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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

FROM DIGITAL EVIDENCE TO ACQUITTAL: A CRITICAL EXAMINATION OF INVESTIGATIVE AND PROCEDURAL FAILURES IN THE PROSECUTION OF CYBER AND ECONOMICS CRIMES IN INDIA

AUTHOR – SIDDHARTH NEGI, STUDENT AT AMITY UNIVERSITY NOIDA

BEST CITATION – SIDDHARTH NEGI, FROM DIGITAL EVIDENCE TO ACQUITTAL: A CRITICAL EXAMINATION OF INVESTIGATIVE AND PROCEDURAL FAILURES IN THE PROSECUTION OF CYBER AND ECONOMICS CRIMES IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (8) OF 2026, PG. 234-245, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

This study critically examines the role of digital evidence in the prosecution of cyber and economic crimes in India, with a specific focus on the gap between evidentiary potential and judicial outcomes. While the legal framework—particularly the Bharatiya Sakshya Adhiniyam, 2023 and the Information Technology Act, 2000—formally recognizes electronic records as admissible evidence, practical challenges continue to undermine their effectiveness in securing convictions. The research analyses investigative and procedural shortcomings, including improper collection, weak chain of custody, lack of technical expertise among law enforcement, and non-compliance with statutory requirements such as certification under Section 63. It further highlights systemic issues such as inadequate forensic infrastructure, jurisdictional complexities, encryption barriers, and delays in expert examination. Judicial hesitation and inconsistent interpretation of admissibility standards further complicate the evidentiary process. Through doctrinal and analytical methods, the study demonstrates that despite legislative advancements, digital evidence often fails to meet the threshold of reliability required in criminal trials, leading to acquittals. The paper concludes by emphasizing the need for capacity building, standardized forensic protocols, inter-agency coordination, and judicial training to bridge the gap between digital evidence and effective prosecution in India s evolving cybercrime landscape.

Keywords:
Digital Evidence, Cyber Crime, Bharatiya Sakshya Adhiniyam, Chain of Custody, Forensic Investigation

1.1 Introduction

India was required to update its legislation in 1996 as a signatory to the current law on electronic commerce, which was enacted by the United Nations Commission on International Trade Law (UNCITRAL) in response to developments in computer technology. Upon the enactment of the Information Technology Act, 2000[208], With the legislative shift towards recognising digital information, the provisions corresponding to the former Sections 65A and 65B of the Indian Evidence Act, 1872 The unique mechanism for proving electronic documents is laid down in Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, where they already reside. There is an explicit inclusion of papers in the phrase "evidence" under Section 2(1)(d) of the BSA, and the definition of "document" encompasses electronic records created for the Court's review.[209] Thus, electronic records are treated as a species of documentary evidence,

[208] The Information Technology Act, 2000 (Act 21 of 2000).

[209] Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(d).

requiring compliance with the specialised evidentiary framework governing digital materials. The BSA preserves the Cardinal Rule of Evidence, commonly referred to as the Best Evidence Rule, which mandates that when documentary evidence is to be adduced, the original document—i.e., *primary evidence*—must ordinarily be produced.[2] Primary evidence enjoys primacy because it represents the most reliable form of the document. Secondary evidence, including electronic output, is admissible only when the law expressly permits its use and when the procedural safeguards stipulated in the BSA—particularly those in Section 63(2) and Section 63(4)—are duly satisfied.[210] This legislative framework ensures that electronic records, though technologically distinct from physical documents, are brought within a structured evidentiary regime that maintains the integrity, accuracy, and reliability of the material presented before the Court.

Electronic writings have developed into a cornerstone of modern society's communication infrastructure as a result of the tremendous expansion of electronic correspondence. The dematerialization of the workplace, omnipresence, and malleability of electronic devices are the three main themes that are shaping the future of a paperless environment.[211] In their daily lives, ninety-one percent of adults who are online now use some kind of electronic communication.Also, instead of having guards stationed at various points around a public space, one guard can sit at a counter and keep an eye on everything through closed-circuit televisions ("CCTV"), which has led to an uptick in the use of this technology in catching shoplifters and other lawbreakers. There has been a noticeable uptick in the use of electronic evidence (e-evidence) in recent years, and this trend is true in both criminal and civil cases.[212]

These days, digital devices are ubiquitous. It facilitates easy communication on a local and global scale. This is driving the ever-increasing dependence on digital forms of information storage, communication, and trade. As a result, new regulations on the admissibility of electronic evidence in civil and criminal proceedings, as well as new laws pertaining to information technology, were necessary. Evidence that is kept, received, or communicated by an electronic device is known as digital evidence. This data and information can be useful in an investigation. It refers to any piece of evidence that a party to a lawsuit may utilize during trial that is either stored or transmitted digitally. Data "stored or transmitted in binary form" that has probative value. This doesn't just apply to data stored on computers; it might also encompass data stored on other digital devices, including mobile phones or electronic multimedia players.

Electronic evidence is any probative information stored or transmitted in digital form[213] A variety of media, including computer hard drives, optical disks, floppy disks, cloud storage, portable devices, memory cards, email, and network servers, can hold this type of data. Digital photos, electronic wallets, word processor documents, accounting program files, spreadsheets, web browser cache, databases, computer memory, backups, printouts, GPS data, hotel electronic door lock logs, digital audio and video files, and so on all constitute electronic evidence. Digital evidence is often more extensive, harder to delete, more malleable, easier to copy, more expressive, and more accessible than traditional evidence.[214]

It is common practice to ask judges to decide whether electronic evidence can be admitted during trials. The decision of the court regarding admissibility issues could have a significant influence on the result of a civil case or decide whether a defendant is convicted or not. These

[210] Ibid., s. 63(2) & s. 63(4).
[211] Nweze C, "Contentious Issues and Responses in Contemporary Evidence Lwa in Nigeria", 2 *Enugu, Institute for Developing Studies* 209 (2006).
[212] Relevancy and Admissibility of Electronic Evidence (LawTeacher) *available at:* http://www.lawteacher.net/commerciallaw/essay/relevancy-and-admissibility-of-electronic-law-essays.php#ixzz2ptS X9VTj (last visited April 2, 2023).
[213] Pollitt, M. M., "Report on Digital Evidence", 7 *International Journal of Law, Management and Humanities* 89 (2001).
[214] Vivek Dubey, "Admissibility of Electronic Evidence: An Indian Perspective"4 *FRACIJ* 82 (2017).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

technological artifacts have both legitimate and illicit uses.[215] .For example, if it is not immediately apparent that the version in the computer's memory is a document, then printing it out on paper may be the best option. Whether you want to claim the printout is an original or a copy is also not an easy task. In addition, evidence in the form of audio or video recordings, emails transferred via computer, or electronically transmitted contracts in business dealings can be considered a document. Computers' widespread use, IT's societal impact, and the capacity to store data digitally have all necessitated changes to Indian law to address the admissibility of digital evidence. To clarify, digital evidence is now admissible in Indian courts thanks to the Information Technology (IT) Act, 2000, which was passed by Parliament in 2000. In addition to revising the Indian Evidence Act of 1872, the Indian Penal Code of 1860, and the Banker's Book Evidence Act of 1891, the IT Act acknowledges transactions conducted through electronic data interchange and other forms of electronic communication; it is based on the UN Commission on International Trade Law Model Law on Electronic Commerce.[216]

1.1.1 *Electronic Evidence – Meaning*

When we talk about evidence, we're referring to the collected facts and figures that show how true or legitimate a belief or statement is. To establish facts in a legal investigation or as testimony in a law court, it is necessary to draw information from human testimony, documents, or tangible objects. This is known as "evidence" in legal jargon. A root term that means "obvious to the eye" or "obvious to the mind" in Latin is where this English word first appeared[217]

An item is considered "electronic" if it contains or is operated with components like transistors and microchips that regulate and direct electric currents that are accessed or performed through a computer or other electronic device, particularly one connected to a network.Legally, any piece of evidence that a party to a case may present at trial that is stored or communicated digitally is known as digital evidence or electronic evidence. The relevance, authenticity, hearsay, and acceptability (or lack thereof) of digital evidence must be determined by the court before it can accept it.[218]

'Electronic evidence,' 'digital evidence,' and 'computer evidence' are all terms that describe the same thing. There is no difference between any of these words. Some insight into the evidence's character may be gleaned from the adjectives used. The word 'electronic' has been described as *"relating to, using, or accessed through a computer or computer network"* Also 'digital' is defined as *"processing, storing, transmitting, representing or displaying data in the form of numerical digits, as in a digital computer"*[219] Of course, the same Microsoft Encarta Dictionary defines a 'computer' as *"an electronic device that accepts, processes, stores and output data at high speed according to programmed instructions"*[220]

1.1.2 *Electronic Record – Definition*

The *Indian Evidence Act, 1872* historically provided the foundational rules governing the admissibility and evaluation of evidence in Indian courts. Enacted during the colonial period, the Act sought to transform diverse customary practices into a uniform evidentiary system applicable across communities and regions. Over the decades, several amendments were introduced to keep the statute aligned with technological and societal developments.

A significant shift occurred with the enactment of the *Information Technology Act, 2000*, which formally recognised electronic records and

---

215 Adegboro, "The Relevance of Electronic Evidence in the Nigeria Legal System" 6 *Igbinedon University Journal* 45 (2008).

216 *Supra* note 1 at 4.

217 Batuklal, *The Law of Evidence* 899 (Central Law Agency, New Delhi, 17th edn., 2017).

218 Eoghan Casey, "Evidence and Computer Crime: Forensic Science, Computers and the Internet" 7 *Academic Press* 45 (2004).

219 *Id.* at 10.

220 Adv Prashant Mali, Digital or Electronic Evidence in Indian Law or in Indian Courts, retrieved from *available at:* http://www.slideshare.net/cyberlawconsulting/electronic-evidence-digital-evidence-in-india (last visited April 03 2023).

digital communications as legally valid. Section 2(t) of the IT Act defines an *electronic record* as:

** data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated microfiche."[221]

This statutory definition brought a broad spectrum of digital material—ranging from emails, text messages, server logs, CCTV footage, images, audio files, and microfilm data—within the scope of legally cognizable records.

Under the Bharatiya Sakshya Adhiniyam, 2023, this recognition has been carried forward and strengthened. The BSA expands the evidentiary framework by explicitly including electronic records within the meaning of *documents* under Section 2(1)(d).[222] This ensures that digital information, irrespective of the device or medium through which it is created or stored, is treated as a valid form of documentary evidence, subject to compliance with the specialised procedures contained in Sections 61 to 65, particularly Section 63, which governs the proof and admissibility of electronic records.[223]

Thus, the evolution from the 1872 Act to the 2023 BSA reflects a deliberate legislative response to the demands of the digital age, ensuring that courts can reliably adjudicate cases involving sophisticated electronic data.

The section has made electronic record legally admissible in the court of law.

Sec. 3 (a) – Scope of definition of evidence expanded to include electronic records.[224]

Sec. 65B – Electronic records must be certified as authentic by the owner or person in control of the computer from which the evidence is collected in order for them to be admissible.[225]

A court may assume that a message's authenticity when it travels from its sender via an email server to its intended recipient.

Sec. 88A – Presumption as to electronic messages.[226]

The Court has the authority to assume that an electronic message that was sent from an originator to an addressee via an email server matches the message that was input into the originator's computer for transmission. However, the Court does not have the authority to presume the identity of the sender[227]

1.1.3 *Mode to prove the Electronic Record under Section 65A*

Electronic documents were required to be proved in strict compliance with Section 65B under the previous Indian Evidence Act, 1872, which included Section 65A as a unique provision regulating the technique of proving electronic records. The Bharatiya Sakshya Adhiniyam, 2023 has superseded this system; Section 63 of that law specifies the sole method for establishing electronic records.[228] Section 63 states that only the specialized procedure outlined in that clause may be used to prove the contents of an electronic record. The statute thereby creates a self-contained code for electronic evidence, distinct from the general rules applicable to ordinary documentary evidence. Much like Section 61 of the earlier Evidence Act (which dealt with proving documents), Section 63 of the BSA lays down a separate evidentiary pathway for digital material, recognising that electronic records require additional safeguards to ensure authenticity and accuracy. Under Section 63(1), any information contained in an electronic

[221] Information Technology Act, 2000, s. 2(t).
[222] Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(d).
[223] Ibid., ss. 61–65, esp. s. 63.
[224] The Information Technology Act 2000 (Act 21 of 2000), S. 3.
[225] The Information Technology Act 2000 (Act 21 of 2000), S. 65B.
[226] The Information Technology Act 2000 (Act 21 of 2000), S. 88.
[227] Sagar Rahurkar, Article on Indian Evidence Act and Digital Evidence, *available at:* http://www.chmag.in/article/apr2013/indian-evidence-act-and-digital-evidence (last visited March 30 2023).
[228] **Bharatiya Sakshya Adhiniyam, 2023**, s. 63 (special procedure for electronic records).

record and produced in printed form, or copied, stored, or recorded in optical or magnetic media, is treated as a document, provided the statutory conditions in Section 63(2) are satisfied.[229] Once these conditions are met—relating to the lawful control of the computer system, its regular use, proper functioning, and the ordinary course of data entry—the electronic record becomes admissible even without production of the original device. Additionally, Section 63(4) requires a certificate when electronic records are sought to be introduced as secondary evidence.[230] This certificate authenticates the manner in which the electronic record was produced, describes the computer system involved, and affirms that the statutory conditions under Section 63(2) have been fulfilled. For instance, system log-in records, access logs, CCTV time stamps, or server-generated reports may be proved through such certification when produced in printed or electronic form. However, courts retain discretion to insist on better or more reliable evidence depending on the circumstances. The certificate is not a testimonial guarantee of the truth of the contents but merely ensures that the computer system operated properly and produced an accurate digital output. Judicial scrutiny remains essential, especially where doubts arise concerning the integrity of the digital record. Thus, Section 63 of the BSA performs a function similar to the earlier Section 65A/65B regime: it provides a separate, technologically appropriate procedure for proving electronic records, distinguishing them from ordinary documentary evidence and ensuring that their admissibility is grounded in reliability, authenticity, and procedural safeguards.

4. *Admissibility and Relevancy of Electronic Evidence*

The provisions corresponding to Sections 65A and 65B of the Indian Evidence Act, 1872—originally inserted through the *Information Technology Act, 2000*—created the first specialised statutory framework for the admissibility of electronic evidence in India. These provisions have now been replaced in substance by Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which serves as the exclusive procedure for proving electronic records.[231] Under the earlier Evidence Act, Section 5 stated that evidence may be given only of *facts in issue* or *relevant facts*. The BSA retains the same foundational principle in Section 4, which defines the scope of facts that may be proved in judicial proceedings.[232] This ensures that electronic evidence, like all other forms of evidence, must first satisfy the test of relevance before questions of admissibility arise.

In its modern form under the BSA, Section 63(1) gives rise to the recognition of electronic records as documents for evidentiary purposes, regardless of whether they are printed, saved, copied, or recorded in optical or magnetic medium.[233] Such electronic output becomes admissible without requiring production of the original device, provided the conditions prescribed in Section 63(2) are fulfilled. These conditions relate to the lawful control of the computer system, its regular use, the normal course of data entry, and the proper functioning of the device. Thus, the BSA affirms the principle that an electronic record, once authenticated in the statutorily mandated manner, is a self-contained documentary record admissible in legal proceedings. The certificate required under Section 63(4)completes the evidentiary chain, ensuring that digital evidence is admitted only after compliance with procedural safeguards designed to maintain reliability, accuracy, and authenticity..[234]

The connection between evidence and the fact being demonstrated is what the term "relevance" means. When a piece of evidence changes the likelihood of a fact, we say that it is relevant. The proof is meaningless if it does not alter the

[229] Ibid., s. 63(1)–(2).
[230] Ibid., s. 63(4).
[231] Bharatiya Sakshya Adhiniyam, 2023, s. 63.
[232] Ibid., s. 4.
[233] Ibid., s. 63(1)–(2).
[234] http:/mja.gov.in/Upload/GR/Title%20NO.190 (As%20Per%20Workshop%20List%20title%20no 190%20pdf).

likelihood of the fact. The evidence's weight is the extent to which it modifies the fact's probability. The court uses common knowledge to decide the significance and relevance of evidence. It has been stated that the law determines admissibility and logical considerations determine relevance. The common law differs from civil law in that it contains numerous regulations on the admissibility of evidence. For example, relevant evidence cannot be presented if the witnesses cannot testify due to incompetence, privileges against self-incrimination, situations involving privileged professional communications, government secrets, or when the evidence cannot be presented due to the rules against hearsay[235]

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023—This particular approach is required in order to prove the contents of electronic records, as stated in Sections 65A and 65B of the Evidence Act. Assuming all legal requirements are met, it recognizes any data stored in an electronic record as a document, allowing its admission without the need to produce the physical copy [236]

4.1. Tape Records: Whether Electronic Device?

In *R.M. Malkani* v. *State of Maharastra*[237],The cassette was seen to be the main and direct proof of the recorded statements. The court has made it plain that audio recordings generated by electronic means can be used as evidence so long as they are pertinent to the case at hand, the speaker can be identified, and the recording can be proven to be accurate by removing any chance of editing, adding, or erasing. The Court went on to say that, under Section 8 of the Act, electronic recordings of pertinent conversations made at the same time as the occurrence in question can be included as evidence, just as a photograph of the same incident. Consequently, the admissibility of such an electronic record as evidence is beyond dispute.[238]

Data stored on a hard drive or other digital medium presents a unique challenge compared to documentary evidence in that it cannot be securely sealed upon seizure. In the matter of State of Punjab v. Amritsar Beverages Ltd[239], As a result of the same problem, a hard copy of the disk was made without the proper seal and signatures. The court ruled that in such cases, it is necessary to copy the data or hard drive, make a hard copy with the seal and signature attached, and then give one copy to the person whose possession it was taken. We have so laid out the process for the confiscation of digital evidence.

4.2. Video Conferencing

The second thing to consider is whether or not video conferencing evidence is permissible under the statute. In the case of In Amitabh Bagchi v. Ena Bagchi[240], It is no longer necessary for an individual to be physically present in order to submit evidence; the Hon'ble Supreme Court has determined that this can be accomplished through the use of video conferencing technology. The idea of electronic records include video conferencing, and sections 65-A and 65-B address facts pertaining to and the admissibility of electronic records.

In the case of, however, it was decided whether or not a witness may be cross-examined by video conference in State of Maharashtra v. Dr Praful B Desai,[241] Video conferencing, as noted by the Supreme Court, is a technological advancement that allows people in the same physical location to communicate with one another in the same way as if they were in the same room. A witness's mere presence is insufficient to establish their presence under the law. Because of this, the court ruled that the

235 Evidence, Encyclopedia Britannica, *available at:* https;//www.britannica.com/topic/evidence-law (last visited March 12, 2018).

236 Smt. K.B. Agarwal, Admissibility of Electronic Record, Video Recording, Computer Outputs, Maharastra, Judicial Academy (Jun.20,2017) *available at*: http://mja.gov.in/Site/Upload/GR/final. html (last visited February 16 2023).

237 *R.M Malkani* v. *State of Maharashtra*, AIR 1973 SC 157.

238 *K.K. Velusamy* v. *N. Palaanisamy*, AIR 1996 SC 1126.

239 *State of Punjab* v. *Amritsar Beverages Ltd,* AIR 2007 SC 590.

240 *Amitabh Bagchi* v. *Ena Bagchi,* AIR 2005 Cal. 11.

241 *State of Maharashtra* v. *Dr Praful B Desai,* AIR 2003 SC 2053.

witness might be present virtually and asserted that no reasonable basis existed to forbid this.

The individual who will be deposed on screen as a witness must first submit an affidavit or undertaking validly verified before a notary or a judge stating that they are the same person before they may be examined via the Audio-Video Link. The opposing party must be given access to a duplicate. (Affidavit for Identification)

Before cross-examining the witness online, the individual conducting the examination must first file an affidavit or undertaking, a copy of which must be sent to the opposing party in order to establish identification.

The examination of the witness must take place during regular court hours in India. The media will administer the oath.

Because of the time difference between India and the United States, the witness has no grounds to claim discomfort.

In order to ensure that the witness is familiar with the paperwork, including the plaint, written statement, and any other necessary documents, it is necessary to send them to the witness before the examination. The witness must then file an acknowledgment with the court regarding this matter.

While the witness appears on the screen, the learned judge is required to make any relevant observations about their demur.

The learned judge is required to take notice of the objections voiced during the witness's deposition and resolve them during the arguments.

Send the evidence to the witness after recording it; have him sign it in the presence of a Notary Public; then add it to the record of the lawsuit proceedings.

Both sides of the recording process will feature the graphic. Additionally, the witness must be alone during the visual conference, and a notary must attest to this fact.

The learned judge has the authority to impose additional requirements based on the specific facts of each case.

The one requesting this service is responsible for paying for and making all necessary preparations for it.

Proof of the Digital Signature of a Person

According to the Section 67A,[242] It must be demonstrated that the digital signature attached is the subscriber's digital signature in accordance with the requirements of Section 65 B in the event that an objection arises about the digital signature of any subscriber.[243]

In the matter of Bodala Murali Krishna v. Smt. Bodala Prathima[244] the court held that, "*...the amendments carried to the Evidence Act by introduction of Sections 65-A and 65-B are in relation to the electronic record. Sections 67-A and 73-A were introduced as regards proof and verification of digital signatures. As regards presumption to be drawn about such records, Sections 85-A, 85-B, 85-C, 88-A and 90-A were added. These provisions are referred only to demonstrate that the emphasis, at present, is to recognize the electronic records and digital signatures, as admissible pieces of evidence.*

4.3. Electronic Messages – Email

In the matter of *Som Prakash* v. *State of Delhi*[245], the hon'ble court observed that "in our technological age nothing more primitive can be conceived of than denying discoveries and nothing cruder can retard forensic efficiency than swearing by traditional oral evidence only thereby discouraging the liberal use of scientific aids to prove guilt." There is a huge need of change in the provisions of law in a completely problem-solving approach to deal with heavy workload on the investigators and judges.

4.4. Call Records

242 The Information Technology Act, 2000 (Act 21 of 2000), S. 67A.
243 *Supra* note 7 at 15.
244 *Bodala Murali Krishna* v. *Smt. Bodala Prathima,* AIR 2007 (2) ALD 72.
245 *Som Prakash* v. *State of Delhi,* AIR 1975 SC 989.

In the Landmark case of *State (NCT of Delhi)* v. *Navjot Sandhu*[246], the case about the 2001 attack on parliament, the conviction was appealed and this case further dealt with the question of admissibility of the telephone call records in detail. The accuses based his case on the argument that the call records can't be taken into consideration for the conviction as the prosecution has clearly failed to produce the relevant certificate under Section 65-B (4) of the Evidence Act. The Hon'ble court held that "the cross- examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records." It was further observed that only because the certificate containing the details in sub-Section (4) of Section 65B is not filed in the instant case, there can't be denial of it as secondary evidence.

5.1 Conclusion

Electronic evidence differs from physical evidence in several ways. Changing electronic evidence is simple. Second, an exact digital copy without damage is safe. Also, evidence can be verified simultaneously. Anomalies explain computer forensics and electronic evidence security. These crimes are notoriously hard to investigate. Some proof is scarce. Investigators struggle with acquisition, assessment, analysis, and preservation. Internet and network technology complicate this. Indians can utilise Chinese computers to steal data from US servers via the Internet. Judicial and technological examples. Electronic evidence trials have poor conviction rates due to these difficulties. Many courts are overworked. Indian state-wise case disposal statistics show a shocking 92% case pendency rate up to 2016.

The 2000 Information Technology Act, revised in 2008 to include cybercrimes, addressed shifting crime. The same Act governed electronic evidence and revised the 1872 Indian Evidence Act. Section 45A of the Evidence Act allows an Examiner of Electronic Evidence or computer forensic examiner to advise on any issue involving digital or electronic information, with a concentration on criminal investigations using forensic science. Despite Section 45A of the Evidence Act in 2009 and Section 79A of the Information Technology Act, 2000, the Central Government did not regulate or notify any Indian agency or laboratory as an Examiner of Electronic Evidence until 2017. A government initiative makes six labs IT Act examiners. Delays in procedural authorisation impacted electronic evidence admissibility.

India's criminal courts still force confessions through physical questioning. Police lack sophisticated criminal investigative procedures and scientific evidence to prove guilt beyond a reasonable doubt. Reporting, apprehending, and convicting a criminal takes time.

Law enforcement and computer forensics professionals strive to gather, store, and analyse electronic evidence, but the judiciary, sometimes uneducated about digital crimes, makes admittance difficult. Courts have considered many Section 65A and 65B admissibility provisions. They evaluated the certificate that must be provided to the court with the evidence under Section 65B, the certifying agencies' credentials, and whether Section 63 allows electronic evidence.

The researcher examined criminal justice stakeholders' interactions with law enforcement, computer forensic laboratories, expert presentations of forensic examination findings, and the judiciary's admissibility procedures. Empirical research evaluated these stakeholders.

Dirty, slippery electronic evidence is hard to manage. Evidence is sometimes circumstantial, and computer activity is hard to link to an individual. This proof is easily manipulated and destroyed. Limited data extraction is shown. Evidence dynamics are widespread in electronic evidence.

[246] *State (NCT of Delhi)* v. *Navjot Sandhu*, AIR 2005 SC 3820.

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

Investigation of most computer and digital crimes is difficult due to their global nature. India's cybercrime servers may be abroad. Facebook's Whatsup has been used for crime and violence. Law authorities cannot access forum messages while investigating Whatsup crimes because to end-to-end encryption. Whatsup is hosted in the US, therefore Indian authorities cannot access its data. Service provider/company can freely exchange information. Private end-to-end communication encryption is broken. Whatsapp resists Indian government requests to trace bogus messages, saying it would violate encryption.

Criminals can hide online, increasing their escape prospects. Anonymous cyberacts support free expression. Online, anyone can share their opinions without being identified or punished. Anonymity makes cybercriminals harder to identify for law enforcement and victims.

Despite escalating cybercrimes in India, states have not increased cybercrime investigation. Few cybercells handle such cases. Gurugram had its first cyber crime police station in 2018. Despite the police station's powerful computer lab, the manufacturing firm only taught three constables for three days, not enough to handle complex offences.

Most police stations lack digital criminal knowledge. This prevents the prosecution from gathering enough evidence.

Interconnected cyberspace makes electronic evidence tampering easier. Law enforcement is unprepared to prevent evidence manipulation during collection and preservation.6 Police harass citizens using antiquated tactics to investigate complex cybercrimes. There are no other IT Act, 2000 cybercrime investigator education standards.

The internet is worldwide, therefore harassment, abuse, etc. are everywhere. Advanced technology could change voices, appearances, etc. online, upsetting society. Internet makes violating Article 21 of the Indian Constitution's right to privacy, life, liberty, and dignity simpler.

Technical skills and evidentiary rules are needed to gather evidence. If such statutes are breached, the defendant's guilt proof may be thrown out. Every computer-based crime scene is unique, therefore detectives must be inventive. Criminal investigators developed SOPs at this time. Evidence collection, storage, and processing must follow forensic science standards.

Due to police illiteracy, courts often discard digital or electronic evidence with broken chains of custody. Chain of custody ensures evidence authenticity and prevents tampering between seizure and court presentation. Few police understand chain of custody.

Cybercrime investigation is slowed by insufficient resources. Distance matters in remote investigations. Most cops take public transit to crime scenes, slowing the procedure. These authorities need funds to investigate fast. Because another state involved in the crime lacks cooperation and coordination, the inquiry cannot be concluded. Coordination is crucial with electronic proof.

Underfunded detectives face escalating cybercrime. Lack of education prevents police from investigating scientific crimes. Instead of complex criminal investigation, they study police basics. While claiming to be "dedicated" to science, numerous departments use outdated methods and equipment. Unfortunately, not all districts have Cyber Cells. Current Cells need skilled staff. State cyber forensic facilities are scarce, therefore specialists may take time to act. Police station commanders receive no ongoing computer offence training.

After hardware acquisition, check storage data before analysis. Hashing software compares data to copies or images. A hash value is generated from input data. Verifying digital evidence involves hashing. It can disprove the opponent's data tampering claim in court. Forensic imaging integrity is verified by MD5.

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

Many academics consider collisions cryptographic hash function vulnerabilities that hinder digital forensics. Multiple files with the same hash value but distinct contents and behaviours clash. Such tools may not check imaging. Electronic gadgets abound and are added daily. Thieves and victims employ expensive gear. Computer forensic examiners/experts are locked with such technology because their flaws may be tough to fix. However, applying legal principles to such analysis may be difficult.

Criminals use new technology, thus forensic labs must be updated. Upgrades are needed to fix new issues. Multiple permissions delay tool purchases. The Procurement Department must assist. Improved research requires frequent expert updates. Maintaining tool purchasing protocols fails forensics. IT authentication and access control require encryption. To ensure privacy, security, and integrity, encryption converts plain text to ciphertext. However, criminals' encryption technology challenges law enforcement. Laws requiring software developers to install a law enforcement back door are being considered. Forensic experts must grasp law and technological aspects of electronic data and equipment. If forensic examination results violate evidence guidelines, court admissibility is at risk.

Judges struggle with expert technological evidence. "Hash" values investigate, discover, and authenticate electronic evidence for court, which could decide the case. Such evidence's admissibility matters in court. Private forensic experts with additional technology are available to defence counsel, complicating admissibility analysis.

Recently, information technology has advanced rapidly, making privacy, confidentiality, and cyberspace crucial to democracy and government effectiveness. Law enforcement needs cyberspace to fight cybercrime but must respect privacy. Privacy concerns can hinder computer crime investigations. No court-tested processes or statutes govern electronic evidence collection, storage, and evaluation. Electronic evidence identification, preservation, acquisition, authentication, and analysis have global best practices. Despite international standards, law enforcement has not enforced the Indian Evidence Act of 1872's primary evidence requirements.

BIBLIOGRAPHY

Statutes

- The Code of Criminal Procedure, 1973 (2 of 1974).
- The Constitution of India, 1950
- The Dissolution of Muslim Marriage Act, 1939 (8 of 1939)
- The Hindu Marriage Act, 1955 (25 of 1955)
- The Indian Penal Code, 1860 (45 of 1860)
- The Special Marriage Act, 1954 (43 of 1954)

Books

- Ashworth Andrew, *"Principles of Criminal Law"*, 53 (Lexis Nexis, New Delhi, 6th edn., 2009).
- Bentham, Introduction to the principles of morals and legislation (1789).
- Dr. J.N. Pandey, *"Constitutional Law of India"*, 321 (Central Law Agency, Allahabad, 59th edn., 2022).
- Hart H.L.A, *"law, liberty, and morality'*, 26 (Lexis Nexis, Delhi, 1st edn., 1963).
- H.M. Seervai, *"Constitutional Law in India"*, 789 (Aggrawal Law House, Allahabad, 4th edn., 2022).
- Durga Das Basu, *"Commentary on Constitution of India"*, 670 (Lexis Nexis, New Delhi, 9th edn., 2016).
- K.D Gaur, *"A text book on the Indian Penal Code"*, 734 (Lexis Nexis, Delhi, 7th edn., 2020).
- Kishor Prasad, *"Problems & Solutions on Criminal Law"*, 567 (Eastern Book Company, New Delhi, 3rd edn., 2016).

- Ratan Lal & Dhiraj Lal, *"The Indian Penal Code"*, 757(Lexis Nexis, Delhi, 36th edn., 2020).
- K.N. Chandrashekhar Pillai, *"R.V. Kelkar's, Criminal Procedure"*, 789 (Eastern Book Compaby, New Delhi, 7th edn., 2021).
- SC Sarkar, *"Indian Penal Code"*,214 (Dwivedi Law Agency, Allahabad, 19th edn., 2014).
- Sriniwass, *"Legal Classic on Criminal Jurisprudence of India"*, 509 (Aggrawal Law House, Allahabad, 1st edn., 2021).
- S.P Tyagi, "An Exclusive Treatise on Marriage and Divorce Laws in India", 490 (Vinod Publications, New Delhi, 4th edn., 2021).
- Bindu Jindal Ed. Gurmanpreet Kaur, Cyber Stalking And Victimization Of Women: An Analytical Study, In Law As A Catalyst Of Social Change In Present Scenario (2016).

Articles

- Amitai Etzioni, Implications Of Select New Technologies For Individual Rights And Public Safety, 15(2) Harv. J. Of L. & Techn (2002)
- Anne Wallace, Using Video Link To Take Forensic Evidence: Lessons From An Australian Case Study, 17(3) Int. J. Of Evidence & Proof 221 – 49 (2013)
- Arunima S Kumar, Cyber Forensics In Kerala, Int'l J. Of Comp. Sci. & Mobile Computing 74 (2013)
- Ashwini Vaidialingam, Authenticating Electronic Evidence: S. 65B, Indian Evidence Act, 1872, Nujs L. Rev. 43 (2015)
- Asou Aminnezhad, A Survey On Privacy Issues In Digital Forensics, 1 (4), Int. J.Of Cyber Sec. & Dig. Forensics (Ijcsdf) 1(4): 311-323
- B. Carrier, Defining Digital Forensic Examination And Analysis Tools Using Abstraction Layers, 1(4), Int. J. Of Digital Evidence, (2003).
- Barry Chen, Computer Forensics In Criminal Investigations, Dartmouth Undergrad. J. Of Sci. (2013)
- Carrie Morgan Whitcomb, A Historical Perspective Of Digital Evidence: A Forensic Scientist's View, 1 (1), Int'l J. Of Digital Evidence (2002)
- Christopher Wall & Jason Paroff, Cracking The Computer Forensics Mystery, 17 (7) Utah Bar Journal (2015)
- Confluence Of Digital Evidence And The Law: On The Forensic Soundness Of Live- Remote Digital Evidence Collection, 2005 Ucla J.L. & Tech. 5
- Dale A. Nance, Reliability And The Admissibility Of Experts, 34, Seton Hall Law Review (2003)
- Felix Freiling & Leonhard Hosch, Controlled Experiments In Digital Evidence Tampering, Digital Investigation 24 (2018)
- Gary C. Kessler, The Impact Of Md5 File Hash Collisions On Digital Forensic Imaging, 11(4) J. Of Dig. For., Sec. & L. 129 (2016)
- G.S Bajpai, *Current Status and Challenges of protection and Support for Victims in India,* 30 IJMLH 21-31 (2022)
- Himanshu Setia, Evidentiary Value Of Forensic Reports In Indian Courts, Res. J. Forensic Sci., Vol. 4(6), 1-7, June (2016)
- Inikpi O. Ademu Et Al., A New Approach Of Digital Forensic Model For Digital Forensic Investigation, (Ijacsa), 2 (12), Int. J. Of Advanced Computer Science And Applications (2011)
- Ishita Chatterjee, Challenges Relating To Enforcement And Admissibility Of Cyber Forensics And Electronic Evidence, [2012] 4 Mlj 17
- John H. Gardner, Expert Evidence, 8 Sch. L. Rev. 3 (1950)
- Julien Hofman, Electronic Evidence In Criminal Cases, 19 S. Afr. J. Crim. Just. 257 (2006)

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

VOLUME 6 AND ISSUE 8 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in