

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.  
All rights reserved.**

## 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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

## ***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.

## **“CYBER FORENSICS AND DIGITAL EVIDENCE: LEGAL AND PRACTICAL CHALLENGES”**

AUTHORED BY - K. RAMANJANEYULU  
LL.M., (Deemed To Be University) School Of Law  
Aurora Higher Education And Research Academy

### **ABSTRACT**

Cyber forensics has become an essential component of modern criminal investigation because computers, mobile phones, cloud platforms, networks, surveillance systems and digital payment applications routinely generate evidence relevant to disputes and offences. At the same time, digital evidence is unusually vulnerable to alteration, deletion, encryption, remote access and loss of contextual information. The legal system therefore has to address two connected questions: how digital material can be collected and preserved scientifically, and how the resulting record can be proved reliably before a court.

This project examines the legal and practical framework governing cyber forensics and digital evidence in India, with particular attention to the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the Information Technology Act, 2000, constitutional safeguards and leading judicial decisions. The study considers acquisition, preservation, hashing, metadata, chain of custody, forensic imaging, cloud evidence, mobile-device evidence, CCTV, call-detail records and electronic communications. It also examines admissibility, authenticity, certificates, expert evidence, privacy, jurisdiction and investigative capacity.

The central finding is that legal recognition of electronic records is no longer the principal difficulty. The more demanding problems concern reliable collection, preservation, documentation, forensic competence, access to third-party data and the ability of investigators and courts to evaluate technical evidence without compromising fairness. A legally admissible digital record must therefore be supported by a trustworthy evidentiary process. The project concludes with suggestions for standardised forensic protocols, stronger training, better preservation mechanisms, clearer inter-agency procedures and continued judicial engagement with emerging technologies.

## 1. INTRODUCTION

Digital technology has changed the nature of evidence. A criminal act may leave no conventional paper trail but may generate browser history, metadata, location information, application logs, emails, chats, photographs, cloud records, transaction trails, CCTV footage or information stored on a mobile device. In many investigations, these records can help establish identity, communication, chronology, intent, location and the connection between a person and an event. Cyber forensics is the discipline through which such material is identified, acquired, preserved, examined and presented in a manner capable of withstanding legal scrutiny.<sup>1</sup>

The expression “digital evidence” is wider than evidence of a conventional cybercrime. Digital evidence may arise in offences involving fraud, cheating, stalking, sexual offences, extortion, terrorism, intellectual property, financial crime, homicide or even ordinary contractual and matrimonial disputes. Consequently, the law of evidence must accommodate digital material without abandoning the principles of authenticity, relevance, reliability and fair trial.

The Bharatiya Sakshya Adhiniyam, 2023 is particularly important in the present Indian framework. It expressly recognises electronic or digital records and provides that such records are not to be denied legal effect merely because they are electronic, subject to the statutory requirements concerning proof. Section 61 gives electronic or digital records legal recognition, section 62 provides the special rule for proving their contents, and section 63 lays down the conditions for admissibility and the certificate mechanism. The Schedule to the BSA also contains a prescribed certificate format referring to devices, digital sources and hash values.<sup>2</sup> The statutory text confirms that electronic or digital records have the same legal effect as other documents subject to section 63.

The procedural side is supplemented by the BNSS. Section 94 permits a court or police officer, subject to its requirements, to require production of documents, electronic communications, communication devices and other things likely to contain digital evidence.<sup>3</sup> The Information Technology Act, 2000 remains relevant to cyber offences and to the broader legal environment surrounding electronic records, computer resources and intermediaries.

The project therefore treats cyber forensics and digital evidence as a combined legal-technical subject. A record that is technically available but poorly preserved may become difficult to

---

<sup>1</sup> Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang, ‘Guide to Integrating Forensic Techniques into Incident Response’ (NIST Special Publication 800-86, National Institute of Standards and Technology 2006).

<sup>2</sup> Bharatiya Sakshya Adhiniyam 2023, ss 61–63 and Schedule.

<sup>3</sup> Bharatiya Nagarik Suraksha Sanhita 2023, s 94.

prove. Conversely, a legally recognised record can lose evidentiary value if the underlying acquisition process is undocumented or vulnerable to challenge.

## 2. RESEARCH PROBLEM

The research problem arises from the gap between the speed and complexity of digital technology and the institutional capacity required to investigate it. Digital evidence can be copied perfectly, but it can also be changed without obvious physical signs. A mobile device may contain encrypted applications, deleted files, multiple user accounts and cloud synchronisation. A cloud record may be stored in another jurisdiction. A CCTV system may automatically overwrite old footage. A social-media account may be controlled by a third party or may be compromised. These realities complicate the traditional assumptions surrounding possession, originality and physical custody.

The legal framework has responded by recognising electronic records and specifying conditions for proof. Yet statutory admissibility is only one part of the problem. Investigators must establish where the evidence came from, who acquired it, how it was preserved, whether it was altered, what tools were used, and whether the person presenting it can explain the process. The research therefore asks whether existing law and forensic practice together provide sufficient safeguards for authenticity and fair adjudication.<sup>4</sup>

## 3. RESEARCH OBJECTIVES

The objectives of this project are:

1. To explain the meaning, scope and stages of cyber forensics and digital evidence.
2. To examine the legal framework under the BSA, BNSS and Information Technology Act.
3. To analyse the principles of authenticity, integrity, relevance, reliability and chain of custody.
4. To study judicial treatment of electronic evidence, particularly the certificate requirement under the earlier Evidence Act and its development into the present BSA framework.
5. To identify practical challenges relating to collection, preservation, analysis, expert evidence, privacy, encryption, cloud computing and cross-border access.

---

<sup>4</sup> Barbara Guttman, Douglas R White, Shannan Williams and Tracy Walraven, 'Digital Evidence Preservation: Considerations for Evidence Handlers' (NISTIR 8387, National Institute of Standards and Technology 2022).

6. To suggest measures for strengthening forensic investigation while protecting fair-trial and privacy interests.
- 7.

#### **4. RESEARCH QUESTIONS**

1. What is cyber forensics and what makes digital evidence legally significant?
2. How does the Bharatiya Sakshya Adhiniyam, 2023 regulate electronic and digital records?
3. What procedural powers under the BNSS assist the collection of digital evidence?
4. What are the major practical threats to authenticity, integrity and chain of custody?
5. What principles emerge from Supreme Court decisions concerning electronic evidence?
6. How can Indian investigative and judicial institutions improve the reliability and fairness of digital evidence?

#### **5. SCOPE OF THE STUDY**

The project focuses primarily on Indian law and practice. It covers electronic evidence generated or stored on computers, mobile devices, storage media, networks, cloud services, communication platforms, CCTV systems and digital payment systems. The study concentrates on criminal investigation and adjudication, while recognising the relevance of digital evidence in civil and other proceedings.

The project also considers the relationship between statutory evidentiary rules and technical forensic procedures. Comparative foreign law is not examined in detail because the central purpose is to understand the Indian legal and institutional framework.

#### **6. RESEARCH METHODOLOGY**

The study follows a doctrinal and analytical methodology. Primary materials include the Constitution of India, the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Information Technology Act, 2000 and reported Supreme Court decisions. Secondary materials include standard works on evidence, cyber law and constitutional law, together with official judicial and governmental material. The project analyses the relationship between statutory admissibility and practical forensic reliability, rather than treating them as separate subjects.

## 7. REVIEW OF LITERATURE

The literature on electronic evidence broadly demonstrates that technological change places pressure on conventional evidentiary concepts. Scholarly writing on cyber law emphasises that digital information is intangible, easily reproducible and often dependent upon technical systems that are difficult for a court to inspect directly. Evidence scholarship has focused particularly on authenticity, reliability, preservation and the dangers of manipulation.<sup>5</sup>

Indian constitutional scholarship is also relevant because digital investigations can implicate privacy, dignity and informational autonomy. The Supreme Court's privacy jurisprudence makes it necessary to consider not only whether investigators can obtain information but also whether collection and use are legally justified and proportionate.<sup>6</sup>

The literature therefore supports an integrated approach: digital evidence must be scientifically reliable, legally obtained and fairly presented.<sup>7</sup>

## 8. CYBER FORENSICS: CONCEPT AND FORENSIC PROCESS

Cyber forensics may be described as the application of scientific methods to the identification, collection, preservation, examination, analysis and presentation of information from digital devices and systems. The forensic process commonly begins with identification of potential sources: a mobile phone, computer, hard disk, pen drive, server, router, DVR, cloud account or online platform. Investigators then seek to preserve the source so that examination does not unnecessarily change the original data.<sup>8</sup>

Forensic imaging is a central technique. Instead of repeatedly examining an original storage device, an investigator may create a forensic image and calculate a cryptographic hash of the relevant data. A hash value functions as a digital integrity marker: if the underlying data changes, the resulting hash will ordinarily change. The BSA Schedule expressly accommodates hash values in its certificate format and refers to algorithms such as SHA-1, SHA-256 and MD5.<sup>9</sup> In practice, the reliability of the evidence depends not only on the hash but also on the documented procedure used to acquire, store and examine the material.

Chain of custody is equally important. It records the movement and handling of evidence from seizure or acquisition to forensic examination and production before the court. A proper chain

<sup>5</sup> Avtar Singh, *Law of Information Technology* (Universal Law Publishing, latest available edn).

<sup>6</sup> Ratanlal and Dhirajlal, *The Law of Evidence* (LexisNexis, latest available edn).

<sup>7</sup> Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

<sup>8</sup> Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang, 'Guide to Integrating Forensic Techniques into Incident Response' (NIST Special Publication 800-86, NIST 2006).

<sup>9</sup> Bharatiya Sakshya Adhiniyam 2023, Schedule.

should identify the item, source, date and time of collection, person responsible, storage location, transfers, forensic tools used and relevant hash information. If the chain is incomplete, the defence may question whether the item produced in court is the same material that was originally collected.

Digital evidence also includes volatile information. Data held in RAM, active network connections, temporary files and certain session information can disappear when a device is shut down. Investigators must therefore distinguish between live acquisition and dead-box examination. The correct method depends on the device, the circumstances and the evidentiary objective. Improper handling may destroy information that cannot later be reconstructed.<sup>10</sup>

Mobile forensics presents additional difficulties. Smartphones contain application databases, photographs, location records, cloud synchronisation, biometric controls and encrypted communications. Modern devices may also use secure hardware and application-level encryption. A forensic examiner must document the extraction method and understand its limitations. A report should not simply state that “data was recovered”; it should explain what was extracted, from which source, by which method and with what limitations.<sup>11</sup>

## 9. LEGAL FRAMEWORK FOR DIGITAL EVIDENCE IN INDIA

The BSA marks an important transition in Indian evidence law. Section 61 provides that an electronic or digital record cannot be rejected merely because it is electronic or digital, while section 62 directs that its contents be proved in accordance with section 63.<sup>12</sup> Section 63 is therefore central to the evidentiary treatment of electronic records. The statutory scheme recognises the need to establish the reliability of the computer or communication device and the circumstances in which the output was produced. The accompanying Schedule prescribes a certificate format containing information about the device or source and the hash value of the record.<sup>13</sup>

The development of Indian case law under the former Indian Evidence Act, 1872 remains important for understanding the present framework. In *Anvar P.V. v P.K. Basheer*, the Supreme Court held that secondary electronic evidence had to satisfy the requirements of section 65B.<sup>14</sup> The decision emphasised the statutory safeguards governing electronic records.

---

<sup>10</sup> Barbara Guttman, Douglas R White, Shannan Williams and Tracy Walraven, ‘Digital Evidence Preservation: Considerations for Evidence Handlers’ (NISTIR 8387, NIST 2022).

<sup>11</sup> National Institute of Standards and Technology, ‘Digital Forensics’, NIST Computer Security Resource Center Glossary.

<sup>12</sup> Bharatiya Sakshya Adhiniyam 2023, ss 61–62.

<sup>13</sup> Bharatiya Sakshya Adhiniyam 2023, s 63 and Schedule.

<sup>14</sup> *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473

In *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, a Constitution Bench reaffirmed the importance of the certificate requirement and clarified the position concerning original electronic records and the circumstances in which the certificate may not be necessary.<sup>15</sup> The Court distinguished the original electronic record from computer output and considered the circumstances in which the certificate requirement operated.

These decisions remain significant for understanding the evidentiary principles that informed the transition to the BSA. The present law should nevertheless be read on its own terms. The BSA has replaced the former section 65B framework with sections 61–63 and the Schedule. The practical lesson is that lawyers and investigators should not mechanically reproduce older terminology; they should identify the applicable provision of the BSA and comply with its present requirements.

The BNSS provides an important investigative mechanism in section 94. It allows a court or police officer to require production of a document, electronic communication, communication device or other thing likely to contain digital evidence when such production is necessary or desirable for an investigation, inquiry, trial or proceeding.<sup>16</sup> This provision is significant because digital evidence is frequently held by third parties such as service providers, banks, employers, platforms or other institutions. The BNSS expressly defines “audio-video electronic” methods broadly enough to include communication devices and electronic communication in specified procedural contexts.

The Information Technology Act also remains relevant. Its provisions address computer-related offences, identity theft, cheating by personation using computer resources, violation of privacy and preservation and retention of information by intermediaries.<sup>17</sup> For cyber-forensic practice, the Act and the evidence statutes must be read together: one may define or regulate conduct and digital systems, while the evidence law governs how the resulting records are proved.

## 10. LEGAL AND PRACTICAL CHALLENGES

The first major legal challenge is **authenticity**. A screenshot, printout or forwarded message may look convincing but may not reveal its original source. A court therefore needs to know whether the material is genuine, complete and connected to the relevant device or account. Authentication can involve testimony, system records, forensic examination, certificates, metadata and corroborating evidence.

<sup>15</sup> *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

<sup>16</sup> Bharatiya Nagarik Suraksha Sanhita 2023, s 94.

<sup>17</sup> Information Technology Act 2000, ss 66–67C.

The second challenge is **integrity**. Digital files can be copied, edited, renamed or transformed. Even when alteration is not visible to an ordinary observer, metadata may change. Forensic procedures must therefore minimise interaction with originals, use appropriate write-blocking or equivalent safeguards where applicable, calculate and record hashes, and maintain detailed examination notes.

The third challenge is **attribution**. The presence of a message on a device does not automatically establish who authored it. A phone may be shared, a computer account may be compromised, credentials may be stolen, or an automated process may generate a record. Attribution should therefore be based on the total evidentiary circumstances rather than on the mere existence of a file or account.

The fourth challenge is **cloud computing**. Evidence may be distributed across data centres and jurisdictions. The investigator may not possess the physical infrastructure on which the data resides. Preservation requests, lawful access mechanisms and cooperation with service providers become important. Data may also be subject to retention limits, encryption and platform-specific formats.<sup>18</sup>

The fifth challenge is **encryption and locked devices**. Strong encryption protects legitimate users but can complicate lawful investigations. Investigators must work within statutory powers and judicial safeguards rather than treating technical difficulty as a justification for unrestricted access.

The sixth challenge concerns **expert evidence**. Courts may need assistance in understanding forensic tools, extraction methods, hash values, metadata and system architecture. Expert testimony can be useful, but expert opinion should not replace proof of the underlying facts. The forensic examiner must be able to explain the method, source, reliability and limitations of the examination.

The seventh challenge is **privacy**. Digital devices contain vast quantities of personal information unrelated to the offence under investigation. The Supreme Court in *Justice K.S. Puttaswamy (Retd.) v Union of India* recognised privacy as constitutionally protected and linked it with dignity and autonomy.<sup>19</sup> Digital searches should therefore be connected to lawful investigative objectives and conducted with safeguards appropriate to the intrusiveness of the search. The question is not merely whether information exists but whether its acquisition and use are legally justified.

---

<sup>18</sup> Scientific Working Group on Digital Evidence, 'Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers' (SWGDE 23-F-004-1.1, 2025).

<sup>19</sup> *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

The eighth challenge is the **preservation of evidence held by private entities**. Banks, telecom operators, social-media platforms, cloud providers and payment intermediaries may each hold only a portion of the relevant evidentiary picture. Delays or inconsistent preservation practices can result in loss of evidence. Standardised preservation requests and clear escalation procedures are therefore important.<sup>20</sup>

## 11. PRACTICAL FORENSIC PROCEDURE AND INSTITUTIONAL ISSUES

A practical cyber-forensic investigation should proceed through a documented sequence. First, investigators should identify potential sources and define the evidentiary objective. Second, they should secure the scene and prevent unnecessary access or alteration. Third, they should document the device or system condition, including relevant identifiers. Fourth, they should acquire data using a method appropriate to the source. Fifth, integrity values and acquisition details should be recorded. Sixth, the original evidence should be preserved and examination should ordinarily be performed on a forensic copy. Seventh, the examiner should maintain a contemporaneous record of tools, versions, commands or relevant procedures and findings. Finally, the report should distinguish raw observations from interpretations.<sup>21</sup>

Training is a major institutional requirement. A police officer who knows criminal procedure but lacks basic digital-forensic knowledge may unintentionally damage evidence. Conversely, a technically skilled examiner who does not understand evidentiary requirements may produce a scientifically interesting report that is difficult to prove. Investigation teams therefore require both technical and legal competence.

Standardisation would improve consistency. Agencies should adopt uniform forms for seizure, imaging, hash verification, storage, transfer and forensic reporting. Digital evidence lockers should record access and movement. Where feasible, automated audit logs can supplement manual registers. Courts can also benefit from concise forensic reports that identify the source, acquisition method, hash, examination process and limitations.

The Supreme Court has repeatedly treated electronic evidence as requiring attention to statutory safeguards rather than informal assumptions about technological reliability. The continuing importance of these safeguards is illustrated by the Court's decisions concerning electronic records and certificates.<sup>22</sup> The judiciary has also shown increasing institutional attention to digital transformation and electronic-evidence management.

<sup>20</sup> Information Technology Act 2000, s 67C.

<sup>21</sup> Kent et al, 'Guide to Integrating Forensic Techniques into Incident Response' (n 1).

<sup>22</sup> *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

Another practical issue is the changing technological environment. Artificial intelligence can generate synthetic images, audio and video. Deepfakes may create apparently authentic material that never existed in the form presented. Metadata alone may not be sufficient to establish authenticity. Future forensic practice may therefore need provenance mechanisms, trusted logs, content-authenticity standards and stronger verification of source devices and accounts.

The law must also address the risk of **over-collection**. A forensic image of a phone can contain years of photographs, health information, private communications, financial records and information concerning third parties. Investigators should therefore use search strategies and legal authorisation appropriate to the scope of the investigation. Privacy-protective procedures can strengthen rather than weaken the legitimacy of digital investigation.<sup>23</sup>

## 12. ANALYSIS AND FINDINGS

The study produces the following principal findings:

**First**, Indian law now expressly recognises electronic and digital records, but admissibility remains dependent upon compliance with statutory requirements and proof of authenticity and integrity. The BSA gives electronic and digital records legal effect subject to its evidentiary requirements.<sup>24</sup>

**Second**, cyber forensics is not merely a technical exercise. The evidentiary value of a digital record depends on the interaction between forensic method, statutory procedure and judicial evaluation.

**Third**, chain of custody remains a practical weakness whenever agencies fail to document seizure, acquisition, storage, transfer and examination comprehensively.

**Fourth**, the transition from the Indian Evidence Act to the BSA requires lawyers, investigators and courts to update their terminology and procedures. Older case law remains valuable as precedent on underlying principles, but current pleadings and certificates should refer to the BSA provisions actually in force.

**Fifth**, cloud evidence, encryption, mobile applications and cross-border data create difficulties that cannot be solved by evidence law alone. Cooperation among police, forensic laboratories, prosecution authorities, service providers and judicial institutions is essential.<sup>25</sup>

---

<sup>23</sup> *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

<sup>24</sup> Bharatiya Sakshya Adhiniyam 2023, ss 61–63.

<sup>25</sup> *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

**Sixth**, privacy and digital investigation must be addressed together. Broad access to a device can expose large quantities of unrelated personal information. Lawful authority, necessity and proportionality are therefore important safeguards.

**Seventh**, expert capacity and institutional infrastructure require continuing development. Standardised forensic protocols, accredited laboratories, trained investigators and reliable digital evidence management systems can reduce disputes over authenticity and custody.

### 13.SUGGESTIONS AND RECOMMENDATIONS

The following measures may strengthen the Indian framework:

**1. Standardised national protocols:**

Nationally consistent protocols should be developed for seizure, imaging, hashing, preservation, examination and reporting of digital evidence.

**2. Continuous training:**

Investigating officers, prosecutors, judges and forensic personnel should receive continuing training on the BSA and modern forensic techniques.

**3. Secure digital evidence repositories:**

Agencies should maintain secure digital evidence repositories with access logs and tamper-evident audit trails.

**4. Detailed forensic reports:**

Forensic laboratories should record tool versions, extraction methods, hash values and known limitations in forensic reports.

**5. Preservation mechanisms:**

Clear procedures should be developed for preservation requests to banks, telecom operators, cloud providers and online platforms.

**6. Cross-border cooperation:**

Mechanisms for lawful and timely access to cross-border digital evidence should be strengthened through international cooperation.

**7. Privacy-sensitive forensic searches:**

Investigators should adopt procedures that allow relevant information to be identified

- 
26. Karen Kent et al, 'Guide to Integrating Forensic Techniques into Incident Response' (NIST Special Publication 800-86, NIST 2006).  
27. Barbara Guttman et al, 'Digital Evidence Preservation: Considerations for Evidence Handlers' (NISTIR 8387, NIST 2022).  
28. Scientific Working Group on Digital Evidence, 'Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers' (2025).

without unnecessarily exposing unrelated personal data.

**8. Judicial scrutiny:**

Courts should focus on source, authenticity, integrity, attribution and relevance rather than treating a screenshot or printout as automatically self-proving.

**9. Emerging technologies:**

Forensic standards should be periodically updated to address artificial intelligence, deepfakes, encrypted applications and synthetic identity fraud.

**10. Institutional interoperability:**

Police systems, forensic laboratories, prosecution offices and courts should develop interoperable systems so that digital evidence can be securely tracked throughout the life of a case.

## 14. CONCLUSION

Cyber forensics and digital evidence have become central to contemporary justice. The Indian legal system has moved beyond the question of whether electronic records can be evidence at all. The present challenge is to ensure that digital evidence is collected lawfully, preserved reliably, examined scientifically and presented transparently.

The Bharatiya Sakshya Adhiniyam, 2023 provides a modern statutory foundation by recognising electronic and digital records and prescribing a specific evidentiary framework. The BNSS strengthens investigative powers relating to documents, electronic communications and devices, while the Information Technology Act continues to provide important substantive and regulatory provisions. Judicial decisions such as *Anvar P.V.* and *Arjun Panditrao Khotkar* demonstrate the Supreme Court's sustained concern with authenticity and statutory compliance. Ultimately, reliable digital evidence requires a chain of trust: from the device or system, through acquisition and preservation, to forensic examination and courtroom presentation. If any link is weak, the evidentiary value may be questioned. At the same time, digital investigation must respect privacy, due process and fair-trial principles. The future of cyber forensics in India therefore lies not simply in acquiring more technology, but in building dependable legal, technical and institutional practices around that technology.

## BIBLIOGRAPHY

### Primary Sources

1. Constitution of India.
2. Information Technology Act 2000.

3. Bharatiya Nagarik Suraksha Sanhita 2023.
4. Bharatiya Sakshya Adhiniyam 2023.
5. *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473.
6. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
7. *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.
8. *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.

### Secondary Sources and Institutional Materials

9. Avtar Singh, *Law of Information Technology* (Universal Law Publishing, latest available edn).
10. Ratanlal and Dhirajlal, *The Law of Evidence* (LexisNexis, latest available edn).
11. Karen Kent, Suzanne Chevalier, Tim Grance and Hung Dang, 'Guide to Integrating Forensic Techniques into Incident Response' (NIST Special Publication 800-86, National Institute of Standards and Technology 2006).
12. Barbara Guttman, Douglas R White, Shannan Williams and Tracy Walraven, 'Digital Evidence Preservation: Considerations for Evidence Handlers' (NISTIR 8387, National Institute of Standards and Technology 2022).
13. Scientific Working Group on Digital Evidence, 'Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers' (SWGDE 23-F-004-1.1, 2025).
14. National Institute of Standards and Technology, 'Digital Forensics', NIST Computer Security Resource Center Glossary.
15. Supreme Court of India, e-Committee materials concerning electronic evidence, digital evidence management and judicial process re-engineering.