THE ADMISSIBILITY OF DIGITAL EVIDENCE: CHALLENGES AND FUTURE IMPLICATIONS

Written by ***Vanshika Shukla***

Assistant Professor, IME Law College, Ghaziabad, India

ABSTRACT

The admissibility of digital evidence is a pivotal concern in modern legal proceedings, given the widespread integration of technology in various aspects of life. The paper examines the challenges associated with admitting digital evidence in court and anticipates future implications. The complexities arise from issues like data authenticity, integrity, and chain of custody in an era of easily manipulated digital content. The evolution of encryption and privacy measures further complicates the landscape. Moreover, courts grapple with technical jargon and the need for specialized expertise to comprehend digital evidence. Looking ahead, the future implications of this challenge are multifaceted. Legal systems must adapt to accommodate emerging technologies like blockchain and artificial intelligence, which introduce novel forms of evidence. Striking a balance between ensuring admissibility standards and embracing innovation is crucial. The paper underscores the necessity for legal professionals to collaborate closely with technology experts, formulate updated protocols, and establish a robust framework that maintains the integrity of the judicial process while harnessing the potential of digital evidence.

Keywords**:** Digital Evidence, Admissibility, Challenges, Future Implications, Authentication.

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

INTRODUCTION

In an increasingly digitized world, the use of digital devices and technologies has become an integral part of both personal and professional spheres. This shift towards digitalization has brought about significant changes in various aspects of life, including communication, commerce, governance, and even crime. Consequently, the legal landscape has had to adapt to this digital revolution, particularly in the realm of evidence presentation in legal proceedings.

The admissibility of evidence, a cornerstone of any just legal system, has encountered new challenges and complexities with the proliferation of digital sources of information. Digital evidence encompasses a wide array of data, including emails, text messages, social media posts, computer files, GPS records, and more. This evidence is often crucial in establishing the facts of a case, identifying perpetrators, and ensuring fair trials. However, its unique nature and the technicalities involved in its collection, preservation, and presentation have raised intricate legal issues. Moreover, we contemplate the ways in which legal precedent, technological innovation, and systemic reforms will shape the evolution of practices surrounding digital evidence. In an age where digital footprints can be as telling as fingerprints, grasping the nuances of admissibility is not merely an academic pursuit—it is a vital endeavor that underpins the bedrock principles of fairness, truth-seeking, and the preservation of rights within the realm of law.

This paper delves into the challenges posed by the admissibility of digital evidence in legal proceedings and explores the potential implications for the future of the legal system. The discussion will encompass both the benefits and drawbacks of digital evidence, the hurdles in ensuring its authenticity and integrity, and the evolving standards for its acceptance in courtrooms. The admissibility of digital evidence is a critical topic in today's legal landscape, given the increasing reliance on digital technologies and the proliferation of electronic data in various aspects of life.

TYPES OF DIGITAL EVIDENCE

Digital evidence refers to any form of electronic data that can be used as evidence in a legal or investigative context. This evidence is collected from digital devices, networks, and online services, and it can play a crucial role in various legal proceedings, such as criminal

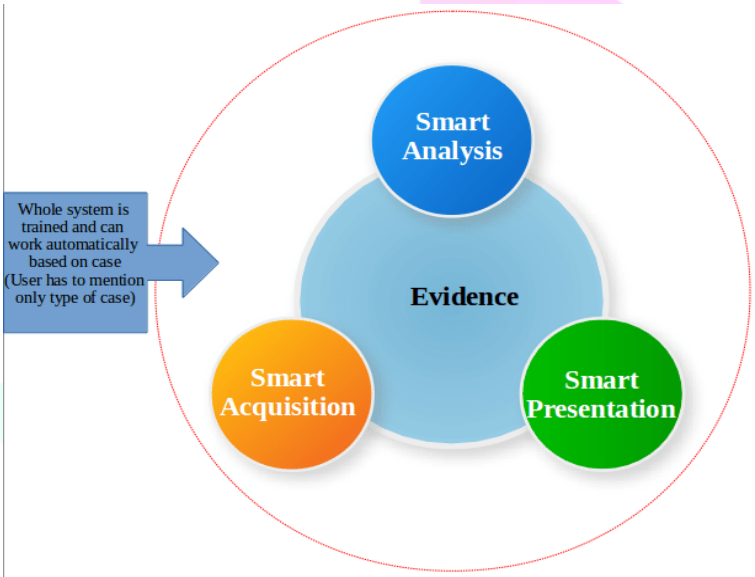
ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

investigations, civil litigation, and cyber security incidents. Here are some common types of digital evidence:

- ***Documents and Files:*** *These include text documents, spreadsheets, presentations, PDFs, and other electronic files that are relevant to the case.*
- ***Emails:*** *Emails and their attachments can provide valuable information about communications and interactions between individuals.*
- ***Instant Messages and Chats:*** *Conversations that occur on platforms like messaging apps, social media, and chat applications can be important in understanding relationships and context.*[i]
- ***Images and Videos:*** *Multimedia files can capture events, actions, or situations that are pertinent to an investigation or legal matter.*
- ***Databases:*** *Data stored in databases can reveal patterns, transactions, and relationships that might be relevant to a case.*
- ***Social Media Posts:*** *Posts, comments, likes, and shares on social media platforms can provide insights into an individual's thoughts, activities, and connections.*
- ***Metadata:*** *Metadata contains information about other data. For example, the metadata of a photo might include the date and time it was taken, the location, and the device used.*
- ***Internet Browsing History:*** *Information about websites visited, searches conducted, and online activities can provide context or a timeline of events.*[ii]
- ***Geolocation Data:*** *Location-based information from devices, apps, or services can help establish a person's whereabouts at a certain time.*
- ***Call Records:*** *Records of phone calls, including call logs and text messages, can be relevant in investigations involving communication patterns.*
- ***Financial Records:*** *Digital records of financial transactions, bank statements, and payment histories can provide insights into a person's financial activities.*
- ***System Logs:*** *Logs from operating systems, applications, and network devices can reveal actions taken on a device or network.*[iii]
- ***Computer Memory:*** *Information stored in RAM or other forms of computer memory can provide real-time insights into a device's state and activities.*
- ***Deleted or Altered Files:*** *Recovery of deleted or altered files can sometimes uncover evidence that was intentionally hidden.*

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

- ***Encryption and Decryption Records:*** *Information about encrypted files, encryption keys, and attempts to decrypt data can be significant in cases involving cyber security.*[iv]
- ***Digital Signatures:*** *Digital signatures can be used to verify the authenticity and integrity of electronic documents.*
- ***Authentication Records:*** *Records of user logins, access attempts, and account activities can help establish who accessed a system or service.*
- ***Network Traffic Data:*** *Information about network connections, data transfers, and communication patterns can provide insights into cyber incidents.*[v]



Proposed AI based Digital Forensic Framework

ADMISSIBILITY OF DIGITAL EVIDENCE

The admissibility of digital evidence in court depends on several factors, including the relevance, authenticity, integrity, and reliability of the evidence. Courts follow specific rules and guidelines to determine whether digital evidence can be admitted and considered during legal proceedings. These rules can vary by jurisdiction and legal system, but there are some common principles that generally apply:

Relevance: The digital evidence must be relevant to the case at hand. It should have a direct connection to the issues being discussed in the legal proceeding.[vi]

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

Authenticity: The party offering the digital evidence must establish its authenticity, proving that the evidence is what it claims to be. This can involve showing the origin of the evidence and how it was collected.

Integrity: The digital evidence should be preserved and presented in a way that maintains its integrity and prevents tampering or alteration.

Hearsay: Hearsay refers to statements made outside of court that are offered as evidence to prove the truth of the matter. Digital evidence that contains hearsay might not be admissible unless it falls under an exception to the hearsay rule.[vii]

Best Evidence Rule: The best evidence rule generally requires that the original or the most reliable form of evidence be presented. In the case of digital evidence, this might involve presenting the original file rather than a printout or a copy.

Expert Testimony: In cases where the digital evidence is complex or technical, expert witnesses might be called to testify about the authenticity, reliability, and interpretation of the evidence.

Chain of Custody: The chain of custody is the documented record of the individuals who had control of the evidence from the time it was collected to when it is presented in court. A proper chain of custody helps establish the integrity of the evidence.[viii]

Legal Requirements: Some jurisdictions might have specific legal requirements for the admissibility of digital evidence, such as electronic signatures, timestamps, and encryption standards.

Technology Reliability: Courts often consider the reliability of the technology and methods used to collect, store, and present digital evidence. Established and widely accepted technologies are more likely to be deemed reliable.

Authentication: Authenticating digital evidence might involve showing that it was generated by a specific device, software, or user. This can be done through metadata, digital signatures, or other forms of verification.

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

Privacy and Data Protection Laws: Digital evidence collection must also comply with privacy and data protection laws. Evidence obtained illegally or in violation of these laws might not be admissible.[ix]

Fairness and Due Process: Courts consider whether the admission of digital evidence would violate a defendant's right to a fair trial or due process.

Moreover, the admissibility of digital evidence is a complex area of law, and legal professionals often work closely with experts in digital forensics and technology to ensure that evidence is properly collected, preserved, and presented in court. The rules and standards can vary widely, so it's essential to consult the relevant laws and legal professionals in the jurisdiction where the case is being heard.[x]

CHALLENGES IN ADMISSIBILITY

Admitting digital evidence in court proceedings can be challenging due to various technical, legal, and procedural factors. Some of the common challenges in the admissibility of digital evidence include:

Authenticity and Tampering: Proving that digital evidence is authentic and has not been tampered with is a significant challenge. It's relatively easy to alter digital files, metadata, and other attributes, making it necessary to establish a clear chain of custody and demonstrate that the evidence presented is unchanged from its original state.

Hearsay: Digital evidence often involves statements made by individuals outside of court, such as emails, text messages, or social media posts.[xi] Hearsay rules can pose challenges in admitting such evidence, particularly if the statements are being offered to prove the truth of the matter asserted.

Chain of Custody: Maintaining a proper chain of custody for digital evidence is crucial to demonstrate that the evidence has not been tampered with or altered during its collection, preservation, and presentation in court. Any breaks or inconsistencies in the chain of custody can weaken the evidence's admissibility.

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

Complex Technology: Many types of digital evidence involve complex technology, such as encryption, data recovery, and digital forensics.[xii] Courts might struggle to understand the technical aspects, leading to challenges in determining the evidence's reliability and relevance.

Privacy Concerns: Admitting certain types of digital evidence might raise privacy concerns, especially when personal or sensitive information is involved. Balancing the need for evidence with individuals' privacy rights can be a delicate matter.

Data Collection Methods: The methods used to collect digital evidence can impact its admissibility. If the evidence was collected improperly, without legal authorization, or in violation of data protection laws, it might be deemed inadmissible.

Metadata and Context: Metadata, while valuable in establishing the origin and history of digital evidence, can also be manipulated or misinterpreted.[xiii] Courts might question the accuracy of metadata and its role in providing context.

Expert Testimony: Presenting and explaining digital evidence often requires expert testimony from professionals in fields such as digital forensics, cyber security, and computer science. Ensuring that these experts are qualified and their testimony is understandable to the court can be a challenge.

Rapidly Evolving Technology: Digital technology evolves quickly, and new forms of evidence and methods of manipulation emerge regularly. Courts may struggle to keep up with these developments and accurately assess the reliability of novel forms of digital evidence.

Adapting Legal Frameworks: Existing legal frameworks might not be well-suited to dealing with digital evidence. Laws and regulations can be outdated and not fully account for the complexities of digital information.

Cross-Border Considerations: Digital evidence might be stored across different jurisdictions, which can complicate issues of jurisdiction, data protection laws, and international legal cooperation.[xiv]

Credibility Challenges: Digital evidence can sometimes be challenged on the grounds of credibility, with arguments that it was fabricated, edited, or manipulated to serve a particular agenda.

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

To address these challenges, legal professionals often work closely with experts in digital forensics, technology, and privacy to ensure that digital evidence is properly collected, preserved, and presented in a manner that withstands legal scrutiny.[xv] Additionally, legal systems and rules of evidence are adapting to accommodate the realities of digital information and technology.

LEGAL PRECEDENTS AND CASE LAW

The admissibility of digital evidence in legal proceedings is a complex and evolving area of law. Courts around the world have been grappling with various issues related to the authenticity, reliability, and integrity of digital evidence.

General Principles and Challenges

Best Evidence Rule: This rule generally states that the best available evidence, which is often the original or a reliable duplicate, should be presented in court.[xvi] In the context of digital evidence, this can raise questions about the integrity and authenticity of electronic records.

Hearsay Rule: Hearsay is an out-of-court statement offered in court to prove the truth of the matter asserted. Digital evidence, such as emails or social media posts, can sometimes be considered hearsay, raising issues of reliability and authenticity.[xvii]

Authentication: One of the key challenges with digital evidence is establishing its authenticity and proving that it has not been tampered with. Courts often consider factors such as metadata, digital signatures, and the chain of custody to determine authenticity.

Notable Cases

Lorraine v. Markel American Insurance Company (2007): This case is often cited for its discussion of the authentication of electronic evidence. It highlights the importance of establishing the reliability of processes that generate electronic records.[xviii]

United States v. Vayner (2008): In this case, the court discussed the authentication of social media evidence. It emphasized the need to establish that the social media profile in question indeed belonged to the person it was attributed to.[xix]

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

State v. Stubblefield (2012): This case dealt with the admissibility of text messages as evidence. The court considered factors like the circumstances of the discovery of the messages and the overall context in determining their admissibility.[xx]

Sedie v. United States (2018): This case highlighted the importance of authenticating digital evidence and discussed the role of metadata in establishing its credibility.[xxi]

State v. Granville (2019): The court in this case discussed the admissibility of electronic copies of original paper records and emphasized the need to establish the accuracy and reliability of the conversion process.[xxii]

Anvar P.V. v. P.K. Basheer & Others (2014): The Supreme Court of India in this case emphasized the importance of adhering to the rules of evidence while admitting electronic records, including secondary evidence of electronic records. The court stated that the person who seeks to rely on electronic records must prove its authenticity in the same way as any other document.[xxiii]

State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru (2005): This case laid down the criteria for admissibility of electronic records under the Indian Evidence Act, 1872. The court held that the electronic evidence must be relevant, authentic, and properly identified.[xxiv]

Shamsher Singh Verma v. State of Haryana (2011): The Supreme Court held that digital evidence like electronic records, including CDs, DVDs, and pen drives, is admissible if it is proved in accordance with the provisions of the Indian Evidence Act.[xxv]

State of Maharashtra v. Dr. Praful B. Desai (2003): In this case, the court emphasized the need for certification of electronic evidence under Section 65B of the Indian Evidence Act. This section deals with the admissibility of electronic records, including computer printouts.[xxvi]

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020): The Supreme Court clarified the requirements for admissibility of electronic evidence under Section 65B of the Indian Evidence Act. The court held that the certificate required under Section 65B(4) must accompany the electronic record when it is produced in evidence, and non-compliance with this requirement renders the electronic evidence inadmissible.[xxvii]

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

Zahira Habibulla H. Sheikh v. State of Gujarat (2004): While this case is not exclusively about digital evidence, it highlighted the importance of fair trial and the credibility of evidence in criminal cases, which has implications for the admissibility of digital evidence as well.[xxviii]

FUTURE TRENDS AND POLICY CONSIDERATIONS

The admissibility of digital evidence is a dynamic field influenced by technological advancements and evolving legal standards. Here are some future trends and policy considerations that may shape the admissibility of digital evidence:

Blockchain and Cryptography: Blockchain technology offers a tamper-proof and transparent way to record transactions. It could play a significant role in ensuring the integrity and authenticity of digital evidence.[xxix] Courts may need to consider the admissibility of evidence stored on blockchains and the legal status of blockchain records.

Machine Learning and AI: As AI and machine learning systems generate and analyze more data, courts will need to address the admissibility of evidence produced by these systems. Policy considerations might include establishing standards for validating the reliability and accuracy of AI-generated evidence.

Metadata and Provenance: Metadata, which provides information about the origin and history of digital files, can be crucial in establishing the authenticity and chain of custody of digital evidence.[xxx] Policy frameworks might evolve to ensure the proper handling and preservation of metadata.

International Standards: With the global nature of digital evidence, international standards for handling and admitting such evidence may become more relevant. Policymakers could consider harmonizing rules and standards across jurisdictions to facilitate cross-border legal proceedings.

Cloud and Remote Storage: As more data is stored remotely on cloud servers, challenges related to access, authenticity, and jurisdictional issues may arise. Policies might be developed to address these challenges and ensure fair and reliable use of cloud-stored evidence.[xxxi]

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

Privacy and Data Protection: Striking a balance between using digital evidence for justice and protecting individuals' privacy rights will continue to be a consideration. Courts and policymakers may need to establish criteria for the collection and admissibility of evidence obtained from personal devices and online platforms.

Digital Signatures and Encryption: Ensuring the admissibility of electronically signed documents and encrypted communications will be important. Policies might address the legal recognition of digital signatures and encryption keys as evidence of authenticity.

Expert Testimony and Education: Courts may increasingly rely on expert witnesses to explain the technical aspects of digital evidence to judges and juries.[xxxii] Policymakers might consider standards for qualifying and training such experts to ensure accurate and unbiased information is presented.

Continuous Learning and Adaptation: Given the rapid pace of technological change, legal professionals, judges, and policymakers need to stay informed about the latest developments in digital technology and its implications for evidence. Regular training and education initiatives may become more crucial.[xxxiii]

Openness to Innovation: Policies and legal systems should remain adaptable to new technologies and methods of evidence collection, analysis, and presentation. This flexibility will allow the legal system to effectively incorporate innovations while ensuring fairness and reliability.[xxxiv]

Ultimately, the evolution of policy considerations will depend on a combination of technological advancements, legal precedents, societal expectations, and the need for a fair and just legal process. It's important for legal systems to strike a balance between embracing innovation and maintaining the integrity of the justice system.

CONCLUSION

Finally, we say that the admissibility of digital evidence stands at the intersection of law and technology, demanding a holistic and adaptive approach. Addressing challenges related to authenticity, evolving technology, privacy, and jurisdiction requires continuous collaboration among legal, technological, and ethical experts. As digital evidence continues to play an

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

increasingly central role in legal proceedings, courts must prioritize the development of comprehensive guidelines and standards to ensure the fairness and integrity of justice. Failure to do so could undermine the credibility of the legal system and erode public trust. Embracing the opportunities and challenges presented by digital evidence is not just a necessity, but a responsibility to uphold the principles of justice in a rapidly digitizing world.

ENDNOTES

[i] Good, Jonathon, and Daniel G. McAuley, 'The Science of Expert Testimony in Forensic Handwriting Analysis: A Case Study in Admissibility' [2019] Jurimetrics [59, 3], 299-328.
[ii] Kessler, Gary C., 'Computer Evidence: Collection and Preservation." [1992] Computers & Security [11, 4], 357-363.
[iii] Rothstein, Samuel J., 'Digital Evidence and the New Criminal Procedure." Notre Dame Law Review' [2019] Notre Dame Law Review [94, 3], 1209-1270.
[iv] Zeleznikow, John, 'Admissibility of electronically generated evidence: A dispute resolution perspective' [2019] Information & Communications Technology Law [28, 1], 51-66.
[v] Schwartz, J., & Ball, D., 'The admissibility of digital evidence in criminal prosecutions: A new approach' [2017] Virginia Journal of Law and Technology [21, 2], 1-52.
[vi] Zelechoski, Amanda, 'The Admissibility of Digital Evidence in Criminal Prosecutions' [2019] American Criminal Law Review [56, 3], 567-612.
[vii] Kohn, Alisha, 'The Emerging Admissibility of Snapchat Evidence' [2016] The John Marshall Journal of Information Technology & Privacy Law [32, 1], 153-171.
[viii] Casey, Mary, 'Digital Evidence and the US Federal Rules of Evidence' [2005] Digital Investigation [2, 4], 281-287.
[ix] Rasinger, & Sebastian M., 'Digital evidence in court: A cross-national comparison of judicial perspectives' [2019] Digital Investigation [30], 48-S56.
[x] Oke, Gbenga, and Akinkunmi Akintunde, 'Admissibility of electronically generated evidence in Nigeria: An overview' [2019] Computer Law & Security Review [35, 6], 719-729.
[xi] Quick, Darren. , 'Legal admissibility of digital evidence in criminal prosecutions: An overview' [2016] Digital Investigation [18], 29-37.
[xii] Brömme, Arslan, and Oliver Brömme, 'On the admissibility of digital evidence: a comprehensive analysis of the requirements in different jurisdictions' [2013] Digital Investigation [10, 4], 381-391.
[xiii] Luiijf, Eric, and Hadi Asghari, 'Challenges of digital evidence in the prosecution of cybercrime' [2013] Crime Science [2, 1], 6.
[xiv] Barney, Daniel A., and Patrick S. Duffy, 'Legal and ethical challenges for digital forensics' [2017] Handbook of Digital Forensics of Multimedia Data and Devices, 37-54.
[xv] Abraham, Bindu Sudhakaran, and Raghavendra S., 'Challenges in digital evidence and its admissibility in the Indian judiciary' [2019] Procedia Computer Science [167], 1663-1672.
[xvi] Casey, Mary, 'Digital Evidence and the US Federal Rules of Evidence' [2005] Digital Investigation [2, 4], 281-287.
[xvii] Zelechoski, Amanda, 'The Admissibility of Digital Evidence in Criminal Prosecutions' [2019] American Criminal Law Review [56, 3], 567-612.
[xviii] Wikipedia contributors, 'Lorraine v. Markel American Insurance Co.' (In Wikipedia, The Free Encyclopedia 2022) <https://en.wikipedia.org/w/index.php?title=Lorraine_v._Markel_American_Insurance_Co.&oldid=1088015246> accessed August 24, 2023.
[xix] COLE, J., 'The Brave New World of Internet Evidence: It's Not as Brave or New as It Seems' [2016] Litigation [42, 4], 37–42.
[xx] findlaw, 'UNITED STATES v. STUBBLEFIELD' (findlaw 2012) <https://caselaw.findlaw.com/court/us-6th-circuit/1611316.html> accessed 24 August, 2023
[xxi] Estrada, P.R.T., Bagatella, J.C.M., Ferrel, C.V. et al, 'Public policies against criminal assets in mexico: challenges and opportunities from the north border states' [2021] Crime Law Soc Change [76], 387–407.

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)

[xxii] Googlebooks, 'State v. Granville' (googleebooks 2019) <https://books.google.co.in/books?id=cd4XEAAAQBAJ&pg=PA82-IA2&lpg=PA82-IA2&dq=State+v.+Granville+(2019):&source=bl&ots=BFN2jykzcH&sig=ACfU3U2avqnKnwo5iT8E9bSOh5XjlGgdaA&hl=en&sa=X&ved=2ahUKEwiNyoaC7fWAAxXs2jgGHR0NCoEQ6AF6BAggEAM#v=onepage&q=State%20v.%20Granville%20(2019)%3A&f=false> accessed 24 August, 2023.
[xxiii] Kurian, 'Anvar P.V vs P.K.Basheer & Ors' (Indiakanoon 2014) <https://indiankanoon.org/doc/187283766/> accessed 24 August, 2023.
[xxiv] Chahakkanojia , 'Analysis: N.C.T of Delhi v/s Navjot Sandhu @ Afsan Guru' (Legal Service India 2005) <https://www.legalserviceindia.com/legal/article-9423-case-analysis-n-c-t-of-delhi-v-s-navjot-sandhu-afsan-guru.html> accessed 24 August, 2023.
[xxv] Pant, P C, 'Shamsher Singh Verma vs State Of Haryana' (Indiankanoon 2015) <https://indiankanoon.org/doc/55466355/> accessed 24 August, 2023.
[xxvi] Variava, 'The State Of Maharashtra vs Dr. Praful B. Desai' (Indiankanoon 2003) <https://indiankanoon.org/doc/560467/> accessed 24 August, 2023.
[xxvii] Nariman, Fali Rohinton , 'Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal' (Indiankanoon 2020) <https://indiankanoon.org/doc/172105947/> accessed 24 August, 2023.
[xxviii] Pasayat A., 'Zahira Habibullah Sheikh & Anr vs State Of Gujarat & Ors' (Indiankanoon 2006) <https://indiankanoon.org/doc/1067991/> accessed 24 August, 2023.
[xxix] Smith, R. A. , 'Admissibility of Digital Evidence in Court: Present and Future Challenges' [2018] Journal of Digital Forensics, Security, and Law [13, 2], 49-62.
[xxx] Simpson, L. G., & Marshall, P. I., 'The Future Implications of Artificial Intelligence on the Admissibility of Digital Evidence.' [2018] AI & Society [33, 4], 603-611.
[xxxi] Phillips, A. M., & Turner, B. L., 'Admissibility and Weight of Social Media Evidence in Litigation' [2017] Trial Evidence [44, 2], 16-21.
[xxxii] Fitzgerald, M., 'Digital Evidence and the Role of Blockchain in Ensuring Admissibility' [2021] Journal of Cybersecurity and Information Management [8, 1], 15-29.
[xxxiii] Quick, Darren, and Peter Green., 'The Challenges of Digital Evidence: A Review of Current Practice' [2016] Australian Journal of Forensic Sciences [48, 1], 47-59.
[xxxiv] Casey, Eoghan, and Chris Daykin., 'From Balancing Scales to Baking a Cake: A New Metaphor for the Authentication of Digital Evidence' [2020] Digital Investigation [32], 41-49.

ISSN 2581 3382
© All Rights Reserved – The Law Brigade Publishers (2023)