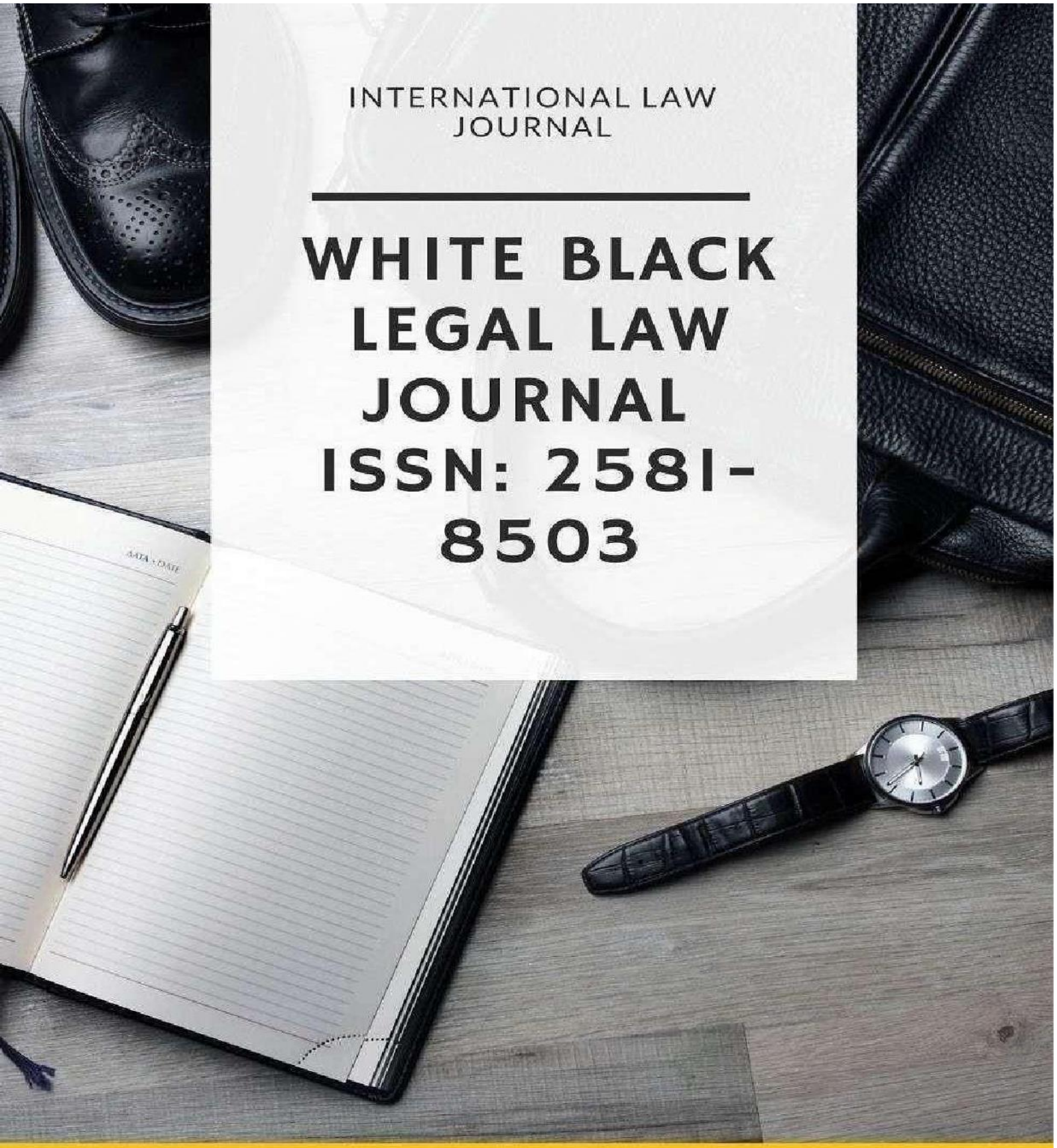


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

WHITE BLACK LEGAL

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

A STUDY ON ADMISSIBILITY OF DIGITAL EVIDENCE IN SEXUAL OFFENCES

AUTHORED BY - A. MOHAMMED ASKAR

ABSTRACT

Digital evidence has become a central feature of the investigation and trial of sexual offences. Messages, photographs, videos, call records, location data and surveillance footage can identify the accused, fix time and place, corroborate the survivor and reveal conduct before and after the offence. At the same time, electronic records can be altered, fabricated or misunderstood, and their use in sexual offence cases raises concerns of privacy, dignity and fair trial that do not arise in the same way in other prosecutions.

This study examines the admissibility of digital evidence in sexual offences under Indian law. It analyses the constitutional protections under Articles 14, 20(3) and 21, the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Nyaya Sanhita, 2023, the Protection of Children from Sexual Offences Act, 2012, the Information Technology Act, 2000, the intermediary rules and selected international instruments. It traces the judicial development of the certificate requirement from Navjot Sandhu to Anvar P.V. and Arjun Panditrao Khotkar, and considers how the new statutory scheme may operate in practice.

The study highlights the importance of a survivor-centred and rights-respecting approach. It identifies practical difficulties in authenticating electronic records, preserving them, protecting intimate material and obtaining timely forensic support. It recommends clearer procedure for the certificate, standard protocols for collection and storage, stronger forensic capacity, early preservation by platforms and telecom operators, and training of police, prosecutors and judges. The study concludes that reliable digital evidence and the dignity of survivors can be secured together through careful procedure and sensitive implementation.

KEYWORDS

Digital Evidence, Electronic Records, Admissibility, Sexual Offences, Bharatiya Sakshya Adhiniyam, Section 63 Certificate, Chain of Custody, Survivor Dignity, Fair Trial, Cyber Forensics.

TABLE OF CONTENTS

S.NO	CONTENT
CHAPTER – I	**INTRODUCTION**
1.1	BACKGROUND OF THE STUDY
1.2	SIGNIFICANCE OF THE STUDY
1.3	REVIEW OF LITERATURE
1.4	RESEARCH GAP
1.5	RESEARCH OBJECTIVES
1.6	RESEARCH QUESTIONS
1.7	RESEARCH METHODOLOGY
1.8	LIMITATIONS OF THE STUDY
1.9	SCHEME OF THE STUDY
CHAPTER – II	**DIGITAL EVIDENCE AND SEXUAL OFFENCES**
2.1	DIGITAL EVIDENCE
2.2	MEANING AND CONCEPT OF DIGITAL EVIDENCE
2.3	EVOLUTION OF DIGITAL EVIDENCE LAW IN INDIA
2.4	DIGITAL EVIDENCE AND THE SURVIVOR'S DIGNITY
2.5	PRINCIPAL FORMS OF DIGITAL EVIDENCE IN SEXUAL OFFENCE CASES
CHAPTER – III	**PRINCIPLES OF EVIDENCE LAW AND FAIR TRIAL**
3.1	MEANING OF ADMISSIBILITY
3.2	DEVELOPMENT OF THE PRINCIPLES
3.3	CORE PRINCIPLES
3.3.1	RELEVANCE
3.3.2	AUTHENTICITY
3.3.3	INTEGRITY AND CHAIN OF CUSTODY
3.3.4	FAIR TRIAL AND THE RIGHTS OF THE ACCUSED
3.3.5	BURDEN AND STANDARD OF PROOF
3.3.6	SURVIVOR-CENTRED PROCEDURE
3.4	CRITIQUE OF THE PRESENT APPROACH
3.5	EVIDENCE LAW AND GENDER JUSTICE
3.6	EVIDENCE LAW AND THE DIGNITY OF THE SURVIVOR
CHAPTER – IV	**LEGAL FRAMEWORK FOR DIGITAL EVIDENCE IN INDIA**
4.1	CONSTITUTION OF INDIA
4.1.1	ARTICLE 14 – RIGHT TO EQUALITY
4.1.2	ARTICLE 20(3) – PROTECTION AGAINST SELF-INCRIMINATION
4.1.3	ARTICLE 21 – LIFE, PERSONAL LIBERTY, PRIVACY AND DIGNITY
4.2	BHARATIYA SAKSHYA ADHINIYAM, 2023
4.2.1	DEFINITIONS AND PRIMARY EVIDENCE
4.2.2	SECTIONS 61 TO 63 – ADMISSIBILITY OF ELECTRONIC RECORDS
4.2.3	EXPERT OPINION AND EXAMINER OF ELECTRONIC EVIDENCE
4.2.4	PRESUMPTIONS AND PROVISIONS SPECIFIC TO SEXUAL OFFENCES
4.2.5	JUDICIAL INTERPRETATION OF THE CERTIFICATE REQUIREMENT
4.3	BHARATIYA NAGARIK SURAKSHA SANHITA, 2023
4.3.1	REGISTRATION AND RECORDING OF INFORMATION
4.3.2	SEARCH, SEIZURE AND PRODUCTION OF DIGITAL MATERIAL
4.3.3	FORENSIC INVESTIGATION AND STATEMENTS BEFORE THE MAGISTRATE
4.3.4	ELECTRONIC TRIAL AND IN-CAMERA PROCEEDINGS

S.NO	CONTENT
4.4	BHARATIYA NYAYA SANHITA, 2023 AND THE POCSO ACT, 2012
4.4.1	SEXUAL OFFENCES UNDER THE BNS
4.4.2	PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT, 2012
4.5	INFORMATION TECHNOLOGY ACT, 2000 AND INTERMEDIARY RULES
4.6	DIGITAL PERSONAL DATA PROTECTION FRAMEWORK
4.7	INTERNATIONAL AND COMPARATIVE FRAMEWORK
4.7.1	BUDAPEST CONVENTION ON CYBERCRIME, 2001
4.7.2	CEDAW AND COMPARATIVE APPROACHES
CHAPTER – V	**FORMS OF DIGITAL EVIDENCE AND MODES OF PROOF**
5.1	ELECTRONIC RECORDS AND MODES OF PROOF
5.2	CCTV AND SURVEILLANCE FOOTAGE
5.3	MOBILE PHONE, MESSAGING AND LOCATION DATA
5.4	AUDIO-VIDEO RECORDINGS AND VOICE EVIDENCE
5.5	INTIMATE IMAGES AND VIDEOS AS EVIDENCE
5.6	FORENSIC IMAGING, HASH VALUES AND CHAIN OF CUSTODY
5.7	TECHNOLOGICAL CHALLENGES
5.8	IMPACT ON PROSECUTION AND SURVIVORS
5.9	SUMMARY OF EVIDENCE TYPES AND PROOF ISSUES
CHAPTER – VI	**ANALYSIS AND LEGAL CHALLENGES**
6.1	SURVIVOR-CENTRED ANALYSIS OF DIGITAL EVIDENCE
6.2	CERTIFICATE REQUIREMENT AND FORMALISM
6.3	PRIVACY, DIGNITY AND SECONDARY VICTIMISATION
6.4	RIGHTS OF THE ACCUSED AND FAIR TRIAL
6.5	GENDER BIAS IN DIGITAL EVIDENCE PRACTICE
6.6	ADEQUACY OF EXISTING LEGAL REMEDIES
6.7	CHALLENGES IN INVESTIGATION AND DIGITAL EVIDENCE
6.8	INTERMEDIARY AND PLATFORM ACCOUNTABILITY
6.9	IDENTIFICATION OF LEGAL GAPS
CHAPTER – VII	**FINDINGS, SUGGESTIONS AND CONCLUSION**
7.1	MAJOR FINDINGS OF THE STUDY
7.2	FINDINGS RELATING TO THE SURVIVOR'S DIGNITY
7.3	FINDINGS RELATING TO PRINCIPLES OF EVIDENCE AND FAIR TRIAL
7.4	FINDINGS RELATING TO THE INDIAN LEGAL FRAMEWORK
7.5	SUGGESTIONS AND RECOMMENDATIONS
7.6	ANSWERS TO THE RESEARCH QUESTIONS
7.7	CONCLUSION
7.8	SCOPE FOR FUTURE RESEARCH
8	**REFERENCES**

WHITE BLACK LEGAL

TABLE OF CASES

S. No.	Name of the Case	Citation	Relevance to Our Article
1	Anvar P.V. v. P.K. Basheer	(2014) 10 SCC 473	Certificate under s. 65B mandatory for secondary electronic evidence
2	Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	(2020) 7 SCC 1	Certificate as pre-condition; production may be directed by court
3	Shafhi Mohammad v. State of H.P.	(2018) 2 SCC 801	Relaxation of certificate where device not in possession
4	State (NCT of Delhi) v. Navjot Sandhu	(2005) 11 SCC 600	Earlier approach to proof of electronic records
5	Tomaso Bruno v. State of U.P.	(2015) 7 SCC 178	Electronic evidence and CCTV footage in criminal trial
6	Sonu @ Amar v. State of Haryana	(2017) 8 SCC 570	Stage at which objection to certificate must be raised
7	Sudhir Chaudhary v. State (NCT of Delhi)	(2016) 8 SCC 307	Proof and reliability of video recordings
8	State of Maharashtra v. Dr. Praful B. Desai	(2003) 4 SCC 601	Video-conference examination as presence
9	Sakshi v. Union of India	(2004) 5 SCC 518	Sensitive procedure in sexual abuse trials
10	Justice K.S. Puttaswamy (Retd.) v. Union of India	(2017) 10 SCC 1	Privacy, dignity and proportionality
11	Shreya Singhal v. Union of India	(2015) 5 SCC 1	Intermediary liability and online content
12	State of Punjab v. Gurmit Singh	(1996) 2 SCC 384	Sensitivity in rape trials and in-camera hearing
13	Bharwada Bhoginbhai Hirjibhai v. State of Gujarat	(1983) 3 SCC 217	Appreciation of prosecutrix's testimony
14	Ram Singh v. Col. Ram Singh	1985 Supp SCC 611	Conditions for admitting tape-recorded statements
15	R.M. Malkani v. State of Maharashtra	(1973) 1 SCC 471	Tape-recorded conversations as evidence
16	State of Bombay v. Kathi Kalu Oghad	AIR 1961 SC 1808	Self-incrimination and compelled specimens
17	Ritesh Sinha v. State of U.P.	(2019) 8 SCC 1	Voice samples of the accused
18	Nipun Saxena v. Union of India	(2019) 2 SCC 703	Non-disclosure of identity of victims
19	Mohd. Ajmal Amir Kasab v. State of Maharashtra	(2012) 9 SCC 1	Reliance on CCTV and electronic records
20	Bodhisattwa Gautam v. Subhra Chakraborty	(1996) 1 SCC 490	Rape as a violation of Article 21
21	Lalita Kumari v. Government of Uttar Pradesh	(2014) 2 SCC 1	Mandatory registration of FIR for cognizable offences

CHAPTER – I
INTRODUCTION

1. INTRODUCTION

"WHEN THE TRUTH IS STORED ON A SCREEN, THE LAW MUST KNOW HOW TO READ IT WITHOUT LOSING THE PERSON BEHIND IT."

Digital technology has changed both the manner in which sexual offences are committed and the manner in which they are proved. Mobile phones, messaging applications, social media accounts, cloud storage, CCTV systems and location services now record fragments of almost every human interaction. In a sexual offence, which is usually committed in private and without independent eyewitnesses, such records may be the only objective material capable of supporting or contradicting the account of the survivor or the accused.

Digital material is, however, fragile. It can be copied, edited, deleted or fabricated with ease, and a copy may look identical to the original. For this reason the law of evidence does not admit electronic records on the strength of their appearance alone. In India, the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which replaced the Indian Evidence Act, 1872 with effect from 1 July 2024, recognises electronic and digital records as documents and prescribes conditions for their admissibility.[1] The Supreme Court had earlier insisted on strict compliance with the corresponding certificate requirement of the Evidence Act.[2]

Sexual offence trials add a further dimension. The digital record may itself contain intimate images or private communications of the survivor, and the process of collecting, exhibiting and examining it can expose her to renewed humiliation. Procedural rules relating to in-camera trial, protection of identity and audio-video recording of statements are therefore as important as rules of authenticity. The practical significance of the issue is considerable, because national crime statistics have recorded more than thirty thousand registered cases of rape in a single year, while conviction rates have remained comparatively low.[3]

This study examines the admissibility of digital evidence in sexual offences under Indian law. It analyses the constitutional, statutory and judicial framework, identifies the difficulties of authentication, investigation and fair trial, and considers whether existing law adequately balances the survivor's dignity, the rights of the accused and the integrity of the evidence.

1.1 Background of the Study

Evidence is the means by which a court reaches a finding of fact. Traditional evidence law was designed around oral testimony and paper documents, and its rules on proof of contents, originals and secondary copies reflect that history. The arrival of computers, mobile phones and the internet required the law to decide how information that exists only as electrical or magnetic signals should be brought before a court. India first addressed the question through the

[1]Bharatiya Sakshya Adhiniyam, 2023, ss. 2(1)(d), 2(1)(e), 61, 62 and 63.
[2]Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[3]National Crime Records Bureau, Crime in India (annual reports), chapters on crimes against women.

Information Technology Act, 2000, which inserted sections 65A and 65B into the Evidence Act. Those provisions have now been carried forward, with changes, into the BSA.

Sexual offences are among the categories of crime in which digital evidence has become most prominent. Chats and voice notes may show the relationship between the parties, threats or inducement. Photographs and videos may be recorded by the offender and later used for blackmail. Call detail records, tower locations and GPS data may place an accused at a particular place. CCTV footage may show movement before and after an incident. Medical and forensic reports, which were once the principal scientific evidence, are now supplemented by digital forensic reports from mobile phones and computers.

The legal difficulty is that the same material raises competing concerns. The prosecution needs to produce it in a form that a court will accept. The accused is entitled to challenge its authenticity and to a fair trial. The survivor is entitled to privacy, dignity and protection from secondary victimisation. A rule that is too rigid may defeat genuine prosecutions on technical grounds, while a rule that is too lax may allow fabricated material to influence a conviction. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) and the Bharatiya Nyaya Sanhita, 2023 (BNS) add further provisions on recording, search, seizure and the definition of offences.

Practical obstacles also arise. Survivors may delete messages out of fear or shame, may not know that metadata matters, or may hand over a phone without understanding the consequences. Police stations may lack forensic tools and trained personnel. Platforms may take time to respond to requests for data. Therefore, admissibility of digital evidence in sexual offences must be studied not only as a technical rule of evidence but also as a question of access to justice.

1.2 Significance of the Study

The study is significant because the outcome of many sexual offence cases now depends on how digital material is collected and proved. A failure to comply with a procedural requirement may result in the exclusion of evidence that is reliable in substance, while careless handling may allow doubt to be raised about evidence that is genuine. Clear understanding of the law helps investigators, prosecutors, defence counsel and judges to deal with such material consistently.

The study is also timely. The BSA, the BNSS and the BNS came into force on 1 July 2024, and their provisions on electronic records, audio-video recording and electronic trial are still being interpreted. Examining the new provisions against the earlier case law helps identify what has changed, what has been retained and what remains uncertain.

Another aspect of significance is the protection of survivors. Digital evidence frequently includes intimate material, and its repeated viewing, circulation or reproduction in court records may aggravate the harm. The study therefore considers how the law can secure reliable

proof while minimising exposure of the survivor, in keeping with the constitutional guarantee of dignity under Article 21.

Finally, the study may contribute to policy discussion on forensic capacity, uniform standards for preservation of electronic records, accountability of online platforms and training of police and judicial officers.

1.3 Review of Literature

The review of literature examines books, legal commentaries, articles, reports and judicial decisions relevant to electronic evidence, sexual offences and the protection of survivors. It helps identify issues already examined and the areas that require further analysis.

Books and Legal Literature

1. Eoghan Casey – Digital Evidence and Computer Crime. This work explains the technical foundations of digital forensics, including acquisition, preservation, analysis and reporting of electronic material. It is relevant because the admissibility of digital evidence in practice depends upon whether technical procedures were followed and documented.
2. Stephen Mason and Daniel Seng (eds.) – Electronic Evidence. This work discusses the treatment of electronic evidence in several legal systems, including questions of authenticity, presumptions and expert evidence. It offers a comparative basis for assessing the Indian certificate-based approach.
3. Ratanlal and Dhirajlal, Sarkar and Batuk Lal – Commentaries on the Law of Evidence. These standard commentaries explain relevance, admissibility, documentary evidence and expert opinion under the Indian Evidence Act. They remain useful for understanding the principles that the BSA has carried forward.
4. Vivek Sood and Pavan Duggal – Works on Indian Cyber Law. These works discuss the Information Technology Act, 2000, cyber offences and the evidentiary treatment of electronic records in India. They are relevant for the interaction between the IT Act, the Evidence Act and the criminal law.

Journal and Research Literature

1. Research on Electronic Evidence in India. Articles on section 65B of the Evidence Act examine the debate between the strict and relaxed views of the certificate requirement and the difficulty of obtaining certificates from third-party platforms. This literature is relevant to the central question of admissibility.
2. Research on Image-Based Sexual Abuse. Scholarship by Clare McGlynn, Erika Rackley and others examines the creation and distribution of intimate images without consent and the harm caused to victims. It is relevant because such material often forms both the offence and the evidence in the same case.

3. Research on Victim Participation and Secondary Victimisation. Studies of criminal procedure in sexual offences examine how intrusive questioning, repeated statements and public hearings affect survivors. They support the study's attention to in-camera trial and audio-video recording.

Legal Literature and Judicial Decisions

1. Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020). These decisions settled that a certificate is a condition for admitting secondary electronic evidence under section 65B of the Evidence Act. They are the foundation of the present discussion, although neither case concerned a sexual offence.
2. State of Punjab v. Gurmit Singh (1996) and Sakshi v. Union of India (2004). These decisions emphasise sensitivity in the trial of sexual offences and permit procedures such as in-camera hearings and screens. They are relevant to the manner in which digital evidence is presented in court.

The literature reviewed provides a sound basis for understanding the technical, evidentiary and gender-related aspects of the subject. However, the application of the new statutes to digital evidence in sexual offence cases requires continuing examination.

Note: Before submitting the research paper, verify the exact titles, publication details and editions of the books and articles used in the final bibliography. The above review identifies relevant literature areas; it should not be treated as a complete verified bibliography.

1.4 Research Gap

Existing literature has examined electronic evidence in general, the certificate requirement under section 65B, cybercrime and the treatment of sexual offence survivors in criminal trials. Most of it treats these topics separately. Writing on electronic evidence is largely concerned with commercial, corruption or terrorism cases, while writing on sexual offences tends to concentrate on testimony, medical evidence and consent.

There is limited analysis of how the admissibility rules operate in sexual offence cases, where the material is intimate, the survivor is the principal witness, the offender may control the device and the stakes for dignity are high. The shift from the Evidence Act to the BSA, and from the Code of Criminal Procedure to the BNSS, has also not yet been examined fully in this context.

Questions such as the effect of a missing certificate on survivor-recorded chats, the use of recordings of victim statements as evidence, the handling of intimate images in court and the role of platforms in preserving data require combined analysis. The present study seeks to address this gap by examining the substantive law of admissibility together with investigative procedure and survivor protection.

1.5 Research Objectives

The main objectives of the study are:

1. To examine the meaning, forms and evidentiary significance of digital evidence in sexual offences.
2. To analyse the principles of relevance, authenticity and fair trial that govern the admission of electronic records.
3. To examine the constitutional provisions, the BSA, the BNSS, the BNS, the Information Technology Act and other laws applicable to digital evidence in sexual offence cases.
4. To identify the legal, technological and practical challenges in collecting, preserving and proving digital evidence and in protecting the survivor during trial.
5. To suggest legal, institutional and technological measures for strengthening the reliable and sensitive use of digital evidence in sexual offence prosecutions.

1.6 Research Questions

The study seeks to answer the following questions:

1. What is digital evidence, and what role does it play in the investigation and trial of sexual offences?
2. What conditions govern the admissibility of electronic and digital records under the BSA, and how do they differ from the earlier law?
3. What procedural safeguards under the BNSS and related laws apply to the collection and recording of digital evidence in sexual offences?
4. What challenges arise in authenticating digital evidence, protecting the survivor's privacy and ensuring a fair trial for the accused?
5. What reforms may improve the admissibility and reliable use of digital evidence in sexual offence cases?

1.7 Research Methodology

The present study follows the doctrinal method of legal research. It involves systematic analysis of existing legal materials to determine the law on a subject. The method is suitable because the study examines how statutory provisions and judicial decisions apply to digital evidence in sexual offence cases.

The primary sources include the Constitution of India, the Bharatiya Sakshya Adhiniyam, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and decisions of the Supreme Court and High Courts.

The secondary sources include textbooks, commentaries, journal articles, reports of the Law Commission and the National Crime Records Bureau, and international instruments. The research is analytical and does not claim to be based on an empirical survey or interviews.

1.8 Limitations of the Study

The study has certain limitations:

1. It concentrates on Indian law and refers to foreign and international materials only for comparison.
2. It focuses on digital evidence in sexual offences and does not examine every category of cybercrime or every form of electronic proof.
3. The BSA, the BNSS and the BNS are recent enactments, and judicial interpretation of several provisions is still developing. Section numbers and case law should be verified against the latest official texts.
4. It is a doctrinal study and does not represent the personal experiences of all survivors or the practices of every police station and court.
5. Forensic tools and technologies change rapidly, and technical statements in the study may require updating.
6. The study does not suggest that any particular item of digital evidence must be accepted or rejected; admissibility and weight depend on the facts of each case.

1.9 Scheme of the Study

The present study is organised into seven chapters.

Chapter I – Introduction explains the background and significance of the study and includes the review of literature, research gap, objectives, questions, methodology, limitations and scheme.

Chapter II – Digital Evidence and Sexual Offences explains the meaning, concept and evolution of digital evidence, its main forms and its relationship with the dignity of survivors.

Chapter III – Principles of Evidence Law and Fair Trial discusses relevance, admissibility, authenticity, integrity and the rights of the accused and the survivor.

Chapter IV – Legal Framework for Digital Evidence in India examines the Constitution, the BSA, the BNSS, the BNS, the POCSO Act, the IT Act, the intermediary rules, the data protection framework and international instruments.

Chapter V – Forms of Digital Evidence and Modes of Proof examines CCTV, mobile data, recordings, intimate material, forensic imaging and the technological challenges of proof.

Chapter VI – Analysis and Legal Challenges critically analyses certification, survivor protection, rights of the accused, investigation, platform accountability and legal gaps.

Chapter VII – Findings, Suggestions and Conclusion presents the findings, recommendations and conclusion.

CHAPTER – II
DIGITAL EVIDENCE AND SEXUAL OFFENCES

2.1 Digital Evidence

Digital evidence is information stored or transmitted in electronic form that may be used to prove or disprove a fact in issue. It includes text messages, emails, social media content, photographs, videos, audio recordings, call records, location data, browser histories, files stored on computers and cloud accounts, and footage from surveillance systems.

In sexual offence cases digital evidence can serve several purposes. It may show contact between the parties, establish identity, fix time and place, reveal threats or coercion, demonstrate the sequence of events and corroborate or contradict testimony. Because it is generated automatically and contemporaneously, it is often regarded as more objective than recollection. That perception must, however, be tested, since electronic records can be altered and their meaning depends on context.

Digital evidence differs from physical evidence in important ways. It is intangible, easily duplicated, dependent on devices and software, and capable of being changed without visible trace. The same file may exist in several places, including the device, a backup and a server. These features explain why the law prescribes special conditions for proving electronic records and why investigative handling is as important as the content itself.

2.2 Meaning and Concept of Digital Evidence

Under the BSA, the term "evidence" includes statements made electronically before the court and documents, including electronic or digital records, produced for inspection of the court. The term "document" has also been defined to include electronic and digital records. [4] The Adhiniyam provides that an electronic or digital record shall not be denied admissibility merely because it is in electronic form, and that such a record has the same legal effect, validity and enforceability as other documents.[5]

Two ideas should be distinguished. The first is admissibility, which asks whether the court may receive the material at all. The second is probative value or weight, which asks how much reliance may be placed on it once received. A record may be admissible and yet carry little weight if its source is doubtful or its context incomplete.

In sexual offence cases it is also useful to distinguish digital evidence that records the offence itself, such as a video made by the offender, from digital evidence that is circumstantial, such as location data or messages before and after the incident. The first category raises acute issues of dignity and handling, while the second typically raises issues of authentication and inference.

[4]Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(d) and s. 2(1)(e).
[5]Bharatiya Sakshya Adhiniyam, 2023, s. 61.

2.3 Evolution of Digital Evidence Law in India

Early Indian evidence law did not contemplate electronic records. Courts initially admitted tape recordings as documents, subject to conditions of relevance, identification of voice and absence of tampering.[6] The Information Technology Act, 2000 introduced sections 65A and 65B into the Evidence Act, providing that the contents of electronic records may be proved in accordance with section 65B.

In State (NCT of Delhi) v. Navjot Sandhu, the Supreme Court held that secondary evidence of electronic records could be given without a certificate under section 65B.[7] That position was overruled in Anvar P.V. v. P.K. Basheer, which held that section 65B is a complete code and that a certificate is mandatory for secondary electronic evidence.[8] Shafhi Mohammad v. State of H.P. later relaxed the requirement where the party was not in possession of the device,[9] but Arjun Panditrao Khotkar restored the strict view while recognising that courts may direct production of the certificate in appropriate cases.

With effect from 1 July 2024 the BSA has replaced the Evidence Act. Sections 61 to 63 now govern electronic and digital records, and a standard-form certificate in a Schedule has been introduced. The BNSS has also expanded the use of electronic communication, audio-video recording and electronic trial. This evolution shows a movement from reluctant acceptance of electronic evidence towards structured and technology-friendly procedure.

2.4 Digital Evidence and the Survivor's Dignity

The Supreme Court has recognised that rape is not merely a physical assault but a violation of the right to life and dignity under Article 21.[10] The use of digital evidence must be consistent with that principle.

Digital evidence can protect dignity by reducing dependence on the survivor's repeated narration. A recorded statement, preserved chat or surveillance footage may spare her from reliving events in detail. At the same time, digital evidence can harm dignity where intimate images are circulated among investigators, reproduced in court files or discussed in open court. A survivor who hands over her phone may also expose unrelated private information, including contacts, photographs and financial data.

The right to privacy recognised in Justice K.S. Puttaswamy v. Union of India requires that any interference with privacy be lawful, necessary and proportionate.[11] Applied to digital evidence, this means that extraction should be limited to what is relevant and that access to the extracted material should be restricted.

---

[6]R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471; Ram Singh v. Col. Ram Singh, 1985 Supp SCC 611.
[7]State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
[8]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[9]Shafhi Mohammad v. State of H.P., (2018) 2 SCC 801. [10]Bodhisattwa Gautam v. Subhra Chakraborty, (1996) 1 SCC 490. [11]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

2.5 Principal Forms of Digital Evidence in Sexual Offence Cases

The principal forms of digital evidence encountered in practice may be grouped as follows:

1. Communications: text messages, chat applications, emails, voice notes and social media messages showing contact, consent, inducement or threats.
2. Audio-visual recordings: videos or photographs made by the offender or by a witness, and recordings of the survivor's statement under investigative procedure.
3. Surveillance records: CCTV footage from public places, hotels, buildings, vehicles and transport systems.
4. Telecommunication and location data: call detail records, cell tower locations, GPS logs and internet protocol addresses.
5. Device and account data: files, deleted data recovered by forensic tools, browsing history, cloud backups and application logs.
6. Transaction records: payment records, booking confirmations and digital identity documents that fix time, place or presence.

CHAPTER – III
PRINCIPLES OF EVIDENCE LAW AND FAIR TRIAL

3.1 Meaning of Admissibility

Admissibility is the legal permission for a court to take a fact or document into account. Evidence is admissible only if it is relevant and is not excluded by a rule of law. Relevance concerns the logical connection between the evidence and a fact in issue, while admissibility concerns compliance with the form and manner of proof prescribed by law.

In relation to digital evidence, the Evidence Act and now the BSA add a further layer. The content of an electronic record must be proved in the manner prescribed in section 63 of the BSA, unless the original device is itself produced as primary evidence. A digital record that is relevant may thus remain inadmissible if the prescribed conditions are not satisfied. Courts have also held that an objection to the absence of a certificate must be taken at the time the document is tendered, and that it cannot ordinarily be raised for the first time at a later stage.[12]

3.2 Development of the Principles

The English common law developed the best evidence rule, which required the production of the original document. Indian law adopted a similar structure through the distinction between primary and secondary evidence. Electronic records challenge this distinction because a copy and an original may be indistinguishable. The BSA responds by treating each electronic record stored in multiple files or storage spaces as primary evidence in certain circumstances.[13]

[12]Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570.
[13]Bharatiya Sakshya Adhiniyam, 2023, s. 57, Explanations.

Judicial attention then shifted to authenticity and integrity. Courts increasingly ask who created the record, with what device, how it was stored, whether it was altered and who had custody. These questions are at the heart of digital forensic practice and are reflected in international standards for the identification, collection and preservation of digital evidence.[14]

3.3 Core Principles

3.3.1 Relevance

Digital evidence must relate to a fact in issue or a relevant fact. In sexual offence cases, the central issues usually include identity, occurrence of the act, absence of consent and, where the victim is a child, age. A private chat that has no bearing on these issues does not become admissible merely because it is available, and its production may unnecessarily intrude upon privacy.

3.3.2 Authenticity

Authenticity means that the record is what it is claimed to be. For electronic records, authenticity is addressed through the certificate, expert opinion, oral testimony of the person who created or recovered the record, and circumstantial indicators such as metadata. The court is concerned with whether the source device, the process of extraction and the integrity of the copy are reliable.

3.3.3 Integrity and Chain of Custody

Integrity requires that the record has not changed between its creation and its production. The chain of custody documents who handled the device or data, when and for what purpose. Hash values, which are mathematical fingerprints of data, are commonly used to show that a forensic copy is identical to the original. Gaps in the chain do not automatically render evidence inadmissible, but they may weaken its weight.

3.3.4 Fair Trial and the Rights of the Accused

The accused is entitled to a fair trial under Article 21. This includes access to the material relied upon against him, the opportunity to challenge its authenticity and, where appropriate, to seek an independent forensic examination. Article 20(3) protects against compulsion to be a witness against oneself, and the extent to which an accused may be compelled to unlock a device or give biometric access has been considered by courts.[15]

3.3.5 Burden and Standard of Proof

The prosecution must prove guilt beyond reasonable doubt, and this burden does not change merely because the evidence is electronic. Digital evidence is evaluated like other evidence: the court asks whether it is genuine, whether it is relevant and whether, taken with the rest of the record, it establishes the charge. A single chat or video seldom proves an offence by itself, and

[14]ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence.
[15]State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808; see also Virendra Khanna v. State of Karnataka (Karnataka High Court, 2021).

courts look for corroboration through testimony, medical findings and surrounding circumstances.

3.3.6 Survivor-Centred Procedure

The law of sexual offences recognises that survivors should be protected from avoidable trauma. This is expressed in in-camera trial, restrictions on disclosing identity, limits on questions regarding past sexual history, and recording of statements by women officers. These principles apply equally to the handling of digital evidence.

3.4 Critique of the Present Approach

The certificate-based approach has been criticised for formalism. Ordinary survivors, who may rely on chats or recordings on their own devices, may not understand the need for a certificate, and the formal requirement can defeat the use of reliable material. Third-party platforms, from which certificates are sought, may not cooperate quickly. The courts have attempted to mitigate hardship by allowing production of the certificate at a later stage in appropriate cases, but the process remains uncertain.

At the same time, relaxation of authentication standards creates risk, since fabricated chats and edited videos can be produced easily. The challenge is to maintain reliability without placing a disproportionate burden on survivors.

3.5 Evidence Law and Gender Justice

Gender justice in evidence law requires that rules should not operate on stereotypes. The Supreme Court has held that the testimony of a prosecutrix, if found reliable, can sustain a conviction without corroboration, and that she should be treated with the care due to an injured witness.[16]

3.6 Evidence Law and the Dignity of the Survivor

Dignity requires that the survivor is treated as a participant in the process and not merely as a source of evidence. The Supreme Court has directed measures such as screens, video links and sensitive questioning, particularly for child victims.[17]

CHAPTER – IV
LEGAL FRAMEWORK FOR DIGITAL EVIDENCE IN INDIA

4.1 Constitution of India

The Constitution does not mention digital evidence, but its fundamental rights shape the manner in which such evidence may be collected and used. Articles 14, 20(3) and 21 are particularly relevant, since they concern equality, protection against self-incrimination and the right to life, liberty, privacy and dignity.

[16]State of Punjab v. Gurmit Singh, (1996) 2 SCC 384; Bharwada Bhoginbhai Hirjibhai v. State of Gujarat, (1983) 3 SCC 217.
[17]Sakshi v. Union of India, (2004) 5 SCC 518.

4.1.1 Article 14 – Right to Equality

Article 14 requires equal protection of the laws. In the present context, a complaint of a sexual offence should not be treated less seriously because the proof is digital, and survivors from different social and economic backgrounds should be able to preserve and produce electronic material with equal effectiveness. Registration of the first information report is mandatory when a cognizable offence is disclosed, and electronic information of a sexual offence cannot be refused on the ground that it is not in written form.[18]

4.1.2 Article 20(3) – Protection against Self-Incrimination

Article 20(3) provides that no person accused of an offence shall be compelled to be a witness against himself. The Supreme Court has distinguished testimonial compulsion from the giving of physical specimens such as fingerprints and handwriting. Directions to give voice samples have been upheld by the Supreme Court,[19] but compelling disclosure of passwords raises more difficult questions because it may involve knowledge in the mind of the accused. The law in this area remains unsettled, and decisions of High Courts have attempted to prescribe safeguards.

4.1.3 Article 21 – Life, Personal Liberty, Privacy and Dignity

Article 21 protects the dignity and privacy of both the survivor and the accused. Puttaswamy recognised informational privacy as a part of the right, and requires that any restriction satisfy legality, legitimate aim and proportionality. Search of a mobile phone or cloud account can reveal extensive personal information, and the principle of proportionality therefore requires that extraction be targeted and that unrelated personal data be protected.

4.2 Bharatiya Sakshya Adhiniyam, 2023

The BSA is the central statute governing admissibility. It does not create a separate regime for sexual offences, but its general provisions on electronic records apply to all proceedings.

4.2.1 Definitions and Primary Evidence

Electronic and digital records are included in the definitions of “document” and “evidence”. The Adhiniyam also treats an electronic record as primary evidence in specified circumstances, for example where it is stored in several files or storage spaces simultaneously. This responds to the practical reality that a single video or chat may exist in a device, a backup and a server.

4.2.2 Sections 61 to 63 – Admissibility of Electronic Records

Section 61 declares that electronic records shall not be denied admissibility merely on the ground that they are electronic. Section 62 provides that the contents of electronic records may be proved in accordance with section 63. Section 63 deems information in an electronic record to be a document, admissible without production of the original, if the prescribed conditions are met, and requires a certificate in the form set out in the Schedule.[20]

[18] Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1.
[19] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
[20] Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63 and the Schedule.

The new certificate has two parts. Part A is to be signed by the person in charge of the device or the party producing the record, and Part B by an expert. The Schedule also calls for the hash value of the record. The requirement of an expert and a hash value is stricter than the former section 65B(4), under which a certificate by a person in a responsible official position sufficed. Whether and how the stricter form will apply to individual survivors who produce records from their own phones is an issue on which judicial guidance is awaited.

4.2.3 Expert Opinion and Examiner of Electronic Evidence

The BSA recognises the opinion of experts on matters of science and technology, and section 79A of the Information Technology Act authorises the Central Government to notify Examiners of Electronic Evidence. Expert evidence is often needed to explain forensic imaging, recovery of deleted data, authenticity of audio and video and the reliability of cell tower records. The court is not bound by expert opinion and evaluates it with other evidence.

4.2.4 Presumptions and Provisions Specific to Sexual Offences

The BSA contains presumptions regarding electronic records and secure digital signatures, but a presumption of authenticity does not ordinarily extend to the truth of the content. In prosecutions for certain rape offences, the BSA also carries forward the presumption of absence of consent where sexual intercourse is proved and the woman states in evidence that she did not consent. The earlier restrictions on evidence of the survivor's character or previous sexual experience, formerly in sections 53A and 146 of the Evidence Act, are also retained in the corresponding provisions. These rules prevent chats or images relating to a survivor's past conduct from being used to cast aspersions unless the law permits.

4.2.5 Judicial Interpretation of the Certificate Requirement

The courts have interpreted the certificate requirement in three stages. In the first, Navjot Sandhu treated section 65B as one route among several. In the second, Anvar held that the section is a special provision which overrides the general rules on secondary evidence, so that a certificate is indispensable. In the third, after the divergent approach in Shafhi Mohammad, the three-judge bench in Arjun Panditrao Khotkar clarified that the certificate is not required when the original device is itself produced and proved by its owner, but is required for copies, printouts and data from servers or networks. The Court also observed that Tomaso Bruno, which had suggested a wider rule, could not be treated as good law on this point.[21] Since section 63 of the BSA is modelled on section 65B, these decisions will continue to guide courts, subject to the changes made by the Schedule.

4.3 Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS governs investigation, inquiry and trial and replaces the Code of Criminal Procedure, 1973. It has several provisions that affect digital evidence.

[21]Tomaso Bruno v. State of U.P., (2015) 7 SCC 178; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

4.3.1 Registration and Recording of Information

Information of a cognizable offence may be given electronically, and the BNSS permits electronic FIR subject to signature within the prescribed time. In cases of sexual offences, information is to be recorded by a woman police officer. The BNSS further provides that the statement of the victim of rape shall be recorded through audio-video electronic means, preferably by mobile phone.[22] Such recordings may later be produced as evidence, and they reduce disputes about what the survivor said.

4.3.2 Search, Seizure and Production of Digital Material

Section 94 allows a court or police officer to summon production of a document or other thing, and the provision expressly extends to electronic communication, including communication devices likely to contain digital evidence. Section 105 requires the process of search and seizure to be recorded through audio-video electronic means, and the recording is to be forwarded to a Magistrate without delay.[23] These provisions help establish the chain of custody for devices seized from the accused or the survivor.

4.3.3 Forensic Investigation and Statements before the Magistrate

For offences punishable with imprisonment of seven years or more, section 176(3) requires the visit of a forensic expert to the scene to collect evidence and requires the process to be videographed.[24] Section 183 provides for recording of the statement of the survivor before a Magistrate, which may also be done by audio-video means. Section 184 relates to medical examination of the survivor of rape. Together, these provisions create documentary and electronic records that reinforce, and may corroborate, the survivor's account.

4.3.4 Electronic Trial and In-Camera Proceedings

Section 530 allows trials, inquiries and proceedings to be held in electronic mode, including the examination of witnesses through audio-video means. The Supreme Court had earlier held that video-conference examination satisfies the requirement of presence.[25] Trial of rape cases is to be conducted in camera, and publication of proceedings without the permission of the court is restricted.

4.4 Bharatiya Nyaya Sanhita, 2023 and the POCSO Act, 2012

4.4.1 Sexual Offences under the BNS

Rape is defined in section 63 and punished in section 64 of the BNS, with aggravated forms in sections 65 to 71. Sexual harassment, including showing pornography against the will of a woman, is addressed in section 75, voyeurism in section 77 and stalking, including monitoring of electronic communication, in section 78. Section 72 prohibits disclosure of the identity of the victim of certain sexual offences, and section 73 restricts printing or publishing court proceedings without permission.

[22]Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 173 and 176.
[23]Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 94 and 105.
[24]Bharatiya Nagarik Suraksha Sanhita, 2023, s. 176(3).
[25]State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601.

Digital evidence may also relate to connected offences such as criminal intimidation, extortion and forgery of electronic records, and to section 238, which penalises causing disappearance of evidence. Deletion of chats or destruction of a device by the accused after the offence may therefore be a separate offence and may support an inference regarding guilt.

4.4.2 Protection of Children from Sexual Offences Act, 2012

The POCSO Act contains specific provisions on child sexual abuse material, including use of a child for pornographic purposes and storage of such material. It allows the statement of the child to be recorded by audio-video means and permits examination through video links, and it requires trial in camera. Presumptions under the Act place a reversed burden on the accused in prescribed circumstances. Digital evidence of age, such as school records stored electronically, and digital evidence of abuse, such as recordings, are frequently decisive in POCSO cases.

4.5 Information Technology Act, 2000 and Intermediary Rules

The IT Act punishes violation of privacy by capturing or publishing images of a private area without consent (section 66E), publication of obscene and sexually explicit material (sections 67 and 67A) and child sexual abuse material (section 67B). Section 65 penalises tampering with computer source documents. These provisions may run along with offences under the BNS.

Section 79 gives intermediaries conditional immunity, and the Supreme Court in Shreya Singhal read it to mean that actual knowledge requires a court order or government notification.[26] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require intermediaries to act on complaints regarding content that exposes a person's private area or shows nudity or a sexual act, including impersonation and morphed images, within a short prescribed time. Significant social media intermediaries providing messaging services must enable identification of the first originator for specified serious offences, a requirement that has been challenged on privacy grounds. For evidence, an important issue is that removal of content should not result in loss of the data needed for prosecution, and platforms should preserve records on lawful request.

4.6 Digital Personal Data Protection Framework

The Digital Personal Data Protection Act, 2023 regulates processing of digital personal data. It exempts, to the extent specified, processing by the State for the prevention, detection, investigation or prosecution of offences. This ensures that data protection law does not hinder legitimate criminal investigation, although the exemption must itself operate within constitutional limits of necessity and proportionality. The Act, with its Rules, is being brought into force in phases, and the applicable provisions must be checked according to commencement dates.

[26]Shreya Singhal v. Union of India, (2015) 5 SCC 1.

4.7 International and Comparative Framework

4.7.1 Budapest Convention on Cybercrime, 2001

The Convention of the Council of Europe provides for expedited preservation of stored computer data, production orders, search and seizure of computer data and mutual assistance. India is not a party to the Convention, but its procedural principles, especially rapid preservation, are useful for obtaining data held by foreign platforms. Mutual legal assistance remains the principal route for cross-border data, and it is often slow.

4.7.2 CEDAW and Comparative Approaches

General Recommendation No. 35 of the CEDAW Committee recognises that gender-based violence occurs in technology-mediated environments and calls for effective remedies and protection.[27] In comparative practice, the United States Federal Rules of Evidence permit authentication of electronic records through certification of a qualified person, and the English approach generally treats the reliability of computer evidence as a question of weight unless a challenge is raised. These approaches show that authenticity can be assured without making a single formal certificate the only route.

CHAPTER – V
FORMS OF DIGITAL EVIDENCE AND MODES OF PROOF

5.1 Electronic Records and Modes of Proof

An electronic record may be proved in two principal ways. The first is production of the original device, such as the phone on which the video was recorded, which is then treated as primary evidence and examined by the court. The second is production of a copy, printout or extraction, whose contents must be proved by the certificate and conditions in section 63 of the BSA.[28]

In practice, most digital evidence in sexual offence cases reaches the court as secondary evidence, since devices are usually returned or must be retained in a police malkhana, and since cloud or platform data cannot be physically produced. The certificate therefore assumes great importance. The Supreme Court in Arjun Panditrao Khotkar has held that the certificate is a pre-condition to secondary electronic evidence, although a court may direct a party to produce it when the party has applied for it and the person concerned is unwilling or unable to give it.

Oral evidence also remains important. A survivor or witness who personally saw or created a chat, photograph or recording can speak to its contents, and the maker of the video can authenticate it. The Supreme Court held in Sudhir Chaudhary v. State (NCT of Delhi) that video recordings that are edited or not accompanied by proper proof cannot be relied upon.[29]

[27]CEDAW Committee, General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19 (2017).
[28]Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[29]Sudhir Chaudhary v. State (NCT of Delhi), (2016) 8 SCC 307.

The table below summarises the main differences between the former and present certificate provisions.

Aspect	Section 65B, Evidence Act, 1872	Section 63, BSA, 2023
Scope	Computer output printed, stored, recorded or copied on optical or magnetic media	Extends to communication devices and semiconductor memory, in addition to optical or magnetic media
Certificate	Signed by a person in a responsible official position	Standard Schedule form, Part A by the person in charge and Part B by an expert
Hash value	Not expressly required	Hash value of the record to be stated in the certificate
Effect	Mandatory for secondary electronic evidence (Anvar; Arjun Panditrao)	Retained as condition for admissibility; judicial guidance on new form awaited

5.2 CCTV and Surveillance Footage

CCTV footage can fix the presence of the accused and survivor at a place, show their movements and demonstrate the time sequence. It may also contradict a false claim. In Mohd. Ajmal Amir Kasab v. State of Maharashtra the Supreme Court relied on CCTV footage together with other evidence.[30] Practical problems include overwriting of footage after a short period, system clocks that are inaccurate, incomplete exports and the absence of a person able to give the certificate. Early written notice to the owner to preserve footage is therefore essential.

5.3 Mobile Phone, Messaging and Location Data

Chats, call records and location data are often central. Call detail records are held by telecom operators and are proved through certificates from their officers. The Supreme Court held in Sonu @ Amar v. State of Haryana that objection to a missing certificate must be raised at the time of exhibiting the record.

Messaging applications raise special issues. Content is often encrypted end to end, and servers may not hold it. The principal source is therefore the device, and forensic extraction is needed for deleted messages. The evidence should show the account holder's identity, since a number or handle may not identify a person. Evidence of identity includes registration records, linked devices, voice or photographs and admissions.

5.4 Audio-Video Recordings and Voice Evidence

Recordings of conversations, including telephonic conversations, are admissible subject to relevance, proof of the speaker's voice, absence of tampering and, for secondary copies, the certificate.[31] Voice identification may require expert comparison of samples, and the Supreme Court has allowed Magistrates to direct an accused to give voice samples. In sexual offence cases, recordings of the survivor's statement under the BNSS have special reliability because they are made by the investigating agency in a prescribed manner.

[30]Mohd. Ajmal Amir Kasab v. State of Maharashtra, (2012) 9 SCC 1.
[31]R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.

Recordings made secretly by a survivor, for example of a threat or confession, are likely to be relevant. A court will ordinarily admit relevant evidence even if it was obtained improperly, but the circumstances of recording may affect weight.

5.5 Intimate Images and Videos as Evidence

Where the offence consists of recording or circulating intimate material, as in voyeurism, blackmail or non-consensual intimate imagery, the material is both the subject of the offence and its evidence. It must be preserved, but its circulation must be minimised. Best practice is to retain it in sealed form, to provide limited access to those who need it, to avoid reproduction in open court and to describe it in the record without unnecessary detail. Child sexual abuse material must never be copied or circulated outside lawful forensic channels.

Survivors need advice not to forward intimate material to others, including to friends, because doing so may complicate proof and cause further harm. Hash-based tools, such as StopNCII.org, allow the survivor to create a digital fingerprint of the image so that participating platforms can detect and block it without the image being uploaded.

5.6 Forensic Imaging, Hash Values and Chain of Custody

Forensic imaging creates a bit-for-bit copy of a device or storage medium, which is verified through a hash value. Analysis is conducted on the copy, so that the original remains unchanged. The report should record the tools used, the examiner's qualifications, the date and place of examination and the findings.

Chain of custody should show the seizure of the device, its sealing, storage, transfer and examination. The audio-video recording of seizure under the BNSS contributes to this. Failure to seal a phone or to isolate it from networks may allow remote deletion or modification, which gives the defence ground to question the integrity of the data.

5.7 Technological Challenges

Several technological developments complicate proof. Encryption and secure applications may prevent extraction. Cloud storage places data in other jurisdictions. Anti-forensic tools allow deletion or alteration of metadata. Self-deleting messages leave little trace unless captured early. AI-generated or manipulated content can make it harder to trust any image or video, and creates a risk that genuine evidence will be dismissed as fabricated, as well as a risk that fabricated material will be accepted.

Detection tools are not infallible, and an expert opinion may be needed on both sides. The law should therefore insist on provenance and corroboration rather than on visual inspection.

5.8 Impact on Prosecution and Survivors

Well-preserved digital evidence can strengthen a prosecution by corroborating testimony, rebutting false defences and reducing delay. Poorly handled evidence may cause acquittals on technical grounds or may leave the survivor's account unsupported. Survivors also bear

emotional burden when asked to produce, explain or watch intimate material. A survivor-centred approach requires that the benefits of digital evidence are obtained with minimum exposure.

5.9 Summary of Evidence Types and Proof Issues

The following table summarises the main categories of digital evidence in sexual offence cases, their usual sources and the principal issue that arises in proving each.

Type of evidence	**Usual source**	**Principal proof issue**
Chats and emails	Survivor's or accused's device; service provider	Identity of sender, completeness, certificate
Photographs and videos	Device of offender or survivor; social media	Origin, editing, manipulation, handling of intimate content
CCTV footage	Owner of premises or system	Overwriting, clock accuracy, export method
Call records and location data	Telecom operator	Certificate from operator, accuracy of tower data
Forensic extraction report	Forensic laboratory or expert	Chain of custody, hash value, expert competence
Recorded statement of survivor	Police or Magistrate under BNSS	Compliance with procedure, secure storage

An illustration shows how these elements work together. Suppose a survivor reports that she was threatened with release of an intimate video after an assault. The investigator preserves her phone and the threatening messages, records the survivor's statement through audio-video means, issues preservation notices to the platform and telecom operator, and seizes the accused's phone with video recording of the seizure. A forensic examiner then images both devices and records hash values. At trial, each item is proved through the survivor's testimony, the certificate under section 63 and the examiner's evidence. If any link is missing, the defence may challenge the evidence, and the court will consider whether the remaining material is sufficient.

CHAPTER – VI
ANALYSIS AND LEGAL CHALLENGES

6.1 Survivor-Centred Analysis of Digital Evidence

A survivor-centred analysis asks not only whether evidence is admissible but also how its collection and use affect the person who has suffered the offence. The survivor is often the first custodian of the digital evidence. She may hold the chats, receive the threats and have the only copy of an incriminating recording. The law places upon her a burden of preservation that she is rarely trained to discharge.

The analysis also recognises that digital evidence may reveal aspects of her life unrelated to the offence. Defence lawyers may use messages or photographs to suggest consent or bad character. The law restricts such use, but enforcement depends on the vigilance of the court.

6.2 Certificate Requirement and Formalism

The strict certificate requirement protects against fabrication, but it may be applied mechanically. A survivor's chat history may be rejected because she did not obtain a certificate, although she herself can testify to it and there is no suggestion of tampering. The new requirement of an expert's signature and of hash values may add cost and delay, particularly for survivors in smaller towns.

It is suggested that courts should treat the certificate as a means of establishing reliability and not as an end in itself. Where the maker of the record is examined and cross-examined, the court should consider whether the purpose of the certificate has been fulfilled, while remaining consistent with the binding decision in Arjun Panditrao Khotkar. Legislative or rule-based clarification would assist.

The practical effect can be illustrated by delay. Where a certificate has to be obtained from a platform based abroad, months may pass, during which the trial cannot proceed on that evidence. Courts have the power to summon the certificate or direct the concerned person to produce it, but this depends on timely applications and on the cooperation of the person who controls the data. A standard protocol for requesting certificates from major platforms would shorten this process.

6.3 Privacy, Dignity and Secondary Victimisation

Extraction of data from a survivor's phone may reveal her entire digital life. Police practice sometimes involves seizing the phone for long periods without limiting the examination. Such practice is difficult to reconcile with the proportionality standard in Puttaswamy. Courts should require that the scope of extraction is defined, that unrelated material is not examined or disclosed, and that devices are returned promptly after imaging.

Secondary victimisation may also occur through the public display of material in open court, through leak of recordings to the media and through unsympathetic questioning about digital history. In-camera hearings, sealed exhibits and strict compliance with sections 72 and 73 of the BNS are essential. The Supreme Court has emphasised non-disclosure of the identity of victims in Nipun Saxena v. Union of India.[32]

6.4 Rights of the Accused and Fair Trial

The accused is entitled to defend himself, and digital evidence relied upon by the prosecution must be capable of testing. He should receive copies of the forensic images and reports, and should be able to request an independent examination. Fabrication of digital evidence by

[32]Nipun Saxena v. Union of India, (2019) 2 SCC 703.

persons in dispute is possible, and false allegations supported by manipulated material, though rare, cannot be excluded.

The balance between his rights and the survivor's privacy may be maintained through protective orders. Counsel and experts may be permitted to examine sensitive material under supervision, without general release. This respects fair trial without exposing the survivor.

Two types of scenario show the tension. In the first, a survivor's chats with the accused before the incident are produced by the defence to suggest a relationship. The court must decide whether they are relevant to consent, and must apply the statutory limits on evidence of past sexual conduct. In the second, the survivor produces chats that contain threats by the accused. Here the prosecution must prove the identity of the sender and the integrity of the messages. The same rules of authenticity apply in both, but the protections of dignity apply mainly to the survivor.

6.5 Gender Bias in Digital Evidence Practice

Bias may enter through expectations that a survivor should have immediately preserved evidence, that her failure to report promptly or her digital communications with the accused imply consent, or that a 'perfect' victim would not have a digital history. Such assumptions are inconsistent with the law, which treats consent as a matter of free and voluntary agreement and not as an inference from earlier contact. Judges, prosecutors and police need training to avoid stereotyping when interpreting digital material.

6.6 Adequacy of Existing Legal Remedies

The BSA, the BNSS and the BNS together provide a modern framework, with electronic recording, forensic visits and electronic trial. However, several provisions, such as the forensic visit under section 176(3), depend on the notification of facilities by State Governments and on the availability of forensic personnel. The framework has also been in operation for a short period, and its practical effect will depend on implementation. The existence of rules does not guarantee that recordings are made, preserved and produced in compliance with law.

6.7 Challenges in Investigation and Digital Evidence

Investigators face limited forensic laboratories, backlog in examination and shortage of trained personnel. Police stations often lack equipment for imaging phones. Evidence may be lost because of delay in sending requests to platforms, which keep data only for limited periods. Foreign platforms may respond slowly or require mutual legal assistance.

Another challenge is attribution, that is, connecting an account, number or device with a particular person. Shared devices, borrowed SIM cards and virtual private networks complicate attribution.

Training is a continuing need. Digital forensic examiners must explain their findings in language that judges and lawyers can follow, and judges should be able to evaluate reports critically. Standard formats for forensic reports, with clear statements of methods and

limitations, would help courts to assess weight and would reduce disputes over technical terminology.

6.8 Intermediary and Platform Accountability

Platforms hold much of the relevant evidence, including account records, access logs and uploaded content. They also control the circulation of intimate material. Accountability requires prompt response to takedown requests, and equal readiness to preserve data before removal. Uniform preservation timelines, designated nodal officers and secure channels for law enforcement requests would help. Any increased access to private communications, however, must be balanced against privacy safeguards.

6.9 Identification of Legal Gaps

The study identifies the following gaps. First, there is no sexual-offence-specific protocol for the handling of digital evidence. Second, judicial interpretation of the new Schedule certificate is awaited, and survivors may be burdened by its requirements. Third, standards for compelled access to devices are unsettled. Fourth, rules for protecting intimate material in court records are not uniform. Fifth, forensic capacity and training remain inadequate. Sixth, the legal position regarding preservation of data by platforms and cross-border access needs clarification.

CHAPTER – VII
FINDINGS, SUGGESTIONS AND CONCLUSION

7.1 Major Findings of the Study

The study finds that digital evidence has become indispensable in the investigation and trial of sexual offences, as it can identify the accused, fix time and place, corroborate the survivor and show conduct before and after the offence. It also finds that admissibility depends on compliance with section 63 of the BSA and its certificate requirement, and that failure to comply may exclude otherwise reliable material.

7.2 Findings Relating to the Survivor's Dignity

The study finds that digital evidence can either protect or harm dignity depending on how it is handled. Unnecessary extraction, circulation and public display of intimate material cause secondary victimisation.

7.3 Findings Relating to Principles of Evidence and Fair Trial

The principles of relevance, authenticity, integrity and fair trial are generally sufficient to deal with digital evidence, but their application requires technical knowledge. The certificate is an important safeguard but should not become a purely formal barrier. The accused's rights, including access to material and independent examination, should be preserved through protective measures.

7.4 Findings Relating to the Indian Legal Framework

The Indian legal framework contains a modern set of provisions in the BSA, the BNSS, the BNS, the POCSO Act and the IT Act. However, there is uncertainty about the Schedule certificate, compelled access to devices, platform preservation and cross-border data.

7.5 Suggestions and Recommendations

The following measures may improve the use of digital evidence in sexual offence cases:

1. Standard protocol: Issue a uniform protocol for collection, imaging, sealing and storage of digital evidence in sexual offence cases, based on recognised standards.
2. Clarification of certificate: Clarify through rules or judicial guidance how the Schedule certificate applies to survivors producing their own records, and permit later production of the certificate where the record is otherwise reliable.
3. Forensic capacity: Establish forensic facilities in every district, train police officers, and provide mobile forensic units.
4. Early preservation: Require preservation notices to platforms, telecom operators and owners of CCTV systems within a fixed time of the complaint.
5. Protection of intimate material: Introduce rules for sealed storage, limited access and non-reproduction of intimate material in court records.
6. Proportionate extraction: Limit device examination to relevant data, and provide for return of devices after imaging.
7. Training and sensitisation: Train judges, prosecutors and police on digital evidence and on gender-sensitive handling.
8. Platform cooperation: Require nodal officers, secure channels and preservation timelines, with safeguards for privacy.
9. Survivor guidance: Provide simple guidance to survivors on preserving chats, screenshots and recordings, and on the dangers of deletion and circulation.

7.6 Answers to the Research Questions

Digital evidence consists of electronic information that can prove or disprove facts, and in sexual offences it serves to identify, locate, corroborate and contextualise. Under the BSA, electronic records are admissible on the same footing as other documents, subject to the conditions of section 63 and the Schedule certificate. The BNSS adds safeguards in recording, search and trial. The principal challenges are authentication, forensic capacity, privacy and fair trial. Reforms in protocols, capacity building, clarification of the certificate and survivor protection can address them.

WHITE BLACK LEGAL

7.7 Conclusion

Digital evidence has become a central feature of the prosecution of sexual offences. It allows courts to look beyond contested oral accounts to contemporaneous records, and it can corroborate survivors who would otherwise have only their word to rely on. At the same time, it is vulnerable to alteration, misunderstanding and misuse. The law of admissibility seeks to ensure that only reliable material is accepted, and the Bharatiya Sakshya Adhiniyam, 2023 continues this effort through sections 61 to 63 and the Schedule certificate.

The study shows that admissibility cannot be treated only as a technical matter. In sexual offence cases the evidence often contains intimate details of a person who has already suffered harm, and the method of collecting and presenting it can add to that harm. The principles of dignity and privacy under Article 21 require that digital evidence be collected proportionately, stored securely, and displayed with care. The rights of the accused to a fair trial and to challenge the evidence are equally important, and can be protected through disclosure, independent examination and protective orders.

The new procedural law gives investigators and courts valuable tools, including audio-video recording of statements and of seizure, forensic visits and electronic trial. Their effect will depend on implementation, which in turn depends on training, infrastructure and institutional commitment. Uncertainty regarding the new certificate, compelled access to devices and platform obligations needs to be resolved through guidance and reform.

In conclusion, a balanced approach is required. The law must insist on authenticity and integrity, without placing impossible formal burdens on survivors. It must protect the accused from fabricated or unreliable material, without exposing survivors to unnecessary intrusion. The value of technology in securing justice will be realised only when it is accompanied by sensitivity, accountability and respect for human dignity.

7.8 Scope for Future Research

Future research may examine judicial interpretation of section 63 of the BSA and the Schedule certificate, empirical studies of forensic delay and outcomes in sexual offence trials, the use of AI-generated and manipulated material as evidence, and comparative approaches to protecting intimate material in court records. Studies of survivors' experiences in providing digital evidence would also be valuable.

8. REFERENCES

A. Cases

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 — section 65B certificate mandatory for secondary electronic evidence.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 — certificate is a pre-condition; courts may direct its production.

3. Shafhi Mohammad v. State of H.P., (2018) 2 SCC 801 — relaxation where the party does not possess the device (overruled in Arjun Panditrao).
4. State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 — earlier view on electronic evidence (overruled in Anvar).
5. Tomaso Bruno v. State of U.P., (2015) 7 SCC 178 — electronic evidence and CCTV footage in criminal trial.
6. Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570 — timing of objection to missing certificate.
7. Sudhir Chaudhary v. State (NCT of Delhi), (2016) 8 SCC 307 — proof of video recordings and edited footage.
8. State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601 — video-conference evidence as presence.
9. Sakshi v. Union of India, (2004) 5 SCC 518 — sensitive procedure in child sexual abuse trials.
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 — privacy, dignity and proportionality.
11. Shreya Singhal v. Union of India, (2015) 5 SCC 1 — intermediary liability and section 79.
12. State of Punjab v. Gurmit Singh, (1996) 2 SCC 384 — sensitivity in rape trials and in-camera hearing.
13. Bharwada Bhoginbhai Hirjibhai v. State of Gujarat, (1983) 3 SCC 217 — corroboration of the prosecutrix's testimony.
14. Ram Singh v. Col. Ram Singh, 1985 Supp SCC 611 — conditions for admissibility of tape-recorded statements.
15. R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471 — tape-recorded conversations as evidence.
16. State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808 — self-incrimination and compelled specimens.
17. Ritesh Sinha v. State of U.P., (2019) 8 SCC 1 — voice samples of the accused.
18. Nipun Saxena v. Union of India, (2019) 2 SCC 703 — non-disclosure of the identity of victims.
19. Mohd. Ajmal Amir Kasab v. State of Maharashtra, (2012) 9 SCC 1 — reliance on CCTV and electronic records.

20. Bodhisattwa Gautam v. Subhra Chakraborty, (1996) 1 SCC 490 — rape as a violation of Article 21.

21. Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1 — mandatory registration of FIR.

These cases provide relevant legal principles, but none should be represented as a direct ruling on every aspect of digital evidence in sexual offences unless the judgment specifically addresses the point.

B. Statutes and Legal Instruments

- Constitution of India, arts. 14, 20(3) and 21.
- Bharatiya Sakshya Adhiniyam, 2023, ss. 2(1)(d), 2(1)(e), 57, 61, 62, 63 and the Schedule.
- Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 94, 105, 173, 176, 183, 184 and 530.
- Bharatiya Nyaya Sanhita, 2023, ss. 63 to 73, 75, 77, 78 and 238.
- Protection of Children from Sexual Offences Act, 2012.
- Information Technology Act, 2000, ss. 65, 66E, 67, 67A, 67B, 79 and 79A.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.
- Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025.
- Council of Europe Convention on Cybercrime (Budapest Convention), 2001.
- CEDAW Committee, General Recommendation No. 35 (2017).
- ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition and preservation of digital evidence.

For statutes and rules, use the official text and check amendments, section numbers and commencement dates before describing a provision as currently operative.

C. Books and Articles

- Eoghan Casey, Digital Evidence and Computer Crime (Academic Press).
- Stephen Mason and Daniel Seng (eds.), Electronic Evidence (Institute of Advanced Legal Studies).
- Ratanlal and Dhirajlal, The Law of Evidence; Sarkar, Law of Evidence; Batuk Lal, The Law of Evidence.
- Vivek Sood, Cyber Law Simplified; Pavan Duggal, Cyber Law: The Indian Perspective.
- Clare McGlynn and Erika Rackley, “Image-Based Sexual Abuse” (2017) 37 Oxford Journal of Legal Studies 534.