

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

# **DIGITAL EVIDENCE AND ITS ADMISSIBILITY IN INDIAN COURTS**

AUTHORED BY - SHRUTI CHAUDHARY

## **I. Introduction**

The fast pace of digitisation in communication, business, and governance has made digital evidence increasingly important in India's legal system. Materials such as CCTV footage, call records, WhatsApp messages, and documents stored on the cloud are now often crucial in both civil and criminal cases. As a result, courts have had to establish clear rules for admitting this kind of evidence, ensuring its reliability while also addressing concerns about possible tampering or misuse.

In India, that framework is primarily grounded in sections 65A and 65B of the Indian Evidence Act, 1872 (as amended by the Information Technology Act, 2000), and has now been re-codified, without changing the basic philosophy, under the Bharatiya Sakshya Adhiniyam, 2023 (BSA). Landmark decisions such as *State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru*<sup>1</sup>, *Anvar P.V. v. P.K. Basheer*<sup>2</sup>, and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*<sup>3</sup>, have progressively clarified the conditions under which electronic records may be admitted in evidence.

## **II. Concept and Forms of Digital Evidence**

In Indian law, the term "electronic record" is preferred over "digital evidence." Under the Information Technology Act, 2000<sup>4</sup>, an electronic record includes any data, record, image, or sound that is created, stored, received, or transmitted in electronic form, as well as information held in microfilm or computer-generated microfiche. For evidentiary purposes, such records are regarded as "documents," which brings them within the framework governing primary and secondary evidence.

In practical terms, digital evidence includes a wide range of materials, such as emails and electronic files like Word documents, PDFs, spreadsheets, and presentations. It also covers

---

<sup>1</sup> State (N.C.T. of Delhi) v. Navjot Sandhu alias Afsan Guru AIR 2005 SC 3820

<sup>2</sup> Anvar P.V v. P.K. Basheer & Ors (2014) 10 SCC 473

<sup>3</sup> Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1

<sup>4</sup> Section 2(1)(t) of the Information Technology Act, 2000

SMS and instant messaging records (including WhatsApp chats), along with content shared on social media platforms. Other examples are call detail records and location data, CCTV footage, and audio or video recordings saved on DVRs, servers, or portable storage devices. Additionally, it extends to server logs, cloud-stored backups, GPS data, and information generated by IoT devices.

Although these types of evidence differ in their technical nature, the core legal issue remains the same: the court must determine the circumstances under which such material can be considered reliable, authentic, and free from tampering when establishing the facts of a case.<sup>5</sup>

### **III. Statutory Framework: IT Act and Evidence Act**

The Information Technology Act, 2000 was introduced to give legal recognition to electronic transactions and digital signatures, while also updating existing laws, including the Evidence Act. Section 4 of the Act specifically acknowledges electronic records, stating that if the law requires information to be in writing or printed form, that requirement is met as long as the information is available electronically and can be accessed for future reference.

To incorporate electronic records into the law of evidence, Sections 65A and 65B were added to the Evidence Act and later re-codified in the BSA as well. Section 62 of BSA makes it clear that electronic records must be proved in the manner laid down in 63 of BSA, thereby creating a distinct framework for such evidence. At the same time, the traditional rules relating to primary and secondary evidence still apply to non-electronic documents, maintaining the overall structure of the Act.

### **IV. Sections 65A–65B: The Special Code for Electronic Records**

Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) states that information contained in an electronic record, when printed on paper or stored, recorded, or copied onto optical or magnetic media produced by a computer, will be treated as a “document,” provided the requirements set out in Section 63(4)(c) are met. These requirements generally include the following:

1. The computer was routinely used to store or process information during the relevant time period.
2. The data was entered into the computer in the normal course of activities.

---

<sup>5</sup> Consultation Paper on Documentary and Electronic Evidence, Third Programme of Law Reform 2008-2014, Project 7, Law Reform Commission, Ireland, December 2009, available at <http://www.lawreform.ie/fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf>

3. The computer was functioning properly, or any malfunction did not impact the accuracy of the record.
4. The output is based on information derived from the regular use of the computer.

When these conditions are satisfied, the “computer output”, such as a printout, CD, DVD, or pen drive, is regarded as a document and can be admitted as evidence of the contents of the original electronic record, as long as the certification requirement under Section 63(4)(c) is also complied with<sup>6</sup>. In this way, Section 62 directs that electronic records must be proved through this specific mechanism, rather than relying on the general rules governing secondary evidence.

### **V. The Section 63(4) Certificate: Nature, Purpose and Content**

Section 63(4) mandates a written certificate signed by a person holding a responsible official position. This certificate must identify the electronic record, explain how it was produced, provide details of the device used, and confirm that the requirements under Section 63(4) have been fulfilled. Its purpose is to establish the authenticity of the computer output, without the need to present the entire computer system before the court.<sup>7</sup>

Courts have repeatedly held that this certificate is a mandatory requirement for admitting secondary electronic evidence, rather than just a procedural formality. It performs three main functions:

- i. It places responsibility on a particular individual who is acquainted with the device or system in question.
- ii. It gives the court confidence that the material produced is an accurate reproduction of the original data.
- iii. By requiring details about the source and method of extraction, it helps reduce concerns about possible tampering.

The key controversy in the case law has been how strictly this requirement must be applied and whether it can be relaxed in somewhat difficult and complex cases.

### **VI. Judicial Evolution: From *Navjot Sandhu* to *Anvar***

Early case law displayed a relatively flexible attitude. In *State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru*<sup>8</sup>, the Supreme Court accepted call detail records and other electronic evidence even without a certificate under Section 65B (4) of the Indian Evidence Act (IEA). Instead, it

---

<sup>6</sup> Section 65A, the Information Technology Act, 2000

<sup>7</sup> The Bharatiya Sakshya Adhinyam, 2023 (BSA)

<sup>8</sup> *State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru* (2005) 11 SCC 600

relied on the general rules governing secondary evidence under Sections 63 to 65. In doing so, the Court permitted officials to establish the authenticity of such records through oral testimony, effectively indicating that Sections 65A and 65B of IEA were not the only means for proving electronic evidence.

This approach created uncertainty about whether the special statutory safeguards for electronic evidence were mandatory or merely recommendatory. The issue resurfaced in *Anvar P.V. v. P.K. Basheer*<sup>9</sup>, where a three-judge bench revisited the interpretation of sections 65A–65B of IEA in an election-law context.

### **VII. *Anvar P.V. v. P.K. Basheer*: A Watershed**

In *Anvar P.V. v. P.K. Basheer*, the Court clarified that Sections 65A and 65B of IEA constitute a complete and self-contained framework for determining the admissibility of electronic records, thereby excluding reliance on the general rules of secondary evidence. It held that secondary electronic materials such as CDs, VCDs, and chips, can be admitted only when the requirements of Section 65B (2) are fulfilled and the evidence is supported by a certificate under Section 65B (4).

The Court further emphasized that oral testimony or any alternative method cannot replace this mandatory certificate. It also stated that, to the extent the decision in *Navjot Sandhu case* allowed electronic evidence to be admitted without complying with Section 65B, it did not represent the correct legal position.

Thus, *Anvar PV case* marked a decisive shift towards strict procedural compliance. It reinforced the idea that the special provisions on electronic records override general secondary-evidence rules under the principle *generalia specialibus non derogant*.

### **VIII. The *Shafhi Mohammad* Interlude and Doctrinal Confusion**

The strict approach adopted in the *Anvar case* quickly led to practical difficulties, especially in situations where a party had no access to or control over the device or server from which the electronic record needed to be produced. In *Shafhi Mohammad v. State of Himachal Pradesh*<sup>10</sup>, a two-judge SC bench held that the requirement of a certificate under Section 65B (4) is procedural in nature and may be dispensed with in situations where the party relying on the electronic record is unable to obtain access to the device from which it was generated.

---

<sup>9</sup> *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473

<sup>10</sup> *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 2 SCC 801

The *Shafhi Mohammad* decision held that Sections 65A and 65B do not constitute an exhaustive code, and that electronic evidence may still be admitted through alternative methods when strict compliance is not feasible. Although this approach eased the burden on litigants who had to rely on third-party systems such as telecom databases or CCTV networks, it stood in clear conflict with the firm position laid down in the *Anvar case*.

This inconsistency in judicial interpretation led to the matter being referred to a larger bench to determine whether the certificate required under Section 65B (4) is in fact compulsory, and, if it is, the specific situations in which it must be produced.

### **IX. Arjun Panditrao Khotkar: Definitive Restatement**

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*<sup>11</sup>, a three-judge bench clarified and consolidated the law. The Court held that:

1. *Anvar P.V. v. P.K. Basheer* correctly states the law; sections 65A–65B are a complete code for admissibility of electronic records.
2. A certificate under section 65B (4) is a condition precedent for the admissibility of secondary electronic evidence (CDs, pen-drives, chips, etc.).
3. *Shafhi Mohammad* case and certain other decisions relaxing this requirement do not lay down the law correctly and stand overruled to that extent.

At the same time, the *Arjun Panditrao* case clarified that when the original electronic device is brought before the court and is capable of direct examination, the material amounts to primary evidence and therefore does not require a Section 65B certificate. The Court further observed that the law does not fix a strict timeline for filing the certificate, and it may be allowed even at a later stage, including during appeal, so long as it does not cause any prejudice to the opposing party.

### **X. Primary vs Secondary Electronic Evidence**

A significant conceptual clarification made in the *Arjun Panditrao* case is the clear distinction between primary and secondary forms of electronic evidence. It held that when the original storage device such as a DVR, hard disk, or mobile phone, is presented in court and its contents are directly accessed or played, the information is to be regarded as primary evidence under the standard rules applicable to documents.

In practice, courts are usually presented with copies rather than original electronic devices,

---

<sup>11</sup> *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1

such as printed emails, CDs with extracted CCTV footage, chat screenshots, or pen drives containing duplicated files. These materials are treated as “computer outputs” and fall under secondary evidence, which can be admitted only if the requirements of Section 65B (2) are met along with a valid certificate under Section 65B (4).<sup>12</sup> For legal practitioners, correctly identifying whether electronic material is primary or secondary evidence is the first and most important step in determining how to establish its admissibility.

## **XI. Relevance, Authenticity and the “Best Evidence” Principle**

Compliance with Sections 65A and 65B of IEA and Sections 62, 63 of BSA, is required, but it alone does not ensure admissibility; the electronic record must also be shown to be relevant and genuine. Courts have consistently warned that digital evidence can be easily altered, duplicated, or fabricated, and therefore its reliability must be proven through both technical safeguards and proper procedural verification.

The “best evidence” rule<sup>13</sup>, along with the court’s authority to draw adverse inferences under Section 119(1)(g) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), is significant in this context. In various rulings, courts have observed that failure to produce available CCTV footage, often considered the most reliable form of evidence, without explanation may lead to an adverse inference against the party withholding it, especially in criminal and bail matters. Accordingly, although Section 65B governs the formal admissibility of electronic records, the evidentiary value attached to such material largely depends on whether the most complete version has been produced and whether any omissions have been properly justified.

## **XII. Chain of Custody and Hash Values**

Modern digital forensics places strong importance on preserving an unbroken chain of custody and confirming the integrity of electronic data through cryptographic hash values like SHA-256. The chain of custody is a documented record that tracks every individual or authority that has handled the device or copied data, from the time it is seized through its storage, examination, and eventual presentation before the court.<sup>14</sup>

Hash values function like unique digital identifiers, in that even a minor change in the contents of a file or storage device will produce a completely different hash output. In recent cases and academic discussions, concerns have been raised about investigative shortcomings where hash

---

<sup>12</sup> The Indian Evidence Act, 1872

<sup>13</sup> Sections 60-64, the Bharatiya Sakshya Adhiniyam, 2023 (BSA)

<sup>14</sup> <https://supremetoday.ai/issue/hash-value-memory-card-evidence-admissibility>

values of devices such as memory cards were not recorded at the time of seizure, or where later verification showed that the device had been accessed or modified on multiple occasions. Best practice therefore requires:

- Imaging devices using forensic tools.
- Computing and recording hash values at seizure and whenever copies are made.
- Presenting hash reports and chain-of-custody documentation to demonstrate that the record produced in court is identical to what was originally seized.

These practices, while not originally spelt out in the Evidence Act, are increasingly being read into the requirements of authenticity and proper custody.

### **XIII. Category-Specific Issues: CCTV, CDRs and Social-Media Evidence**

Although the legal requirements remain the same across the board, different types of digital evidence present their own specific difficulties.

#### **(a) CCTV Footage**

Courts often treat CCTV recordings as strong circumstantial evidence, especially in criminal cases. However, their admissibility depends on proving a clear and uninterrupted chain from the point of recording to their extraction and presentation in court. This includes the original DVR or camera system, the process used to copy the footage onto devices like CDs or pen drives, and the required Section 65B certificate. If available footage is not produced, or only edited portions are submitted, courts may draw an adverse inference under Section 119(1)(g) of the BSA.

#### **(b) Call Detail Records (CDRs)**

CDRs are typically issued by telecom service providers and must be supported by a Section 65B certificate from an authorised official. Disputes often arise regarding the completeness of the records, the accuracy of location data, and whether the certificate properly explains the system used to generate them. Courts have, in many cases, relied on CDRs to either support or challenge claims such as alibis, making careful scrutiny of their reliability essential.<sup>15</sup>

#### **(c) Emails, Chats and Social Media**

Printed copies or screenshots of emails, messaging app conversations, and social media posts are classic examples of secondary electronic evidence. Courts approach such

---

<sup>15</sup> <https://ijlr.iledu.in/anvar-p-v-v-p-k-basheer-ors-2014-10-scc-473-section-65a-and-65b-admissibility-of-electronic-records-of-indian-evidence-act-1872/>

material with caution due to its ease of manipulation or fabrication. As a result, admissibility depends not only on proper certification under Section 65B but also on supporting evidence such as server logs, seizure of original devices, or acknowledgements from the alleged creator.

#### **XIV. Criminal Procedure, Forensic Protocols and Digital Evidence**

While the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 does not have a dedicated, single chapter titled "Digital Evidence, but its provisions on search, seizure and production of documents<sup>16</sup>, are routinely invoked to secure electronic records and devices. These statutory rules are further supported by forensic standards and court-issued guidelines that set out the proper methods for seizing, imaging, and preserving digital evidence.

Standard protocols now recommend that investigating officers:

- Seize devices lawfully and document them in detail.
- Create bit-by-bit forensic images rather than working on the original media.
- Compute and record hash values for devices and extracted files.
- Maintain strict access control and detailed logs of every instance of handling.

Failure to follow these procedures does not necessarily make the evidence inadmissible, but it can greatly reduce the evidentiary value the court assigns to it and create stronger grounds for the defence to contest its reliability.<sup>17</sup>

#### **XV. Emerging Regime under the Bharatiya Sakshya Adhinyam, 2023**

The Bharatiya Sakshya Adhinyam, 2023 seeks to modernise and reorganise the law of evidence, including the provisions on documentary and electronic evidence. Section 2 explicitly includes electronic records within the definition of "document," listing emails, text messages, CCTV footage, CDRs, cloud data, server logs and social-media content.

Section 57<sup>18</sup> treats electronic records as documentary evidence on the same footing as traditional paper documents, and when read along with Section 61, it reinforces the requirement that secondary electronic evidence must be supported by a certificate issued by a responsible official. This certificate should identify the relevant device, explain how the record was produced, and confirm the integrity of the system. In this way, Section 61 reflects the principles

---

<sup>16</sup> Sec 96, 97, 103, 105, 185 etc. of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)

<sup>17</sup> <https://www.freelaw.in/legalarticles/Forensic-and-Electronic-Evidence-2025-Chain-of-Custody-DNA-and-Admissibility>

<sup>18</sup> Sec 57 of the Bharatiya Sakshya Adhinyam, 2023 (BSA)

developed under Sections 65A and 65B. At the same time, Section 62 introduces limited flexibility, where securing such a certificate is not reasonably possible, such as in cases involving foreign-based platforms or non-cooperative service providers.<sup>19</sup>

Section 63(4) along with the accompanying Schedule lays down the prescribed form of the certificate and specifically requires the inclusion of hash values. This gives statutory backing to forensic integrity verification methods that had earlier evolved through judicial decisions and investigative practice. In this way, the BSA not only carries forward the principles of Section 65B but also refines them, placing stronger emphasis on proper custody of electronic records and well-documented proof of their integrity.<sup>20</sup>

## **XVI. Practical Implications for Investigators and Prosecutors**

For investigating authorities, the legal framework on digital evidence imposes strict procedural duties in practice. Officers are required to locate relevant electronic sources at the earliest opportunity, seize devices in accordance with law, and promptly generate and record hash values to preserve data integrity. Every subsequent step in handling the material must also be carefully documented. In addition, they must obtain Section 65B-type certificates from telecom companies, internal technical personnel, or system custodians when retrieving data such as call records, server logs, or CCTV footage.

Failure to present the most reliable available digital evidence, for example, known CCTV footage, may lead courts to draw adverse inferences and can influence decisions even at the bail stage. On the other hand, prosecutors are expected to foresee potential challenges to admissibility and should be ready to support their case with expert evidence explaining hash values, system records, and forensic procedures to prove authenticity.<sup>21</sup>

## **XVII. Practical Implications for Defence and Civil Litigants**

For defence lawyers, a clear understanding of the rules on admissibility offers important grounds to question prosecution evidence. They may examine whether a valid Section 63 certificate has been produced, whether it is signed by a person holding a responsible official position, whether the requirements under Section 63 (4) of BSA are actually satisfied, and whether the chain of custody and hash records genuinely establish the integrity of the electronic material.

---

<sup>19</sup> Bharatiya Sakshya Adhiniyam, 2023 (BSA)

<sup>20</sup> <https://elplaw.in/leadership/bhartiya-sakshya-adhiniyam-2023-a-dynamic-shift-to-the-digital-era/>

<sup>21</sup> <https://www.tclindia.in/cctv-footages-are-material-piece-of-evidence/>

Where there are deficiencies such as missing hash values, unexplained access to devices, or incomplete submission of CCTV footage or chat records, counsel may request that the evidence be excluded or argue that it should carry limited evidentiary value. In civil cases as well, parties relying on emails, digital contracts, or other electronic communications must take proactive steps, including preserving server logs, obtaining certificates from IT personnel or service providers, and ensuring that the copies submitted in court can be clearly linked to their original sources.<sup>22</sup>

### **XVIII. Comparative and Policy Perspectives**

India follows a special statutory framework for electronic evidence, built around Section 63(4) of the BSA. This approach differs from that of some other common law countries. In the United Kingdom, for instance, early law provided specific rules for computer-generated evidence, but over time these were integrated into the general evidentiary regime, with greater emphasis placed on the evidentiary value of the material rather than on strict admissibility requirements.<sup>23</sup> India's decision to maintain a stricter standard for admissibility is driven by concerns over the risk of tampering and the uneven ability of investigative agencies to manage digital forensic processes. From a policy perspective, however, this strict approach also creates a conflict: while it helps prevent the use of manipulated evidence, it can disadvantage genuine litigants who rely on data held by foreign entities or uncooperative service providers, particularly in the context of cloud services and cross-border digital platforms. The limited flexibility introduced in the BSA's certification requirements partly seeks to address this challenge.

### **XIX. Conclusion**

Digital evidence is now an indispensable component of fact-finding in Indian courts. The combined effect of sections 65A–65B of the IEA, their judicial interpretation in *Anvar* and *Arjun Panditrao*, and the statutory re-articulation under the Bharatiya Sakshya Adhinyam, 2023, is a framework that treats electronic records as fully admissible but subject to strict safeguards on authenticity and integrity.

In the future, the success of this legal framework is likely to depend more on how effectively investigators, lawyers, and judges adopt established best practices rather than on further changes in legal doctrine. This includes maintaining a strict chain of custody, verifying hash

<sup>22</sup> <https://corporate.cyrilamarchandblogs.com/2020/07/section-65b-of-the-indian-evidence-act-1872-requirements-for-admissibility-of-electronic-evidence-revisited-by-the-supreme-court/>

<sup>23</sup> <https://www.rostrumlegal.com/threshold-admissibility-of-electronic-evidence-anvar-and-thereafter/>

values, obtaining certifications in a timely manner, and carefully understanding the advantages and limitations of various types of digital evidence. If implemented properly, this approach would enable Indian courts to make full use of digital evidence while still ensuring fairness and reliability in adjudication.

