WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

"LEGAL ADMISSIBILITY AND EVIDENTIARY VALUE OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS"

SOMYA SINGH[1], DR. VANDITA CHAHAR[2]

[1] (STUDENT)
[2] (ASSISTANT PROFESSOR) (CO-AUTHOR), JAIPUR NATIONAL UNIVERSITY, JAGATPURA, JAIPUR

ABSTRACT :

In the digital era, electronic evidence has emerged as a vital component in the investigation and prosecution of criminal offenses. From emails and mobile data to surveillance footage and digital footprints, electronic records offer significant support in establishing facts and ensuring justice. This research examines the legal admissibility and evidentiary value of electronic evidence in criminal proceedings, with a focus on existing legal frameworks, judicial interpretations, and practical challenges.

The study identifies critical issues such as authentication, data integrity, privacy concerns, and the potential for tampering or manipulation of digital records. It highlights how legal systems, particularly in India and select common law jurisdictions, have responded to these challenges through legislation like the Indian Evidence Act, 1872 (as amended), and judicial precedents that lay down the conditions for admissibility under Section 65B.

A doctrinal methodology has been adopted, analysing statutory provisions, landmark judgments, and scholarly commentary. Comparative insights are drawn from jurisdictions including the United States and the United Kingdom to understand evolving global standards and best practices. Findings suggest that while courts increasingly rely on electronic evidence, inconsistencies in judicial interpretation and lack of technical expertise often hinder its effective use. The study underscores the need for clear procedural safeguards, robust digital forensic mechanisms, and continuous judicial training to enhance the credibility and reliability of such evidence.

In conclusion, electronic evidence holds immense potential to strengthen criminal justice systems, provided its legal treatment is consistent, technologically informed, and rights-based. This research contributes to on-going discourse by offering practical recommendations for legal reform and capacity-building in the field of digital evidence.

Key Words: Electronic Evidence,Admissibility,Criminal Proceedings ,Digital Forensics, Indian Evidence Act ,Section 65B,Judicial Interpretation ,Legal Framework ,Evidentiary Value Cybercrime, Data Authentication, Comparative Law, Procedural Safeguards, Digital Evidence, Criminal Justice System

INTRODUCTION

In an increasingly digitized world, the landscape of criminal investigations and adjudication is undergoing a substantial transformation. Traditional forms of evidence, such as oral testimonies and physical exhibits, are now supplemented—and in many cases, replaced—by electronic evidence, which includes emails, text messages, call records, digital photographs, CCTV footage, GPS data, and metadata. As crimes evolve to exploit technology, especially in areas such as cybercrime, financial fraud, organized crime, and terrorism, the legal system is compelled to adapt and integrate digital tools into the process of justice. The shift brings with it not only new opportunities for effective law enforcement but also complex challenges regarding the legal admissibility, reliability, and handling of such evidence in criminal proceedings.

Electronic evidence is inherently different from traditional forms. It is intangible, easily alterable, and often exists in large, complex datasets. These characteristics raise serious concerns related to authenticity, chain of custody, privacy, and the technical knowledge required to handle and interpret such information. The Indian legal framework, while acknowledging the evidentiary value of electronic records, continues to grapple with procedural ambiguities—most notably surrounding the application of Section 65B of the Indian Evidence Act, 1872, which governs the admissibility of electronic records. Since the landmark judgment in *State (NCT of Delhi) v. Navjot Sandhu* (2005), followed by the influential *Anvar P.V. v. P.K. Basheer* (2014) ruling and the clarificatory *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), Indian courts have tried to establish clearer standards. However, inconsistency in interpretation and implementation continues to obstruct the smooth inclusion of digital evidence in legal proceedings.

A growing body of literature emphasizes the need to reform and harmonize the procedural and evidentiary rules surrounding digital materials. Scholars and practitioners have pointed out that while digital tools improve fact-finding, they also increase the risk of wrongful conviction or acquittal if not handled properly. Comparative legal systems, such as those in the United States and the United Kingdom, have begun to institutionalize digital forensic

practices and guidelines to ensure the admissibility of electronic evidence meets both technical and constitutional standards. Learning from these models may help Indian courts refine their own procedures.

The present study is rooted in a doctrinal approach. It critically examines statutory laws, significant case law, and secondary legal literature to assess the current position of electronic evidence within the Indian criminal justice system. The focus is on addressing key concerns such as the authenticity and reliability of electronic records, procedural compliance under Section 65B, the role of certification, and the importance of the chain of custody in ensuring evidentiary integrity. Additionally, the paper includes a comparative lens to understand how other jurisdictions tackle similar challenges and whether such practices can inform or be integrated into Indian legal reforms.

The hypothesis underpinning this research is that while Indian law recognizes electronic evidence as admissible, the lack of a uniform procedural framework and technical capacity weakens its actual evidentiary value in practice. This hypothesis is tested by evaluating judicial interpretations, procedural lapses, and the effectiveness of current safeguards.

The rationale for choosing this topic lies in its immediate relevance. As criminal activities become more technologically sophisticated, the demand for legally sound and forensically accurate digital evidence will continue to grow. Bridging the gap between legal formalism and technological advancement is crucial for the credibility of the criminal justice process.

The paper's findings indicate that although electronic evidence is increasingly accepted by courts, it often fails to meet admissibility standards due to procedural irregularities or insufficient understanding of technical requirements. As a result, the paper concludes with key recommendations aimed at legal reform, judicial training, and the institutionalization of digital forensic procedures. These reforms are not only necessary but urgent, to uphold the rights of both the accused and the victims, and to ensure that justice in the digital age is both efficient and equitable.

The increasing reliance on electronic evidence in criminal proceedings has prompted a significant body of legal scholarship, jurisprudence, and policy discourse. The literature on this subject spans multiple dimensions—legal, technological, and procedural—each reflecting the complexities involved in integrating digital material into evidentiary frameworks. This section presents a review of key literature, focusing on the evolution of the legal status of electronic evidence, judicial interpretations, comparative perspectives, and the challenges faced in its admissibility and evidentiary evaluation.

1. EVOLUTION OF ELECTRONIC EVIDENCE IN LEGAL SYSTEMS

Electronic evidence is broadly defined as any data or information of probative value that is stored or transmitted in digital form. Scholars such as Stephen Mason (2020) emphasize that digital evidence, due to its volatility and ease of manipulation, requires an entirely different legal and procedural treatment compared to traditional evidence. Early legal frameworks did not anticipate the emergence of digital formats, leading to interpretative challenges when applying existing rules of evidence.

In the Indian context, the amendment of the Indian Evidence Act, 1872 through the Information Technology Act, 2000 marked a significant shift. Sections 65A and 65B were inserted to provide legal recognition to electronic records, thereby aligning with international developments such as the Model Law on Electronic Commerce (1996) adopted by UNCITRAL. However, scholars argue that the statutory framework in India lacks technical depth and has been plagued by inconsistent judicial interpretation (Chand, 2019; Mehta, 2021).

2. JUDICIAL INTERPRETATION OF SECTION 65B

A major focus of the literature concerns Section 65B of the Indian Evidence Act, which prescribes conditions for the admissibility of electronic records. Legal commentators frequently cite ***Anvar P.V. v. P.K. Basheer*** **(2014)** as a landmark judgment wherein the Supreme Court clarified that electronic evidence must be accompanied by a certificate under Section 65B(4) for it to be admissible. This overturned the earlier precedent in ***State (NCT of Delhi) v. Navjot Sandhu*** **(2005)**, which allowed for broader admissibility of electronic records without strict compliance.

Subsequent scholarship explores the implications of this stricter standard. For instance, Basu (2017) argues that while the intent behind Section 65B is to ensure authenticity, the practical enforcement of the certificate requirement is often burdensome and impractical, especially when the data source is not directly accessible to the party presenting the evidence. A series of judgments following *Anvar* reflect a growing judicial concern about procedural rigidity and its impact on the fairness of trials.

The Supreme Court revisited the issue in ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*** **(2020)**, reaffirming the mandatory nature of the 65B certificate unless the original device is produced in court. Scholars such as Datar (2021) have welcomed the clarity provided by this ruling but caution that the lack of a uniform procedural framework still leaves room for subjective interpretation by lower courts.

3. CHALLENGES OF AUTHENTICATION AND RELIABILITY

A recurring theme in the literature is the issue of authenticity and the risk of manipulation. Digital evidence is inherently fragile and can be altered without leaving a trace, unless robust forensic protocols are followed. Authors such as Kesan and Hayes (2014) emphasize the need for digital chain-of-custody protocols, encryption standards, and metadata analysis as tools for authenticating electronic evidence.

In the Indian context, literature highlights the gap in forensic infrastructure and the need for specialized training. Saxena (2020) notes that many trial courts lack the technical expertise to properly assess the integrity of digital records, leading to either undue scepticism or over-reliance on seemingly authentic documents. There is a general consensus that courts must be equipped with both technical tools and judicial training to evaluate digital evidence reliably.

4. COMPARATIVE LEGAL APPROACHES

The literature often draws comparisons between India and other jurisdictions to highlight best practices. In the United States, the Federal Rules of Evidence emphasize the "best evidence rule" and allow for various forms of authentication, including expert testimony and digital signatures. The Sedona Conference (2019) provides detailed guidelines on managing electronic discovery and preserving the integrity of digital evidence.

In the United Kingdom, the Police and Criminal Evidence Act (PACE) and associated Codes of Practice provide a structured approach for collecting and preserving electronic evidence. For example, the Association of Chief Police Officers (ACPO) guidelines require strict procedures for data acquisition and forensic imaging. Scholars such as Redmayne (2001) argue that the UK's approach balances flexibility with rigorous standards of reliability, offering valuable lessons for jurisdictions like India.

Australian law also offers insights, especially regarding the role of expert witnesses in establishing the probative value of digital material. According to Biddle and Macdonald (2018), courts in Australia actively engage with technical experts during trials involving complex digital evidence, ensuring a more informed adjudication process.

5. ADMISSIBILITY VS. EVIDENTIARY VALUE

The distinction between admissibility and evidentiary value is another key area explored in the literature. While admissibility pertains to whether a piece of evidence can be formally considered by the court, evidentiary value relates to its weight or persuasive power. This distinction is especially important for electronic evidence, which may be admitted but still questioned in terms of its credibility or reliability.

Scholars such as Upendra Baxi (2015) and R. Prakash (2022) argue that Indian courts often conflate these two concepts, either over-emphasizing procedural compliance or neglecting the probative strength of digital materials. As a result, valuable evidence is either discarded on technical grounds or admitted without adequate scrutiny, affecting the outcome of trials.

6. NEED FOR LEGAL AND INSTITUTIONAL REFORM

There is a growing consensus in the literature that legal reform must be accompanied by institutional and infrastructural changes. A report by the Vidhi Centre for Legal Policy (2021) recommends developing national guidelines for digital evidence handling, establishing digital forensics laboratories at the district level, and creating a certification system for admissible formats. The report also calls for greater inter-agency coordination between police, prosecution, and forensic experts.

Academic studies further emphasize the importance of judicial education. Rao (2022) suggests that continuing legal education programs should include modules on digital evidence, covering aspects like metadata interpretation, encryption, and blockchain evidence. Without such reforms, scholars warn that procedural innovations alone may not achieve the intended outcomes of fairness and efficiency.

METHOD & MATERIALS

This research adopted a *doctrinal legal methodology*, which is traditionally used for normative legal analysis. The doctrinal method focuses on the study of legal texts—such as statutes, case law, rules, and legal principles—to systematically interpret and critically assess the existing legal framework. The aim was to understand how electronic evidence is treated within the Indian criminal justice system, particularly in terms of its admissibility and evidentiary value, and to evaluate its effectiveness by comparing it with practices in other jurisdictions.

Materials Used

The primary materials for this study included:

- *Statutory Provisions:* The Indian Evidence Act, 1872 (with special focus on Sections 3, 65A, and 65B), the Code of Criminal Procedure, 1973, and the Information Technology Act, 2000 were closely examined. Relevant rules and amendments were also considered, particularly those introduced post-2000 to accommodate digital and electronic records.
- *Judicial Decisions:* Landmark and recent judgments from the Supreme Court and High Courts of India formed a key component of the analysis. Notable among these were ***State (NCT of Delhi) v. Navjot Sandhu*** **(2005),** ***Anvar P.V. v. P.K. Basheer*** **(2014), and** ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*** **(2020).** These cases were examined to track the evolving judicial interpretation of electronic evidence.
- *Secondary Sources:* A wide range of legal commentaries, journal articles, law commission reports, and policy briefs were consulted. These included academic discussions on digital forensics, procedural law, and comparative analyses from jurisdictions such as the United Kingdom, the United States, and Australia.
- *Reports and Guidelines:* The study incorporated guidelines issued by the Ministry of Home Affairs, the Department of Electronics and Information Technology (DeitY), and the National Crime Records Bureau (NCRB) related to digital evidence collection, preservation, and admissibility. Reports from the Law Commission of India and international organizations such as UNCITRAL and INTERPOL were also reviewed.

Procedure and Logical Framework

The research was conducted in a series of logically structured steps, outlined below:

1. *Identification of the Research Problem:* The issue of inconsistent application and interpretation of electronic evidence in Indian courts was identified as the core problem. The study was designed to explore how statutory and judicial frameworks manage the admissibility and evidentiary reliability of such evidence.
2. *Legal Framework Analysis:* A close textual analysis of the Indian Evidence Act, especially Sections 65A and 65B, was undertaken. This was done to understand the legislative intent, structure, and mandatory requirements for admissibility. Amendments brought by the Information Technology Act, 2000 were also analyzed in context.
3. *Case Law Compilation and Examination:* Leading cases were selected based on their doctrinal relevance and frequency of citation in judicial decisions and academic works. A comparative reading was done to highlight contradictions, evolving interpretations, and key judicial pronouncements that have influenced the treatment of digital evidence.
4. *Comparative Jurisdictional Analysis:* The legal treatment of electronic evidence in common law countries—particularly the United Kingdom, United States, and Australia—was studied. These jurisdictions were chosen due to their similar legal roots, advanced forensic standards, and comprehensive evidentiary rules. The comparative method was employed to identify best practices and reformative suggestions applicable to the Indian context.
5. *Assessment of Procedural and Forensic Gaps:* By reviewing existing forensic practices, police procedures, and judicial capacity in handling electronic records, the research identified systemic challenges. Reports from the National Judicial Academy and BPR&D (Bureau of Police Research and Development) were also included in this analysis.
6. *Doctrinal Interpretation and Synthesis:* The research synthesized legal texts, judicial interpretations, and secondary literature to draw conclusions about the coherence, effectiveness, and deficiencies of the current legal framework. This doctrinal synthesis helped develop normative recommendations for reform.

Justification for the Approach

The doctrinal method was chosen for its effectiveness in interpreting legal principles and tracking jurisprudential evolution. Given that the research questions revolve around legal standards, judicial practices, and evidentiary doctrines, a non-empirical, normative approach was most appropriate. It allowed for an in-depth engagement with the law as it exists in texts and as interpreted by courts, which is central to understanding both the promise and pitfalls of using electronic evidence in criminal trials.

Moreover, the incorporation of a comparative approach enriched the analysis by exposing the Indian legal system to global standards, offering context-sensitive but forward-looking suggestions for legal reform.

RESULTS

The research yielded a series of important findings regarding the legal admissibility and evidentiary treatment of electronic evidence in criminal proceedings, particularly within the Indian context. By examining statutory provisions, judicial interpretations, and comparative frameworks, the study revealed both significant progress and persisting challenges in the effective incorporation of electronic evidence into the criminal justice system.

1. Interpretation and Application of Section 65B, Indian Evidence Act

One of the most significant findings pertained to the interpretation of Section 65B of the Indian Evidence Act, 1872. The study revealed a trend of fluctuating judicial interpretations regarding the mandatory nature of the Section 65B(4) certificate, which is required to authenticate electronic records. Initially, **in *State (NCT of Delhi) v. Navjot Sandhu* (2005)**, the Supreme Court held that even without a certificate, electronic evidence could be admitted under other provisions. However, this position was overturned in ***Anvar P.V. v. P.K. Basheer* (2014),** where the Court emphasized that the certificate was mandatory. This created a rigid standard, which was again nuanced in ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020),** where the Court clarified that while the certificate is mandatory, it can be produced at any stage before the trial concludes.

These shifting interpretations caused inconsistencies in lower courts, with several cases being dismissed or delayed due to procedural non-compliance. The research observed that this lack of uniformity adversely affected the admissibility of critical evidence, especially in cybercrime and financial fraud cases.

2. Challenges in Establishing Authenticity and Chain of Custody

The study found that the **authenticity and integrity** of electronic evidence were frequently challenged in court. The requirement of maintaining an unbroken chain of custody, while legally recognized, was often undermined in practice due to poor handling procedures by investigative agencies.

In several cases reviewed, evidence such as CCTV footage or call records was either not preserved in original form or lacked metadata to confirm authenticity. This compromised the credibility of the evidence. For instance, in many cases involving mobile data or digital documents, the failure to produce original devices or hash values led to questions of tampering or fabrication.

Courts demonstrated caution in accepting electronic records that were not adequately authenticated, even when they were crucial to the prosecution's case. This was particularly evident in cases related to terrorism, organized crime, and cyber offenses.

3. Observations on Digital Forensic Capabilities

The research observed that India's **digital forensic infrastructure** remains underdeveloped relative to the increasing demand. Many states lacked well-equipped forensic labs capable of timely and reliable extraction, preservation, and analysis of digital data.

Moreover, police personnel and investigating officers often lacked training in handling digital evidence, resulting in errors such as failing to isolate devices, improper imaging of data, and lack of documentation. The study found that many forensic reports submitted in courts lacked clarity or failed to address core issues such as data origin, tampering detection, or device log history.

This technical deficit hindered the ability of prosecutors to present a strong case and contributed to judicial skepticism in accepting digital records as primary evidence.

4. Comparative Jurisdictional Insights

The comparative analysis with the United States, United Kingdom, and Australia provided important context for understanding best practices and gaps in India. For instance:

- In the **U.S.**, the Federal Rules of Evidence emphasize the reliability and chain of custody of digital evidence but also allow for broad judicial discretion. The Daubert standard enables judges to evaluate the scientific reliability of forensic methods.
- The **U.K.** has detailed protocols for digital forensic processes, such as the Association of Chief Police Officers (ACPO) Guidelines, which ensure the integrity of data from collection to court presentation.
- **Australia's Evidence Act 1995** offers a comprehensive approach to electronic communications, with less emphasis on procedural formalities and more focus on probative value.

The research concluded that these jurisdictions have embraced flexible, technologically sound frameworks for assessing electronic evidence, in contrast to India's procedural rigidity and technical gaps.

5. Judicial Trends and Evolving Standards

A positive trend identified during the study was the **increasing willingness of Indian courts to engage with digital evidence** in a more sophisticated manner. Recent judgments demonstrated a better understanding of technical terms such as hash values, server logs, IP tracking, and data metadata.

Additionally, courts began to invoke constitutional safeguards—such as the right to privacy under ***Justice K.S. Puttaswamy v. Union of India***—while considering admissibility and surveillance-based evidence. This indicates a move toward balancing evidentiary value with fundamental rights, particularly in cases involving personal devices and communications.

However, despite judicial evolution, the research found that **lower courts continued to struggle** with digital complexity, often relying heavily on expert opinion and forensic reports without clear standards for evaluation.

6. Lack of Uniform Procedural Guidelines

Finally, the study discovered a **notable absence of uniform procedures or model guidelines** for the handling and admission of electronic evidence across India. While the Indian Evidence Act and Information Technology Act offer a basic framework, there are no centralized protocols governing:

- Digital evidence seizure and preservation;
- Certification standards under Section 65B;
- Timelines for submission and verification;
- Protocols for private-sector cooperation (e.g., with ISPs or mobile operators).

This procedural ambiguity frequently led to delays, evidentiary disputes, and even acquittals on technical grounds.

DISCUSSION

The integration of electronic evidence into criminal proceedings reflects a profound shift in both investigative strategies and judicial decision-making in the digital age. As established in the research findings, the increasing prevalence of digital technologies in everyday life has necessitated the evolution of evidentiary norms to accommodate novel forms of proof, including emails, surveillance footage, call detail records (CDRs), GPS logs, mobile applications, and social media content. However, despite this evolution, the legal, procedural, and technical challenges associated with electronic evidence continue to present significant hurdles, particularly in jurisdictions like India.

Trends and Evolving Judicial Approaches

The results indicate a clear trend toward greater judicial acceptance of electronic evidence. Indian courts, especially the higher judiciary, have progressively acknowledged the probative value of digital records. The seminal decisions in ***Anvar P.V. v. P.K. Basheer*** **and** ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*** represent critical milestones in this regard. These rulings clarified the mandatory nature of the Section 65B certificate for electronic evidence and emphasized compliance with procedural formalities to ensure authenticity and reliability.

However, the evolving jurisprudence has also introduced complexities. The shift from the flexible approach in *Navjot Sandhu* (2005) to the stricter interpretation in *Anvar P.V.* (2014), and then to the nuanced position in *Arjun Panditrao* (2020), demonstrates the judiciary's struggle to balance evidentiary reliability with practical feasibility. While this legal trajectory has helped raise standards for admissibility, it has also exposed inconsistencies in interpretation and application, particularly in lower courts.

The inconsistency in judicial application stems partly from the lack of specialized knowledge among judges and legal practitioners. Many trial courts continue to admit or reject electronic evidence based on subjective assessments rather than clear, uniform standards. This inconsistency undermines the legal certainty that is essential in criminal trials, where the rights of both the accused and the victims are at stake.

Authentication, Integrity, and Chain of Custody

One of the principal challenges revealed in the study is ensuring the **authenticity and integrity** of electronic evidence. Digital data is inherently susceptible to alteration, deletion, or duplication. As such, courts must be vigilant in requiring demonstrable proof that the evidence has not been

tampered with. The importance of the **chain of custody**—the systematic documentation of the evidence's handling from its collection to its presentation in court—cannot be overstated.

Unfortunately, as the findings show, Indian law enforcement agencies often fall short in this respect. There are multiple instances where digital devices were seized without proper imaging, metadata was not preserved, and forensic procedures were poorly documented. This has led to the exclusion of otherwise probative evidence on grounds of unreliability. In contrast, jurisdictions such as the United States and the United Kingdom have well-established protocols to maintain the integrity of digital records, including the use of hashing techniques, standardized forensic software, and certified chain-of-custody logs.

Privacy Concerns and Constitutional Safeguards

The increased reliance on electronic evidence also raises **constitutional and ethical concerns**, particularly regarding privacy. In the post-*Puttaswamy* era, Indian courts are expected to strike a balance between the public interest in crime detection and the individual's right to privacy. This becomes especially important in cases involving intrusive surveillance, mobile phone data extraction, and social media tracking.

The discussion around consent, proportionality, and judicial oversight in digital investigations is still nascent in India. For example, while search warrants are generally required for accessing physical premises, the standards for digital searches remain ambiguous. Without legislative or judicial clarity, there is a risk of law enforcement agencies overreaching in their investigative methods, potentially violating fundamental rights.

Comparative Legal Standards and Best Practices

The comparative analysis underscores the fact that India lags behind several common law jurisdictions in adopting clear, uniform, and technologically robust standards for electronic evidence.

In the **United States**, the Federal Rules of Evidence and the *Daubert* standard give trial judges a gatekeeping role in evaluating scientific and technical evidence. Forensic tools and procedures used to generate digital evidence are scrutinized for reliability and general acceptance in the relevant expert community. In contrast, Indian courts rarely assess the scientific reliability of digital forensic techniques, often deferring entirely to expert opinion without rigorous examination.

In the **United Kingdom**, the ACPO (Association of Chief Police Officers) Guidelines provide detailed instructions for the seizure, handling, and analysis of digital evidence. These guidelines are binding on investigators and ensure that digital data is treated with the same caution and formality as physical evidence. They also require that a digital forensic expert be present during the acquisition and analysis process—something still rarely seen in Indian practice.

In **Australia**, electronic communications and computer records are dealt with under the Evidence Act 1995, which emphasizes the "best evidence" principle while allowing for a degree of procedural flexibility. Australian courts assess electronic evidence based on its probative value and context rather than relying solely on formal technicalities, which often result in unjust exclusions in India.

Implications and the Way Forward

The implications of these findings are profound for the administration of justice. Given the increasing reliance on electronic records in criminal investigations—ranging from cybercrimes and white-collar offenses to terrorism and organized crime—it is imperative that the legal framework governing such evidence be both reliable and efficient.

There is a clear need for **procedural reform** in Indian law to standardize the process of collecting, certifying, and presenting electronic evidence. This could take the form of:

- Standard operating procedures (SOPs) for police and forensic agencies;
- Uniform certification formats for compliance with Section 65B;
- Specialized digital evidence units within law enforcement;
- Mandatory training programs for judicial officers and prosecutors on digital evidence handling.

Additionally, there must be greater **collaboration between law and technology**, including partnerships between legal institutions, forensic labs, and academic bodies. Legal professionals must be sensitized to technological advancements such as block chain evidence authentication, cloud computing, and AI-based data analysis.

Lastly, legislative clarity is needed on contentious issues such as the treatment of cloud-stored data, jurisdiction in cross-border data access, and admissibility of intercepted communications.

Limitations and Exceptions

While this research presents a detailed analysis, it is not without limitations. The study relies heavily on doctrinal methods and legal sources, and therefore does not include empirical data such as interviews with legal practitioners or forensic experts. Additionally, because technological change is rapid, the relevance of current legal standards may diminish quickly, necessitating on-going scholarly engagement.

There are also exceptions to the general trends. In certain high-profile cases, courts have shown remarkable sophistication in handling digital evidence. However, these are not yet reflective of the broader judicial practice across the country.

CASE LAWS

1. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473

- **Court:** Supreme Court of India
- **Parties:** Anvar P.V. (Appellant) vs. P.K. Basheer & Others (Respondents)
- **Facts:** The appellant presented a CD to prove alleged defamatory speech. The High Court allowed it as evidence without a certificate under Section 65B.
- **Issue:** Whether electronic evidence (like CDs) is admissible without a certificate under Section 65B of the Indian Evidence Act, 1872.
- **Judgment:** The Supreme Court held that **Section 65B certificate is mandatory** for electronic evidence to be admissible. Secondary electronic records without the certificate are inadmissible.
- **Significance:** Set strict criteria for the admissibility of electronic records.

2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1

- **Court:** Supreme Court of India
- **Parties:** Arjun Panditrao Khotkar (Appellant) vs. Kailash Kushanrao Gorantyal (Respondent)
- **Facts:** A video recording of nomination filing was submitted without a Section 65B certificate.
- **Issue:** Can electronic evidence be admitted without a 65B certificate if the original device is produced in court?
- **Judgment:** Reaffirmed **Anvar's case** and clarified that the certificate is mandatory unless the original device is produced.
- **Significance:** Reinforced the requirement and clarified practical scenarios regarding 65B certification.

3. State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru (2005) 11 SCC 600

- **Court:** Supreme Court of India
- **Parties:** State (NCT of Delhi) vs. Navjot Sandhu & Others
- **Facts:** Involved the 2001 Indian Parliament attack. Call records and SIM card data were submitted as evidence.
- **Issue:** Whether electronic records like call logs and SIM data without Section 65B certificate are admissible.
- **Judgment:** The Court allowed secondary evidence (printouts) without certification under Section 65B.
- **Significance:** Later overruled by **Anvar v. Basheer**; significant as it highlighted the earlier liberal approach to electronic evidence.

4. Tomaso Bruno v. State of Uttar Pradesh (2015) 7 SCC 178

- **Court:** Supreme Court of India
- **Parties:** Tomaso Bruno & Another (Appellants) vs. State of Uttar Pradesh (Respondent)
- **Facts:** Accused in a murder case challenged the absence of CCTV footage that could prove innocence.
- **Issue:** Whether the non-production of electronic evidence by the prosecution affects the fairness of the trial.
- **Judgment:** The Court emphasized the **importance of electronic evidence**, stating that its non-production amounts to suppression and affects justice delivery.
- **Significance:** Highlighted that electronic evidence can exonerate the accused and must not be suppressed.

5. Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801

- **Court:** Supreme Court of India
- **Parties:** Shafhi Mohammad (Appellant) vs. State of Himachal Pradesh (Respondent)
- **Facts:** The appellant challenged the non-consideration of video evidence on procedural grounds.
- **Issue:** Is a Section 65B certificate always mandatory?
- **Judgment:** The Court held that a 65B certificate is **not mandatory if the party doesn't have control over the device**. This was **later overruled** in Arjun Panditrao.
- **Significance:** Though overruled, it played a vital role in shaping debates around access and control of digital sources.

Recent Case laws

- **Case Title:** State of Tamil Nadu v. Governor of Tamil Nadu & Union of India
- **Court:** Supreme Court of India
- **Bench:** Justices J.B. Pardiwala and R. Mahadevan
- **Date of Judgment:** April 8, 2025

Parties Involved:

- **Petitioner:** State of Tamil Nadu **Respondents:** Governor of Tamil Nadu and Union of India

Facts: Between January 13, 2020, and April 28, 2023, the Tamil Nadu Legislative Assembly passed 12 bills aimed at amending the oversight and appointment processes of state universities. These bills were submitted to the Governor of Tamil Nadu for assent. Two bills proposed shifting inspection and inquiry powers from the Governor (acting as ex officio Chancellor) to the State Government, while eight others sought to transfer the authority to appoint Vice-Chancellors from the Governor to the State Government. Additional provisions included replacing the Secretary to the Tamil Nadu Department of Law in university syndicates with the Secretary to the Department of Finance and centralizing oversight under the Department of Higher Education.

On October 31, 2023, the Government of Tamil Nadu filed a writ petition in the Supreme Court, challenging Governor R.N. Ravi's prolonged withholding of assent to these bills. Subsequently, on November 13, 2023, the Governor withheld assent for 10 bills and reserved 2 bills for the

President's consideration. In response, the Tamil Nadu Legislative Assembly reintroduced and re-approved the 10 bills on November 18, 2023, and resubmitted them to the Governor.

Judgment: On April 8, 2025, the Supreme Court ruled that a State Governor does not possess the constitutional authority to exercise an absolute or pocket veto over legislation duly passed by the State Legislative Assembly. The Court emphasized that such actions undermine the spirit of parliamentary democracy. The bench invoked its extraordinary powers under Article 142 of the Constitution to clear the 10 pending bills, thereby limiting the Governor's discretionary power to withhold assent indefinitely.

Significance: This landmark judgment reinforces the principles of federalism and parliamentary democracy by delineating the constitutional boundaries of a Governor's powers concerning state legislation. It ensures that Governors cannot indefinitely withhold assent to bills passed by State Assemblies, thereby preventing potential legislative stalemates.

CONCLUSION

In an age where digital interactions increasingly shape human behavior, the role of **electronic evidence** in criminal proceedings has become both indispensable and transformative. This research underscores the critical importance of a legal framework that can reliably accommodate digital evidence, ensuring that justice is served through methods that are both technologically informed and constitutionally sound.

The study reveals that **while courts are progressively acknowledging the legitimacy and probative value of electronic evidence**, several structural and procedural deficiencies continue to limit its effective use. Among the most pressing concerns are the **inconsistencies in judicial interpretation of Section 65B of the Indian Evidence Act**, insufficient **technical expertise among legal actors**, and the absence of **uniform protocols** for collecting, preserving, and authenticating digital data. These gaps, if left unaddressed, risk undermining both the integrity of criminal trials and the protection of individual rights.

Comparative insights from jurisdictions such as the United States and the United Kingdom demonstrate that **standardized procedures, forensic rigor, and judicial training** significantly enhance the evidentiary reliability of electronic records. These global practices offer a valuable blueprint for reform in India and other developing legal systems grappling with the same challenges.

The principal conclusion of this study is that the **admissibility and evidentiary value of electronic evidence** must not be treated as a mere procedural formality. Rather, it must be seen as a cornerstone of modern criminal justice—one that requires **robust legal safeguards, interdisciplinary cooperation, and constant technological adaptation**.

Practically, this research advocates for:

- **Legislative clarity** on the technical requirements for admissibility;
- **Capacity-building initiatives** to train judges, prosecutors, and police officers in digital evidence handling;
- **Adoption of best practices** from established legal systems to ensure reliability and fairness;
- **Creation of specialized forensic infrastructure and digital evidence units** within law enforcement agencies.

Ultimately, the integration of electronic evidence into criminal trials must align with constitutional principles, procedural fairness, and the rule of law. When governed by a transparent, consistent, and technologically competent framework, electronic evidence can greatly enhance the efficacy, speed, and credibility of the criminal justice process.

REFERENCE:

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. Indian Evidence Act, 1872 (as amended). Government of India. [Available at: https://legislative.gov.in/sites/default/files/A1872-01.pdf]
4. Navjot Sandhu v. State (also known as the Parliament Attack Case), (2005) 11 SCC 600.
5. Federal Rules of Evidence (U.S.). (2023). Cornell Law School – Legal Information Institute. [https://www.law.cornell.edu/rules/fre]
6. ACPO. (2012). *Good Practice Guide for Digital Evidence* (4th ed.). Association of Chief Police Officers, UK. [https://www.digital-detective.net/digital-forensics-documents/]
   Puttaswamy v. Union of India, (2017) 10 SCC 1.
7. Singh, A. (2021). *Electronic Evidence and Indian Legal System: Challenges and Future Prospects*. *Journal of Cyber Law & Policy*, 3(1), 45–67.
8. ACPO. (2012). *Good practice guide for digital evidence* (4th ed.). Association of Chief Police Officers. https://www.digital-detective.net/digital-forensics-documents/
9. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
10. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
11. Bhansali, R. (2020). *Admissibility of electronic evidence: Emerging trends and judicial response in India*. *Indian Journal of Law and Technology*, 16(2), 120–145.
12. Indian Evidence Act, 1872 (as amended). Government of India. https://legislative.gov.in/sites/default/files/A1872-01.pdf
13. Navjot Sandhu v. State (2005) 11 SCC 600.
14. Puttaswamy v. Union of India, (2017) 10 SCC 1.

15. Singh, A. (2021). Electronic evidence and the Indian legal system: Challenges and future prospects. *Journal of Cyber Law & Policy*, 3(1), 45–67.
16. United States Federal Rules of Evidence. (2023). Cornell Law School Legal Information Institute. https://www.law.cornell.edu/rules/fre
17. UK Parliament. (1990). *Computer Misuse Act 1990*. https://www.legislation.gov.uk/ukpga/1990/18/contents
18. State of Tamil Nadu v. Governor of Tamil Nadu & Union of India (2025)
19. "How Supreme Court cleared 10 Bills using extraordinary powers," *India Today*, April 8, 2025.
20. Supreme Court of India. (2014). *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
21. Supreme Court of India. (2020). *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
22. Supreme Court of India. (2005). *State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru*, (2005) 11 SCC 600.
23. Supreme Court of India. (2015). *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
24. Supreme Court of India. (2018). *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.