INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 4 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 4 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-4-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE STATUTORY EVOLUTION OF DIGITAL EVIDENCE JURISPRUDENCE: AN ANALYSIS UNDER THE BHARTIYA SAKSHYA ADHINIYAM AND INFORMATION TECHNOLOGY ACT

AUTHOR – KRATIKA MISHRA* & PROF. (DR) TAPAN KUMAR CHANDOLA**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – KRATIKA MISHRA & PROF. (DR) TAPAN KUMAR CHANDOLA, THE STATUTORY EVOLUTION OF DIGITAL EVIDENCE JURISPRUDENCE: AN ANALYSIS UNDER THE BHARTIYA SAKSHYA ADHINIYAM AND INFORMATION TECHNOLOGY ACT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (4) OF 2026, PG. 829-840, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I477

ABSTRACT

This paper argues critically the position, its admissibility in the court, and practical issues relating to digital evidence in contemporary criminal justice administration of cybercrime. With the rapid digitalization of the society, electronic records have become the centre of attention of criminal investigations. The current project involves use of a doctrinal research methodology to examine the process of replacing old aspects of evidentiary rules with newly updated systems, in this case, India, Bharatiya Sakshya Adhiniyam (BSA) and Information Technology (IT) Act, 2000. It discusses the hard statutory prerequisites of authenticity and the chain of custody that cannot be negotiable in order to overcome the volatility of data as it is. Additionally, the paper has also found that administrative bottlenecks that create severe obstacles such as technical challenges, such as end-to-end encryption, and procedural failures, such as ineffective forensic infrastructure and occurrence of transnational jurisdiction issues are a significant impediment to advancing AI use in cybercrime. Analysing the landmark Supreme Court decisions, the study shows inescapable errors in judicial practise. Finally, the paper concludes that the substantive laws have been developed, but the practical implementation remains behind, suggesting that the creation of the cyber court system and more forensic preparation should be implemented as soon as possible to protect criminal justice in the era of modernity.

KEYWORDS: Bhartiya Sakshya Adhiniyam, Information Technology, Artificial Intelligence, Cybercrime.

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

High rate of digitization of the society has essentially changed criminal activities with the emergence of sophisticated cybercrimes.[1667] Therefore, digital evidence is becoming more and more the new reality of the criminal justice system, as emails, server logs, etc., are used to research and prosecute crimes. Since physical evidence has played the second fiddle, the complexity of electronic records has come to the forefront, especially as far as the law enforcers and the courts are concerned in delivering just, precise and practical justice in the present day.[1668]

[1667] V.K. Unni, *Cyber Crimes and the Indian Legal Framework*, 21 J. Marshall J. Computer & Info. L. 355 (2003).

[1668] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279 (2005).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1.2 Significance of the Study

The present research is quite important as it gives a critical analysis of the changing legal provisions that regulate digital evidence.[1669] It provides an insight into the practical difficulties and evidentiary challenges, thus helping lawmakers, legal professionals, and investigators to balance the use of technology and the promotion of procedural fairness and legal predictability.

1.3 Literature Review

The literature available abounds with the basics of electronic evidence. Such analysts as Stephen Mason focus on the technical weaknesses of digital records, and jurisprudence books break down admissibility criteria, especially the need to have a statutory certification.[1670] Recent journals point to such new threats as deepfakes and cloud forensics. Nevertheless, technical forensics and legal admissibility are largely discussed in literature in isolated silos as opposed to an integrated challenge. The discussion is often lagging behind the rapid changes in technology, which have shown an ongoing necessity to constantly revise the focus of study in such a way that incorporates the technical aspects of the contemporary world along with the legal practises.[1671]

1.4 Research Questions

1. Which are the most crucial legal and technical conditions that define whether digital evidence can be accepted in court or not?
2. What is the impact of the current technological advances on the current procedural and statutory frameworks?

1.5 Research Objectives

1. To examine the legal framework of the admissibility of the digital evidence.
2. To determine technical and procedural problems of investigators.
3. To propose the reforms in the law dealing with the electronic evidence effectively.

1.6 Hypothesis

The existing laws and legal processes lack the skills needed to deal with the complexity, unpredictability and international ease of present digital evidence, which creates discrepancy in the delivery of criminal justice.

1.7 Research Methodology

The research methodology used in this project is a doctrinal research. It is based on the secondary sources, such as statutes, judicial precedents, legal treatises, and peer-reviewed journals. The analytical method is applied to analyse the current legislations, review landmark cases, and analyse how technology and procedural laws interact with each other in the criminal justice system.

1.8 Scope of Study

This paper is limited to the admissibility of digital evidence in cyber crimes, the legal aspects related to the procedures and the legal usefulness of the evidence. It should mainly be concentrated on the legal system of the Indian setting, areas of the statutory provisions and current trends in the judicial system with references to the general concepts of technology that may be implemented in the contemporary forensics.

1.9 Limitations of Study

The limited number of words allows makes this study a condensed analysis, as opposed to a comprehensive commentary. Moreover, the dynamic and ever-changing environment of the technology implies that some of the modern cyber threats or new forensic techniques remain unexplored in the narrow scope of the given brief project.

[1669] Apar Gupta, *The Admissibility of Electronic Evidence in India*, 11 Indian J. L. & Tech. 1 (2015).
[1670] Stephen Mason & Daniel Seng, *Electronic Evidence and Electronic Signatures* 45 (5th ed. 2021).
[1671] Karnika Seth, *Computers, Internet and New Technology Laws* 112 (3rd ed. 2022).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CHAPTER 2: CONCEPTUAL FRAMEWORK OF DIGITAL EVIDENCE

2.1 Defining Digital Evidence in the Modern Era

Digital evidence refers to any probative information that can be stored or transmitted in digital form that can be used by a party to a court case in court.[1672] This goes well beyond computer files in the modern world to encompass emails, social media chat, GPS positioning of smartphones, logs on a server, the Internet of Things (IoT) device metrics, and blockchain transactions among others. Digital evidence, as opposed to physical evidence, is latent, and this requires special equipment and knowledge to be extracted, interpreted, and placed in a readable human form.[1673] Since cyber crimes are on the increase, it is important to broadly define digital evidence to detect the digital footprint that contemporary criminal people have left behind.

2.2 Characteristics and Nature of Electronic Records

This quality of electronic records makes them very different compared to the normal physical evidence. To start with, digital evidence is very volatile; information that may be contained in Random Access Memory (RAM) or transient networks is destroyed immediately a system is shut down.[1674] Second, it is essentially weak. Electronic records are relatively easy to modify, corrupt, or destroy either by malicious individuals or unintentionally through misuse. Third, electronic information can be copied endlessly. It is not like a tangible weapon such as a physical one where once an item is copied it becomes incomplete and thus difficult to determine the original source. Lastly, it can frequently include hidden metadata such as data about data e.g. creation dates, author information and file paths.[1675] These peculiarities predetermine that common criminal scene instructions are not enough; these are special regulations that are needed to ensure the integrity and admissibility of electronic documentaries as one of the legal resources in the process of court trials.

2.3 The Role of Digital Evidence in Cyber Investigations

In the contemporary cyber investigations, digital evidence has been supporting, as it is often the only linkage between a culprit and an offence. Its role is multifaceted. It is mostly applied in the process of rebuilding digital crime scenes.[1676] Investigators are able to identify the path of the exact sequence of events by examining the system logs, the registry and network traffic and identify how a system was compromised and what data was stolen. Besides, the digital evidence plays a great role in proving the intent and attribution. Communication logins, coded messages, and transactions traced on digital ledgers are evidence of mens rea and can be used to link pseudonymous internet identity to other identities in the real world.[1677] In addition to the purely cyber-dependent group of crimes well documented through prosecution such as hacking, malware deployment, and even ransomware distribution, digital evidence is becoming critical on the traditional crimes that include financial frauds, human trafficking, and even murder, whereby the smartphones and the GPS system have delivered ways to provide irrefutable information with regard to time and location vulnerability. Also, it helps in innocent boys being cleared of blame due to the corroboration of the alibis by verifiable digital footprints. In the end, it is the task of digital evidence to convert intangible binary code into an interesting, rational narrative that courts can appraise and as such is the unquestioned key to the effective administration of criminal justice nowadays.

[1672] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* 24 (3rd ed. 2011).
[1673] Id. at 30.
[1674] M.K. Geetha, *Evidentiary Value of Electronic Records in Criminal Justice System*, 9 Crim. L.J. 112 (2020).
[1675] Ryan Williams, *The Probative Value of Electronic Evidence*, 31 Harv. J.L. & Tech. 199 (2017).
[1676] Ministry of Home Affairs, *Manual on Cyber Crime Investigation*, Gov't of India (2019).
[1677] Pavan Duggal, *Cyberlaw: The Indian Perspective* 88 (2015).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

2.4 The Standard Digital Forensics Process

Digital evidence should be digitally admissible, thus the investigators follow a standardised digital forensics procedure. The general stages of this are four rigid steps, namely, Identification, Collection, Analysis, and Reporting. Identification is the initial step that should be carried out on a crime scene, whereby any possible electronic evidence is identified, beyond the conventional devices. Then, there should come Collection, or acquisition which should not distort the original data. Write blockers are used by the investigators and cryptographic hashes (such as MD5 or SHA-256) are generated to allow the precise bit-by-bit imaging of the storage media without alteration.[1678] Analysis phase is a part of recovery of deleted files, decryption of data and reconstruction of the history of crime based on the digital evidence. Last but not the least, Reporting is the process involving the translation of the highly technical findings into the understandable format of the judiciary, giving details of the methodology employed in ensuring the chain of custody was not broken at any point in time. This is a strict approach that can not be compromised in demonstrating evidentiary authenticity in court.

CHAPTER 3: STATUTORY FRAMEWORK GOVERNING ELECTRONIC EVIDENCE

3.1 Overview of the Cyber Legal Regime

The legal basis of the cyber crimes and electronic evidence in India has undergone development in order to adapt to the digital revolution. The regime at first depended much on Information Technology (IT) Act, 2000, which was to offer legal sanction on electronic transactions and define cyber crimes.[1679] Nevertheless, the criminal law, both substantive and procedural, also needed urgent modernization. Thus, India has shifted to a new model of laws replacing the colonial laws with the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA).[1680] The integrated regime establishes a complete legal ecosystem in an effort to deal with the realities of current cyber justice administration.

3.2 Evidentiary Laws and Electronic Records

In India, the historic legal basis of admissibility of digital evidence was the Indian Evidence Act, 1872, Section 65B. According to this provision, certain certificate was required to verify the authenticity of the electronic records, which meant that the computer system was functioning correctly and that information was not altered. This structure has further been updated due to the newly established Bharatiya Sakshya Adhiniyam (BSA) 2023. Within the BSA, the electronic records have been clearly given the legal consideration that is given to the conventional documents.[1681] Section 63 of the BSA is concerned with the admissibility of electronic records, which makes it clear that adequate certification should be made in an effort to establish authenticity.[1682] More importantly, the BSA broadens the definition of electronic evidence to clearly encompass the mobile phone digital records, server logs, locational evidence, and cloud-based information. The high stipulation to certification will guard against the factual vulnerability and instability of the digital information so as not to jeopardise the integrity of the trial. Through their requirement to adhere technically, the evidentiary laws are an objectively strict gatekeeper, which can be used to philtre manipulated or unreliable digital artefacts before they can be introduced to affect the decisions of the judiciary. This legal development is the key point of recognition by the judiciary: even though digital evidence is extremely necessary, its admission must be under strict procedural presuppositions to preserve the integrity of the criminal justice

[1678] Rakesh Kumar, *Challenges of Cyber Crime Investigation in India*, 5 Int'l J. Cyber Criminology 489 (2011).
[1679] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[1680] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[1681] Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India).
[1682] S. Chakraborty, *Digital Evidence and its Admissibility: A Critical Analysis of Section 65B of the Indian Evidence Act*, 8 NLUJ L. Rev. 45 (2021).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

administration against criminal technological manipulations.

3.3 Information Technology and Cyber Crime Legislation

The Information Technology (IT) Act, 2000, is still the main special law in the sphere of the cyber crimes in India.[1683] It elaborates on substantive offences of unauthorised access to computers, data theft, propagation of malware and identity theft as per Sections 43 and several additional subsections of Section 66. It also criminalises the communication of sexually explicit electronic content under the Section 67. More importantly, the Act has got extra-territorial jurisdiction which is theoretically the authorities can be able to prosecute crime committed on the computer networks that are located in India irrespective of the physical whereabouts of the offender anywhere in the world. Moreover, the new legislation introduced as the Bharatij Nyaya Sanhita, 2023, contains specifically provisions addressing digital forgery, cyber fraud, and technologically enabled organised crimes that form a strong substantive deterrence to the IT Act. The IT act also sets up the principle of intermediary liability, a legal bond in which the internet service providers are obligated to cooperate with law enforcement to maintain and decrypt important digital data. Nonetheless, the governing of such advanced offences as state-sponsored cyberattacks, ransomware, and deepfakes constantly tests the limits of such laws. As a result, the area of cyber laws is often limited to a reactive position, where the courts have to be creative in adapting the time-honoured criminal principles into unknown digital environments to make justice effective and prevent syndicates, which take advantage of the law loopholes.

3.4 Interplay Between Procedural and Substantive Law

Effective legal action of cyber crimes solely depends on the smooth interrelation between substantive and procedural laws. Whereas the substantive laws, such as the IT Act and BNS, describe the offences and the sanctions to be applied to perpetrators, they can only be effectively implemented in the context of the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the standards of evidence provided by the BSA. The critical stages in search, seizure, and investigation of digital devices are regulated by the BNSS to observe the constitutional rights.[1684] In the meantime, the BSA determines the way extracted data is introduced in the court. Violation of a procedural compliance will always render the substantive digital evidence to be inadmissible in the court of law, and the prosecution will collapse.[1685]

CHAPTER 4: LEGAL ADMISSIBILITY AND EVIDENTIARY VALUE

4.1 The Concept of Admissibility vs. Authenticity

Regarding digital evidence, the knowledge of the difference between admissibility and authenticity is central to the administration of criminal justice.[1686] The term admissibility is related to the legal quality of evidence that defines the possibility to formally present it and accept it in the court. This is largely a law issue, controlled by the rules and the steps set out in statutes. On the other hand, authenticity is a question of truth of fact: is it what the proponent of the digital record actually says it is? Evidence can be found legally admissible yet not authentic in case of interference with it. In the case of electronic records authenticity is distinctly difficult, because it is volatile. The only way to prove it is to show that the data has not been modified between creation and collection and presentation. Thus although the laws in place such as the Bharatiya Sakshya Adhiniyam define the principles of admissibility, strong forensic science and expert testimony are quite necessary to prove the under-pinning authenticity of the digital artifact in the

[1683] The Information Technology Act, 2000, § 43.

[1684] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).

[1685] Yatindra Singh, *Cyber Laws* 55 (6th ed. 2016).

[1686] Tejas Karia, Akhil Anand & Bahaar Dhawan, *The Supreme Court of India Re-defines Admissibility of Electronic Evidence*, 12 Digital Evidence & Elec. Signature L. Rev. 33 (2015).

presence of the judge of a court of law during a trial.[1687]

4.2 Overcoming the Hearsay Rule in Digital Contexts

Hearsay rule has always been oblivious to out-of-court utterances that seek to support the veracity of the fact that is claimed, which is a major challenge to digital evidence.[1688] Since computer generated records e.g. server logs or automatic timestamps are generated oblivious to human awareness, courts were at first confused as to how to classify them. Are they hearsay? The current jurisprudence makes a distinction between computer generated records and computer stored records. Human statements are stored in the records of a computer such as an email written by a suspect, and like most forms of hearsay, are usually subject to the traditional hearsay exceptions, including admissions against interest. On the other hand, computer generated records which are generated by the workings of the system automatically, with no human interference is becoming considered as real evidence as opposed to hearsay. Laws have now laid down certain processes, such as certification by the Bharatiya Sakshya Adhiniyam, to conquer the hearsay objections. The proponents can effectively evade the hearsay rule by proving that the computer was in reasonable operation and the data had been generated when the normal operations were going on. Digital records are admissible.[1689]

4.3 The Critical Importance of the Chain of Custody

Chain of custody The chronological record, or paper trail, of the sequence of custody, control, transfer, analysis, and disposition of electronic evidence. The most important thing in digital forensics is ensuring that a chain of custody is unbroken since the electronic records are prone to some form of invisible modification, destruction, or corruption.[1690] When there is a slash in the chain of command it is just easy to claim by the opposing attorney that the evidence has been affected and can, therefore, not be legally used or completely deprive of its probative nature. To remain in this chain, it takes careful process once a device is captured. Investigators are required to disconnect devices in networks to avoid remote wiping, employ specific hardware used to write-block during collection of data, and to create cryptographic hash values (SHA-256) of original data.[1691] The meanings that we give to these hash values are the digital fingerprints; even a change of one bit of data during the analysis causes the change in the hash value and immediately points to the court about the tampering activity. Any person working with the evidence is to sign the custody log reporting what they did to the evidence and how long they have carried it. Finally, ironclad chain of custody is the reason judicial faith in the forensic process because the digital evidence presented in the courtroom is the very same data collected at the crime scene and ensures that this was not altered.

4.4 Probative Value of Digital Evidence in Court

After overcoming the challenges of admissibility and authenticity, the court then has to see that digital evidence has probative value; the intensity or convincing ability that the evidence has towards proving a fact in dispute. In contemporary probation of cyber crimes of criminal justice management, electronic records may have a probative value of high degree of certainty or a circumstantial one. To provide an example, cryptographically secure blockchain registries or digitally signed agreements have a tremendous probative mass since they are structurally difficult to use.[1692] The same way, GPS location information supporting a physical presence of a suspect at a crime scene underlines impressive objective evidence. The probative value of digital evidence however is less when the digital

[1687] Id. at 35.
[1688] Apar Gupta, supra note 3, at 14.
[1689] Eoghan Casey, supra note 6, at 102.
[1690] Ministry of Home Affairs, supra note 10, at 45.
[1691] Ryan Williams, supra note 9, at 205.
[1692] M.K. Geetha, supra note 8, at 115.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

evidence is alone and unaccompanied by corroborating evidence particularly when they use shared computers or when the IP addresses are spoofed because it can be difficult to state with certainty that the digital act is caused by a particular human actor. Courts are naturally conservative in nature and in a given case, additional traditional evidence may be needed to help put the digital evidence into perspective. A judge will consider the accuracy of the tools and methods deployed in forensics, the experience of the witnessing analyst and the strength of the chain of custody. Therefore, although admissible digital evidence in court opens the door to the court, its final probative value is solely determined by its capacity to create an unimpeachable, logical cause and effect chain between the accused and the crime.

CHAPTER 5: COMPLEXITIES AND CHALLENGES IN ADMINISTRATION

5.1 Technical Hurdles

The technical challenges to criminal justice administration are probably more than ever before with cyber criminals having highly entrenched countermeasures. First of all is the widespread application of end to end encryption. [1693]On the one hand, the encryption of legitimate communications and commerce should ensure that investigators cannot access vital evidence that may be used to resolve a crime, a phenomenon called going dark. The police are used to decrypting information without cryptographic decision keys that they cannot read. Moreover, offenders are addressing the problem with anti-forensics equipment (data wiping tools, steganography (concealing data in the files) and IP spoofing) that is tailor-made to defuse the investigation and erase the digital footprint. Moreover, the intensive development of the Artificial Intelligence (AI) is adding one serious stratum of complications.[1694] The so-called deepfakes, AI-created hyper-realistic manipulated audio and video, are aimed at the very core of the evidentiary reliability. When the digital evidence can be created in such a manner that it sounds much real, courts find it difficult to know the difference between true documents and malicious fake ones. It is necessary to ensure that forensic analysts keep coming up with new verification algorithms in order to identify microscopic anomalies in digital media. These emerging technical interventions determine that the tools that are being employed by the police have to be constantly and heavily upgraded merely to keep pace with a minimum requirement of their operation against technologically oriented criminal operations.

5.2 Procedural and Infrastructural Deficits

In addition to technical countermeasures, criminal justice system has been greatly handicapped by the lack of procedural and infrastructural shortages. It has a persistent lack of sufficiently trained first responders, specialised cyber investigators. Conventional police departments are not always technically literate to handle volatile digital evidence in a manner that will allow its correct identification and seizure without its accidental alteration and, thus, the breach of the chain of custody during the first step. Also, state-sponsored forensic infrastructure is critically and progressively underdeveloped. The digital device volume in criminal cases is often overwhelming to state and regional cyber forensic laboratories and causes enormous backlogs.[1695] One modern smartphone may store terabytes of information that may take weeks to analyse. This structural shortcoming leads to excessive delays in the processes, which infringes with the right to a prompt trial of the accused and enables digital tracks to become obsolete before being processed in investigations that require time.[1696]

[1693] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013).
[1694] Karnika Seth, supra note 5, at 210.
[1695] Rakesh Kumar, supra note 12, at 492.
[1696] Id. at 495.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

5.3 Jurisdictional and Cloud Storage Dilemmas

Digital evidence inherently defies the geographical line, which poses significant jurisdictional problems on law enforcement. Contemporary cyber criminality is transnational in nature; a malefactor in one nation uses a server in a second one to defraud a third country victim. The traditional criminal justice administration is a territorial one basing on physical warrants and local jurisdiction. This is, however, no longer the case, as much of the contemporary digital evidence is not located on the physical machine of the suspect, but instead in the cloud, scattered over servers in other jurisdictions. In cases where the domestic investigators are required to access email or get social media logs that are stored on server in other locations, local warrants are not enough. In its place they have to depend upon Mutual Legal Assistance Treaties (MLATs). [1697]The MLAT process is infamously bureaucratic, cumbersome and sluggish and in most cases it takes months or years to implement. Before the process of foreign data being officially secured, the criminal racket has most often disappeared. Another drawback of cloud storage is the complicated issue of data sovereignty and legality of extraction of remote cross-border data, which often puts investigators in an area of legal uncertainty.[1698]

5.4 Balancing Privacy Rights with Investigative Needs

The last and the biggest issue is on whether there should be a trade off between the basic right to privacy and proper investigation by the state. The common smartphones and laptops are not the filing cabinets; they are the all-inclusive archives of the personal, medical, financial, and sexual life of a person. Therefore, the seizure of such machines and the search signify an enormous invasion of the privacy of the individual.[1699] Courts are also subjecting greater scrutiny to the manner in which digital searches are handled to maintain that such searches do not extend to some procedural overreach or are not carried out as fishing expeditions by the law enforcement. The main legal issue is the determination of the proper area of a digital warrant. Is a right of an investigator seeking money-related crimes to go through the personal photographs or coded message apps of the suspect? Coming up with procedural protections which enable the police to obtain pertinent digital evidence whilst nevertheless providing legal protection to unrelated, extremely sensitive personal information is a hotly debated one, and courts, to stay within the boundaries of the fourth amendment and amicable justice, must continuously make minor adjustments to the scales.

CHAPTER 6: JUDICIAL TRENDS AND CRITICAL ANALYSIS

6.1 Evolution of Jurisprudence on Electronic Evidence

The jurisprudence of electronic evidence in India has gone through an incredible transformation, whereby, the courts were already lenient in the actions of the prosecuting and accused parties, but now are strict in consistently following the procedures. Original courts categorised digital records equally as other paper documents and in many cases, skipped the specialised certification provisions of Section 65B of the Indian Evidence Act.[1700] It was common to find that judges accepted electronic evidence as general testimony by witnesses and this is indicative of a battle by the judiciary to understand the vulnerability of digital information. Nevertheless, the Supreme Court evolvedly course-corrected with the realisation of the intricacies of digital manipulation. Judiciary realised that electronic records are highly prone to tampering and therefore high requirements must be used. The development of this led to the formation of technical certification to act as a necessary condition to admissibility. Now easily becoming

[1697] Pavan Duggal, supra note 11, at 150.
[1698] Orin S. Kerr, supra note 2, at 285.
[1699] Law Commission of India, *Report No. 277: Wrongful Prosecution (Miscarriage of Justice): Legal Remedies* (2018).
[1700] S. Chakraborty, supra note 16, at 50.

part of the strategy of the Bharatiya Sakshya Adhiniyam (BSA), this conservative approach to interpretation is the foundation of the digital jurisprudence, so that the technological progress does not disrupt the wholeness of the criminal justice administration system or the original right to a fair trial.

6.2 Analysis of Landmark Judicial Pronouncements

A three-decade series of Supreme Court landmark cases would be the best way to comprehend the trajectory of digital evidence admissibility. First, in the case of State (NCT of Delhi) v. Navjot Sandhu[1701], the Court took a very lenient stance, the Court, adopted a rather lenient decision, in which the secondary electronic evidence could be introduced as general evidence evidence without a certain statutory certificate. This virtually watered down the legislative protection against computer sabotage. On uncovering this vital weakness, a bigger bench in Anvar P. V. v. P.K. Basheer[1702] clearly quashed Navjot Sandhu. As held by the Court in Anvar, it created a stern legal precedent: any electronic record cannot be used as secondary evidence unless there is the obligatory certificate at the time of their creation. This case settled the authenticity requirements to the ground. This literal meaning, however, formed practical difficulties on the part of investigators who found it difficult to obtain certificates of uncooperative third-party device owners. As a way out of this stalemate, the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[1703] clarifying it was definite. It confirmed that the certificate is a non-derogable precondition, which is needed as the obligatory precondition to admission. However, it made an expedient caveat, that in cases where an investigating authority has availed themselves of every available method of obtaining the certificate, and where they fail because of forces outside their power, the court may waive the condition. All these pronouncements indicate a highly delicate judicial balancing act a need to make sure that the absolute integrity of the electronic records is upheld and at the same time technical impossibility is not allowed to stall criminal prosecutions.

6.3 Inconsistencies in Judicial Application

Although these laws have been clarified through the rulings of the apex court, there are still many inconsistencies on how these laws are applied every day by the lower courts. Relevant courts often have a hard time in determining the exact time restrictions of submitting electronic certificates.[1704] Although jurisprudence indicates that the certificate must be a part of the charge sheet, lower courts are inconsistent in allowing the submission of the certificate at the later stages of a trial process, which results in a lack of procedural clarity and slows down the process of justice. Moreover, the discretionary rule of exception that was differentiated regarding receiving third-party certificates is randomly utilised. Other judges inflexibly reject crucial digital evidence when the certificate is prevented due to technical bureaucratic obstacles and are too lenient to an extent of admitting unauthenticated information. Also, a dramatic mismatch exists regarding the consideration of the probative practise of complex evidence such as blockchain records or encrypted communications in court.[1705] Such inconsistency in judicial decisions among jurisdictions brings inconsistency to the administration of cyber crime and destroys certainty of the law by encouraging cybercriminals who manipulate the inconsistencies of processes.

6.4 The Need for Specialized Cyber Courts

The very deep technicalities of the topic and the continuous judicial contradictions are strong arguments in favour of the creation of special

[1701] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India).
[1702] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
[1703] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).
[1704] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).
[1705] *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178 (India).

cyber courts.[1706] The conventional criminal courts are grossly overstretched and predominately lack technical expertise to convict any highly advanced digital forensics, algorithmic biases, or sophisticated cryptographic files. Special cyber courts under the supervision of specially trained judges with specialised training in computer science and computer jurisprudence would enhance the speed and precision of the contemporary criminal justice administration significantly. Such special forums would be able to quickly assess the admissibility of volatile electronic records, learn the subtleties of cloud-based jurisdictional issues and actively utilise the complex evidentiary models. The use of specialised courts would remove systems backlog since expert digital trial processes are integrated into the judiciary. Finally, an upgraded, committed legal infrastructure ceases being a fringe benefit of the administration but an essential requirement against the changing environment of advanced cyber criminality.

CHAPTER 7: CONCLUSION AND RECOMMENDATIONS

7.1 Summary of Key Findings

Digital evidence is a subject of the comprehensive analysis conducted in the current criminal justice administration, and several issues are essential findings. To begin with, digital evidence has ceased being a supportive investigative mechanism instead of the main point of proving criminal liability in both cyber and conventional offences. This however, with regard to its nature of volatility, fragility and duplicability, requires unbelievably strict forensic procedures. Second, although the legal shift to the Bharatiya Sakshya Adhiniyam (BSA) is more sophisticated as it offers a modernised framework that records the electronic records as an explicit consideration, law admissibility remains to be a necessity based on high qualifications to defy hearsay and establish veracity. Third, a continuous line of custody is inadmissible to proving the probative value of digital records in the court. Fourth, police have a dire infrastructural and technical challenge, such as the spread of end-to-end encryption, anti-forensics, and deepfakes generated with AI. Moreover, the research on jurisdictional issues of cloud-based data storage can be seen as a significant hindrance to timely investigations hindered horrifically by significantly bulky Mutual Legal Assistance Treaties (MLATs). Lastly, lower courts do not always apply these rules uniformly in spite of the fact that clarification of Supreme Court judgement requires statutory certificates. The technical illiteracy of conventional judicial personnel and first responders remains a bottleneck in successful prosecution of high tech cyber crimes with a potential endemic failure of system to keep up with the quick change in technology and procedures.

7.2 Testing of the Hypothesis

These results of this research are a conclusive support to the hypothesis formulated. Even with the appointment of modernised acts such as the Bharatiya Sakshya Adhiniyam, the actual procedural machineries involved in forensic collection and international data retrieval are still grossly enlightened to cope with the speed, volatility and transnationality of the current digital crimes. State forensics are routinely overwhelmed by technical countermeasures, including deepfakes and advanced encryption, and chronic infrastructural shortages are being used to create drastic delays in investigations. Therefore, such technical and procedural deficiencies are a direct consequence, leading to the lack of uniform judicial treatment and unpredictable trials outcome that is now afflicting the contemporary cyber crime criminal justice administration.

7.3 Recommendations for Legal and Procedural Reform

In order to eliminate the mentioned shortcomings, a number of immediate reforms are suggested. To start with, the creation of special, technology-dotted, cyber courts is the

[1706] Yatindra Singh, supra note 19, at 120.

most important. To enhance the application of complicated evidentiary laws in a speedy and consistent manner, these courts need to be led by judges who have specialised knowledge on digital jurisprudence. Second, the state needs to make substantial investments in extending and upgrading regional cyber forensic labs to get rid of paralysing evidence pipes and supply investigators, with the latest decryption and anti-deepfake gear. Third, regular and compulsory technical training sessions should be established to all the first responders so that volatile digital evidence is legally preserved at the crime scene without tampering with the chain of custody. Fourth, the governments should intensify efforts in modernising the treaties on Mutual Legal Assistance (MLATs) and negotiate bilateral agreements on data sharing to hasten the process of obtaining cloud-based evidence across national borders. Lastly, certain procedural rules on strike of the balance between privacy rights and digital search warrants are to be proposed by the legislature so that the investigators would be able to retrieve the required data without engaging in unconstitutional intrusion into personal files.

7.4 Concluding Remarks

Criminal justice is at a strategic junction in technological applications. The digital evidence is no longer a specialty of the forensic niche; it is the inherent reality of the contemporary law enforcement. Although the recent legislative overhauls show extremely good intentions on the part of the legislature, above the legislative backing, the mechanism of the procedures and the technical infrastructure must be weighed back to the pre-industrial stages. After all, winning the fight against advanced cyber criminality must take an active synergized strategy in which law, forensic science and international co-operation will work together to harmonise and converge. It is only through constant changes in our legal and technological systems that we are able to protect the justice integrity in an ever sophisticated online world.

BIBLIOGRAPHY

I. Books

- Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed. 2011).
- Karnika Seth, *Computers, Internet and New Technology Laws* (3rd ed. 2022).
- Pavan Duggal, *Cyberlaw: The Indian Perspective* (2015).
- Stephen Mason & Daniel Seng, *Electronic Evidence and Electronic Signatures* (5th ed. 2021).
- Yatindra Singh, *Cyber Laws* (6th ed. 2016).

II. Journal Articles

- Apar Gupta, The Admissibility of Electronic Evidence in India, 11 Indian J. L. & Tech. 1 (2015).
- M.K. Geetha, Evidentiary Value of Electronic Records in Criminal Justice System, 9 Crim. L.J. 112 (2020).
- Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279 (2005).
- Rakesh Kumar, Challenges of Cyber Crime Investigation in India, 5 Int'l J. Cyber Criminology 489 (2011).
- Ryan Williams, The Probative Value of Electronic Evidence, 31 Harv. J.L. & Tech. 199 (2017).
- S. Chakraborty, Digital Evidence and its Admissibility: A Critical Analysis of Section 65B of the Indian Evidence Act, 8 NLUJ L. Rev. 45 (2021)
- Tejas Karia, Akhil Anand & Bahaar Dhawan, The Supreme Court of India Re-defines Admissibility of Electronic Evidence, 12 Digital Evidence & Elec. Signature L. Rev. 33 (2015).
- V.K. Unni, Cyber Crimes and the Indian Legal Framework, 21 J. Marshall J. Computer & Info. L. 355 (2003).

III. Statutes and Legislative Materials

- Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
- Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
- Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
- The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

IV. Case Laws

- *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).
- *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).
- *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India).
- *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178 (India).

V. Reports and Government Publications

- Law Commission of India, Report No. 277: *Wrongful Prosecution (Miscarriage of Justice): Legal Remedies* (2018).
- Ministry of Home Affairs, *Manual on Cyber Crime Investigation*, Gov't of India (2019).

  United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2013).