Raised	Practicality and drawbacks of the redundancy test, increased costs, disadvantages to small litigants, and adverse impacts on evidence.
Commission's Review	Found no compelling evidence indicating issues with current rules, noted differing opinions within the legal community.
Commission's Decision	Opted for minor adjustments rather than significant changes to the law.
Current Status	Rules for using electronic evidence in Australia remain unchanged.
Ongoing Discussions	Emphasize the importance of balancing accuracy and accessibility in legal cases involving electronic evidence.

(fig.5)

NAVIGATING LEGAL CHALLENGES IN DIGITAL EVIDENCE: A CRITICAL ANALYSIS

Electronic evidence has come under scrutiny after, recently, WhatsApp communications were leaked during investigations and included as evidence in criminal trials. The investigation step included leaks of these WhatsApp communications before the trial. With these changes, the legal environment for electronic evidence deserves more examination. [32]

Digital evidence is comparatively new, or perhaps it is better to say that the relevance of the same has been comparatively new. Nevertheless, the Bharatiya Sakshya Adhiniyam 2023 was

[31] Lewis, M., Privileging confidential communications: The uniform Evidence Act inquiry.
[32] Karia, Tejas, Akhil Anand, and Bahaar Dhawan. "The Supreme Court of India re-defines admissibility of electronic evidence in India." *Digital Evidence & Elec. Signature L. Rev.* 12 (2015): 33.

amended to address these concerns. According to the Bill, digital evidence is key. However, it's not comprehensive in nature, and there are still a lot of grey areas.

Digital Evidence Under Bharatiya Sakshya Adhiniyam: Critique and Analysis

In ***Arjun Panditrao Khotkar v. Kailash Kishanrao Goratyal***[33] Mr. Arjun Panditrao Khotkar was challenged in his election from Jalna-101 Legislative Assembly Constituency since his nomination papers were submitted late. The Election Commission delivered CDs with video camera recordings per High Court order. Despite several Petitioner requests, the Election Commission did not furnish the required certifications under Section 65B of the Indian Evidence Act.. Although the purpose of this certification is to guarantee the precision of digital evidence, it may present a challenge in terms of the simplicity with which it can be produced in court.

Another critical issue is **the absence of comprehensive safeguards** to prevent the tampering or taint of electronic records during investigations. Significant concerns regarding the integrity and reliability of digital evidence presented in legal proceedings are raised by this deficiency. Unlike physical documents and testimonies, due to technological advancement, ***it's easy to alter or manipulate e evidence without leaving any trace***

Thirdly, **Digital evidence has been categorized both as primary and secondary evidence.** The admissibility, reliability, and ***evidentiary of both are not the same***. Primary evidence contains more reliability and value and carries a higher evidentiary value. On the other hand, secondary electronic evidence includes copies or reproductions of original copies. Secondary evidence is generally admissible when the original primary evidence is unavailable. Now, this distinction creates ***challenges in determining the admissibility criteria*** under Bharatiya sakshya Adhiniyam.[34]

Contemporary Admissibility Challenges

Understanding the significance of digital evidence is crucial in the investigation of cybercrimes. **However, it can also pose risks to individuals' privacy rights.** These rights are

[33]Arjun Panditrao Khotkar v. Kailash Kishanrao Goratyal AIR 2020 Supreme Court 4908
[34] Chadha, V., & Sivaraman, J. (2024). Critical analysis of the law on admissibility of electronic evidence in India. *Jindal Global Law Review*, 1-14.

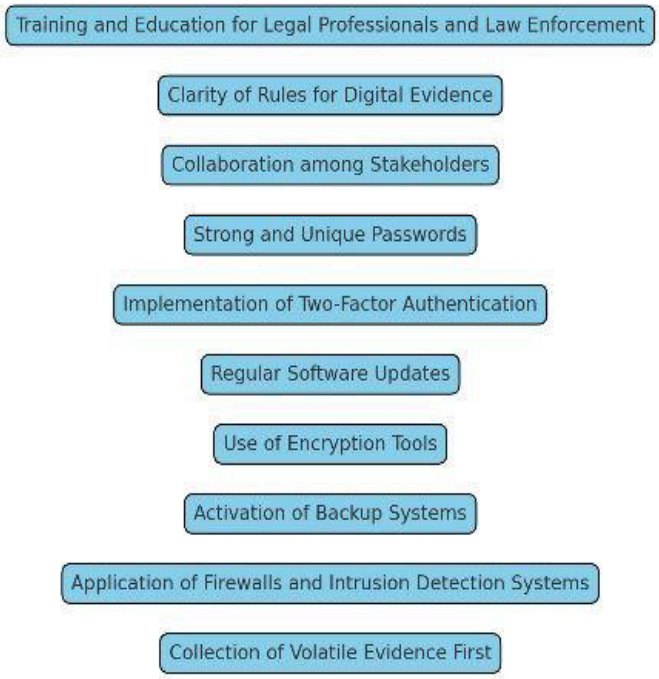
safeguarded by **Article 21 of the Constitution**,[35] which affirms that every person is entitled to life and liberty. This argument was also supported in the case of ***Justice K.S Puttaswamy vs Union of India (2018)***[36]. This has the potential to be exploited to the detriment of individual rights. Tracking someone's online movement without their permission is a clear violation of privacy.

Determining and regulating digital technologies like AI, blockchain, and IoT has been difficult due to technological evolution. Because of this innovation, courts must become acclimated to handling evidence from modern technology. I feel that they need to grasp and comprehend this new technology to make fair legal choices with such facts. Artificial intelligence-generated evidence is difficult for the court to accept. **AI-generated evidence** is typically ***perceived as black boxes***, which might present problems. That suggests the system analyses information and draws decisions without transparency or accuracy. **Determining if such evidence preceded by such methods is credible is difficult.** [37]

Indian intellectual property is becoming a significant source of revenue.[38] Proof of intellectual property ownership requires significant proof. The violation may have resulted from unauthorized copying, distribution, and modification of digital material. The digital proof helps prove a work's originality in some instances. However, due to a lack of comprehensive provisions for addressing the same, it is misused and mishandled. It will reduce unlawful copying and dissemination.

[35] Indian Const. art. 21.
[36] Justice K.S.Puttaswamy(Retd) vs Union Of India AIR 2018 SC (SUPP) 1841.
[37] Verma, R., Govindaraj, J. and 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.
[38] Pandey, A.K. And Sharma, A., 2024. The Function of Digital Evidence and Forensic Computers in Cybercrimes Investigation: A Case Study of India.

SUGGESTIONS AND RECOMMENDATION



Training Programs

Training legal and law enforcement personnel is crucial. Training in digital techniques and software will improve their use and assist gather more accurate evidence for cases. It will add credibility and judicial admissibility to such evidence.

Clear regulations for digital evidence collection, storage, and presentation are needed. There should be rules for employing forensic tools, managing digital evidence properly, and practices.

Collaborative Work with Every Department:

Working collaboratively is crucial for police, attorneys, and IT professionals. They may collaborate on new technology, methods, and norms. Collaboration helps solve digital evidence issues because individuals from diverse organisations learn about each other's work, evidence specifics, and court regulations for gathering and presenting it.

Two Factor Authentication System

Use strong, unique passwords for all accounts to prevent unauthorized access. Using two-factor authentication increases security. It gives consumers a cell phone code for

further verification. Two-factor authentication ensures identification by requiring two authentication factors. Updating software, operating systems, and apps reduces cybercrime. Updating software periodically prevents unauthorized use and hacking. The system is updated regularly to provide the newest security.

Safeguarding Sensitive Data

An active backup system may preserve data. It is useful for recovering data after a cyber assault. Network traffic may be monitored and controlled via firewalls and IDSs. It will reduce unauthorized access. Volatile digital evidence is significant since it changes quickly. This is transient digital data that may be changed or lost. Powering off a device may swiftly influence this form of evidence, usually kept in RAM. Collecting sensitive data first and least sensitive last.

CONCLUDING THOUGHTS

Digital evidence admissibility in India has changed judicial procedures. The Indian Evidence Act of 1872 was amended by the Information Technology Act of 2000 [39]to embrace digital evidence as technology advances. This change recognizes the relevance of digital data in court.

Parliament made digital evidence admissible in Bharatiya Sakshya Adhiniyam 2023 after realizing its value. Bill recognized digital evidence as primary. The government needed clear procedures for acquiring and promoting this evidence. The ICC formally recognized digital evidence in numerous instances. More technology means more data on digital gadgets. This may cause technological abuse and criminality. Lawyers, judges, and others must know how to handle and utilize digital evidence. It takes teamwork to utilize this evidence ethically and serve justice.

[39] The Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2008 (India).

BIBLIOGRAPHY

Statutes

- Bharatiya Sakshya Adhiniyam, No. 11 § 2(e), Acts of Parliament, 2023 (India).
- Bharatiya Sakshya Adhiniyam, No. 11 § 61, Acts of Parliament, 2023 (India).
- Bharatiya Sakshya Adhiniyam, No. 11 of 2023, § 32 (India).
- Bharatiya Sakshya Adhiniyam, No. 11, Acts of Parliament, 2023 (India).
- Fed. R. Evid. (1975).
- Fed. R. Evid. Rule 401 (1975).
- Fed. R. Evid. Rule 402 (1975).
- Fed. R. Evid. Rule 801 (1975).
- Fed. R. Evid. Rule 802 (1975).
- Indian Const. art. 21.
- Indian Evidence Act, No. 1 of 1872, (India).
- Indian Evidence Act, No. 1 of 1872, § 65B (India).
- Representation of the People Act, 1951, § 123(4) (India).
- The Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2008 (India).
- Uniform Evidence Act 1955 (Australia).
- Uniform Evidence Act 1955, § 146 (Australia).
- Uniform Evidence Act 1955, § 147 (Australia).

Indian cases

- Anvar PV v. PK Basheer & Ors (2014 10 SCC 473)
- Arjun Panditrao Khotkar v. Kailash Kishanrao Goratyal AIR 2020 SUPREME COURT 4908
- Bharat Jatav v. State of Madhya Pradesh, MCRC NO.17346 of 2021, decided on 02-09-2021.
- Justice K.S.Puttaswamy(Retd) vs Union Of India AIR 2018 SC (SUPP) 1841
- Shafhi Mahommad v. The State of Himachal Pradesh (2018) (2015) 7 SCC 178
- State (N.C.T of Delhi) v. Navjot Sandhu @ Afsan Guru, 2005 11 SCC 600
- Tomaso Bruno & Anr. Versus State of U.P. (2015) 3 SCC (Cri) 54

Articles and Journals

- Chadha, V., & Sivaraman, J. (2024). Critical analysis of the law on admissibility of electronic evidence in India. *Jindal Global Law Review*, 1-14.
- Dubey, V., 2017. Admissibility of electronic evidence: an Indian perspective. *Forensic Research and Criminology International Journal*, *4*(2), pp.58-63.
- Gelb A, Mukherjee A. Building on digital ID for inclusive services: lessons from India. CGD NOTES. 2019 Sep;2020.1
- HELLBERG, I., & MULLER, E. (2012). The Mumbai terrorist attacks 2008. *MEGA-CRISES: Understanding the Prospects, Nature, Characteristics, and the Effects of Cataclysmic Events*, 168.
- Karia, Tejas D. "Digital Evidence: An Indian Perspective." *Digital Evidence & Elec. Signature L. Rev.* 5 (2008): 214.
- Karia, Tejas, Akhil Anand, and Bahaar Dhawan. "The Supreme Court of India re-

defines admissibility of electronic evidence in India." *Digital Evidence & Elec. Signature L. Rev.* 12 (2015): 33.

- Lallie, Harjinder Singh. "An overview of the digital forensic investigation infrastructure of India." *Digital Investigation* 9, no. 1 (2012): 3-7.

- Lewis, M., Privileging confidential communications: The uniform Evidence Act inquiry

- Monahan, T., & Stainbrook, M. (2013). Learning from the lessons of the 2008 Mumbai terrorist attacks. *The Police Chief*, *78*, 24-32.

- Mumbai train blasts: Death for five for 2006 bombings, BBC News (30 September 2015)

- PANDEY, A.K. and SHARMA, A., 2024. The Function of Digital Evidence and Forensic Computers in Cybercrimes Investigation: A Case Study of India

- The Judicial Philosophy of Justice V.R Krishna Iyer, Bar and Bench, People's Philosophy edition column 2022

- Verma, R., Govindaraj, J. and 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.

- Yadav, D., Mishra, M., & Prakash, S. (2013, September). Mobile Forensics challenges and admissibility of electronic evidence in India. In *2013 5th International Conference and Computational Intelligence and Communication Networks* (pp. 237-242). IEEE.