INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

PROVING CYBER OFFENCES UNDER BHARATIYA NYAYA SANHITA: EVIDENTIARY CHALLENGES IN THE DIGITAL AGE

AUTHORED BY - SWARA SAWANT & DISHA GUPTA

Abstract

Cyber-crime has increased rapidly with the expansion of digital technology and internet penetration. India has also witnessed a rise in offences such as online fraud, identity theft, cyber stalking, data breaches, and financial scams. The introduction of the Bharatiya Nyaya Sanhita (BNS) has replaced the old criminal code and attempts to modernize criminal law in line with present-day realities. Even though the new framework aims to address modern crimes, the process of proving cyber offences still faces many evidentiary challenges.

Digital evidence is complex, volatile, and easily manipulated, which makes investigation and prosecution difficult. Unlike traditional crimes where physical evidence such as weapons or fingerprints can be presented, cyber offences rely on electronic records such as emails, server logs, IP addresses, and metadata. These forms of evidence require technical expertise for proper collection and analysis.

This research paper studies the nature of cyber offences within the framework of the Bharatiya Nyaya Sanhita and focuses on the evidentiary difficulties that arise during investigation and trial. The study explores issues such as authenticity of digital records, chain of custody, jurisdiction problems, technical knowledge gaps, and dependence on electronic evidence. Courts often struggle to interpret technical material, while investigators sometimes fail to collect evidence in a legally admissible manner. The paper concludes by suggesting improvements in forensic infrastructure, training, and legal procedures.

Keywords

Cyber offences, Digital evidence, Bharatiya Nyaya Sanhita, Cyber-crime investigation Electronic records, Evidentiary challenges, Digital forensics

ISSN: 2582-6433

Introduction

The modern world is deeply connected through digital technology. Communication, financial transactions, education, entertainment, and government services are now conducted through the internet. While this digital transformation has created many opportunities, it has also generated new forms of criminal activity. Cyber-crime is no longer limited to highly skilled hackers but now includes ordinary individuals who exploit technology for fraud, harassment, identity theft, and illegal surveillance. India has experienced rapid growth in internet users and smartphone penetration over the last decade. With affordable data and increasing digital awareness, more people are relying on online platforms for everyday activities. However, this growth has also been accompanied by a sharp rise in cyber-related offences. Online banking fraud, phishing attacks, data theft, and cyber harassment are frequently reported cases.

Traditional criminal law frameworks were not designed to deal with such technologically driven offences. Because of this gap, the Indian legal system has gradually adapted to address digital crime through laws such as the Information Technology Act and now the Bharatiya Nyaya Sanhita. However, the real challenge lies not only in defining cyber offences but in proving them in a court of law. Unlike physical crimes, cyber offences often leave behind digital traces that are invisible and easily alterable. This makes the process of evidence collection, preservation, and presentation much more complicated. Therefore, understanding evidentiary challenges becomes very important in ensuring justice in cybercrime cases.

This paper aims to examine these challenges in detail, particularly in the context of the evolving legal framework in India. It focuses on the difficulties faced during the investigation and trial of cyber offences, and highlights the gap between legal provisions and their practical implementation. By analysing both legal and practical aspects, the study seeks to contribute towards a better understanding of how cyber offences can be effectively proved in the digital age.

Literature Review

Scholars have pointed out that cyber-crime differs from traditional crime mainly because the evidence exists in digital form. Digital information can be copied, modified, or erased easily, which raises serious questions regarding authenticity and reliability. Many researchers have emphasized that electronic evidence lacks the stability of physical evidence. Studies also highlight the role of digital forensic science in cybercrime investigations. Forensic experts use specialized tools to recover deleted files, analyse system logs, and trace online activities.

ISSN: 2582-6433

However, the effectiveness of forensic analysis depends on how well the evidence is preserved at the initial stage.

Legal scholars have also discussed the importance of procedural compliance. Courts require strict adherence to rules related to admissibility of electronic evidence. Failure to follow proper procedures can lead to rejection of crucial evidence. Some research papers have pointed out that many cybercrime cases fail due to technical errors rather than lack of proof. Another important aspect discussed in literature is the lack of technical knowledge among legal professionals. Judges and lawyers may not always understand complex digital concepts, which can affect the outcome of cases. This creates a gap between technological advancements and legal understanding.

(Varsha, 2025)

(Rashotte, 2024)

(Moussa, 2021)[1]

Methodology

This research adopts a doctrinal method of legal analysis. The study relies on secondary sources such as statutory provisions, judicial interpretations, textbooks, research articles, and online legal databases. This study adopts a **doctrinal research methodology**, which focuses on analysing existing legal principles, statutory provisions, and judicial interpretations relating to cyber offences and digital evidence. Primary sources such as the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and the Indian Evidence Act, 1872 have been examined to understand the legal framework governing cybercrimes in India. In addition, relevant case laws and judicial precedents have been referred to in order to assess how courts interpret and apply provisions concerning electronic evidence, particularly in relation to admissibility and authentication.

The research also relies on secondary sources including legal commentaries, academic journals, research papers, and authoritative online databases. A qualitative approach has been used to identify and analyse the key challenges in proving cyber offences, especially those arising from the nature of digital evidence. The study further evaluates procedural issues such as collection, preservation, and presentation of electronic records, with the aim of highlighting gaps between legal provisions and practical implementation. This method helps in developing a

[1] Cyber Crime in India: Trends, Challenges, and Solutions -Rahul Pandit
Cyber Crimes: A Primer On Internet Threats And Email Abuses -G. Ram Kumar
Landmark Judgements on Cyber Crimes and Cyber laws -Dr. Chintan Pathak & Associates

ISSN: 2582-6433

comprehensive understanding of both theoretical and real-world issues in cybercrime adjudication. A qualitative approach is used to identify the major evidentiary challenges faced in cyber offence prosecution. The research involves analysing existing laws related to cyber-crime and studying how courts deal with electronic evidence. The aim is to understand both legal and practical difficulties in proving cyber offences.

Further, the study also includes a critical review of existing literature on cyber laws in India to identify gaps in current research. Many articles focus on explaining statutory provisions but do not adequately address the real-world problems faced during investigation and prosecution. By comparing these studies with the present legal framework, this paper attempts to highlight areas that require improvement. The methodology, therefore, is not limited to describing the law but also aims to evaluate its effectiveness and suggest practical solutions for strengthening the process of proving cyber offences in the digital age.

Results

The study reveals that proving cyber offences presents multiple evidentiary challenges, primarily due to the fragile and intangible nature of digital evidence. Unlike traditional forms of evidence, electronic records can be easily altered, deleted, or manipulated within seconds, raising serious concerns regarding their authenticity and reliability. Issues related to proper authentication and compliance with legal requirements, particularly under Section 65B of the Indian Evidence Act, 1872, often create hurdles in the admissibility of such evidence. Furthermore, maintaining an unbroken chain of custody remains a significant challenge, as any procedural lapse in handling digital data may lead to doubts about its integrity and result in its rejection by courts.

Another major finding is the lack of technical expertise among investigators and legal professionals, which adversely affects the quality of evidence collection and interpretation. Cybercrimes frequently involve cross-border elements, leading to jurisdictional complexities and delays in investigation. The study also highlights the growing use of encryption and anonymity tools by offenders, making it difficult to trace identities and establish guilt beyond reasonable doubt. Additionally, the over-dependence on electronic devices and digital records means that any failure in properly securing or presenting such evidence can weaken the prosecution's case. These challenges collectively demonstrate the urgent need for improved forensic infrastructure, specialised training, and stronger coordination between legal and technical domains.

The study identifies multiple evidentiary challenges in proving cyber offences:

ISSN: 2582-6433

Fragile Nature of Digital Evidence

Digital evidence is extremely fragile and can be altered within seconds. Even a minor change in a file can affect its integrity. Investigators must act quickly to preserve data before it is lost or modified.

Issues Of Authentication

Authentication of electronic records is essential because courts require proof that the data has not been tampered with. It is often difficult to prove who created or accessed a particular digital record.

Chain of Custody

Maintaining a proper chain of custody is crucial. If there is any gap in handling evidence, it may be challenged in court. Improper documentation can lead to doubts about the reliability of evidence.

Lack of technical Expertise

Many law enforcement officers lack training in cyber forensics. This results in improper collection and handling of evidence. Similarly, judges may find it difficult to understand technical details.

Jurisdictional overview

Cyber-crimes often cross-national boundaries. An offence committed in one country may affect victims in another. This creates confusion regarding which court has jurisdiction.

Dependence on Electronical Device

Cybercrime cases rely heavily on digital evidence. If such evidence is not properly collected or presented, it becomes difficult to prove the offence.

Encryption and Anonymity

Offenders often use encryption and anonymous networks to hide their identity. This makes it difficult for investigators to trace the actual culprit.

Discussion or Views

In my opinion, the biggest challenge in proving cyber offences is the gap between law and technology. While laws are being updated, the implementation is still weak. Cybercrime investigation requires strong technical expertise, which is currently lacking in many parts of the system. Law enforcement agencies should receive specialized training in digital forensics and cyber investigation. Proper training can help in better evidence collection and reduce errors. Courts also need greater awareness regarding technological issues. Judges should be

ISSN: 2582-6433

provided with basic technical training so that they can understand digital evidence more effectively.

Another issue is the complexity of legal procedures. Sometimes, even when evidence is strong, it is not presented properly in court. This creates confusion and weakens the case. Simplifying procedures related to electronic evidence can improve the situation. Investment in cyber forensic infrastructure is also very important. Advanced tools and laboratories can help in accurate analysis of digital evidence. Additionally, international cooperation should be strengthened to deal with cross-border cyber-crimes.

Conclusion

Cyber offences present complex evidentiary problems in the criminal justice system. The intangible and volatile nature of digital evidence makes it difficult to collect, preserve, and present in court. Issues such as lack of technical knowledge, improper handling of evidence, and jurisdictional challenges further complicate the process. Bharatiya Nyaya Sanhita is a step forward in addressing modern crimes, but more efforts are needed to ensure effective implementation. Strengthening forensic infrastructure, providing better training for investigators and judges, and simplifying legal procedures will significantly improve cybercrime prosecution. In conclusion, addressing evidentiary challenges is essential for ensuring justice in cyber offence cases and maintaining trust in the digital system.

There is a need for better training, improved digital forensic systems, and clearer procedures for handling electronic evidence. Greater coordination between countries is also important to deal with cyber offences that go beyond national boundaries. This paper also points out that existing studies do not fully address these real-world evidentiary problems. By focusing on these gaps, it tries to bring a more practical perspective to the discussion. In the end, ensuring that digital evidence is properly collected and presented is essential not only for securing convictions but also for maintaining trust in the legal system in an increasingly digital world.[2]

[2] Theft & Fraud: CBI v. Arif Azim (Sony Sambandh Case)
Privacy & Data Protection: K.S. Puttaswamy v. Union of India
Corporate Negligence (SIM Swap): Daffodils Furnishing v. Idea Cellular & Ors
Obscenity/Electronic Records: Sharat Babu Digumarti v. Govt.
Intellectual Property/Unauthorized Access: Syed Asifuddin v. State of Andhra Pradesh

ISSN: 2582-6433

References

1. The Bharatiya Nyaya Sanhita, 2023 [Act Number Act No. 45 of 2023]
2. Information Technology Act, 2000 [Act Number: Act No. 21 of 2000.]
3. Indian Evidence Act, 1872 [Act Number: Act No. 1 of 1872]
4. https://link.springer.com/article/10.1186/s41935-021-00234-6
5. https://www.techjockey.com/blog/top-tools-and-techniques-used-in-digital-forensics-investigations?
6. https://www.fortinet.com/blog/industry-trends/gaps-in-skills-knowledge-technology-pave-way-for-breaches
7. Landmark Judgements on Cyber Crimes and Cyber law -Dr. Chintan Pathak & Associates
8. Cyber Crime in India: Trends, Challenges, and Solutions -Rahul Pandit
9. Cyber Crimes: A Primer On Internet Threats And Email Abuses -G. Ram Kumar