Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023:

Sanjay Rambhau Salkute

B.Sc.; LL.M.; M.B.A.; D.C.S.A.
Retired District Judge, Pune (Maharashtra), India

Abstract:

This (Part IV) conclusion paper, explains that Section 63 of the Bharatiya Sakshya Adhiniyam [BSA] does not apply to quasi-judicial proceedings such as tribunals, domestic inquiries, or arbitration. Therefore, before such forums, the focus shifts to the four essential substantive qualities of electronic evidence: authenticity, integrity, reliability, and accuracy. In practice, parties often produce electronic records without disclosing a secure hash value. It is studied that, the absence of a hash value does not automatically make the record inadmissible, but the integrity must be proved by other reliable means. Even before tribunals, when device is produced or electronic record is produced, the opposing party must be given a fair opportunity to test the electronic evidence, such as through cross-examination, access for forensic examination, or by filing an independent expert opinion. This discussion is intended as a preliminary study for law students and in continuation to the concept explained in Part I, that, ‘ the certificate under Section 63(4) is not mandatory where the Evidence Act is not strictly applicable’. It also clarifies that the applicability of the BSA depends on the true legal character of the forum. The name of a body, such as a Family Court or Labour Court, is not decisive; the key question is whether it functions as a court in the strict legal sense or as a quasi-judicial authority. The illustrations are only explanatory and do not attempt a full technical treatment of forensic issues. This paper concludes the preliminary study series on the concept of the trial court as the guardian of electronic and digital records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023.

Keyword: Quasi-Judicial, Disciplinary enquiry, electronic record, digital device, electronic device, certificate under 63(4), tribunal electronic evidence, electronic record in arbitration.

1. Introductions:

In quasi-judicial proceedings, tribunals, the statement that the Evidence Act is “not strictly applicable” is meant to simplify the process is not strictly applicable, it does not mean that forum can ignore the search for truth. The relaxation relates only to technical and procedural rules, for example, strict formats of documents, the sequence of examining witnesses, or the rigid application of the hearsay rule. However, the decision must still rest on reliable and relevant material that has real probative value. The basic

principles of natural justice continue to apply. This means that a party must be given a fair chance to present its case, to challenge the evidence against it, and to cross-examine witnesses where necessary. The process may be less formal, but it must remain fair, rational, and based on credible evidence.

Union of India v. T.R. Varma [1], The Hon'ble Court identified four essential conditions that must be satisfied for an inquiry to be fair, even where the Evidence Act does not strictly apply. First, each party must be allowed to produce all relevant evidence in support of their case. Second, the evidence of the opposing side must be recorded in the presence of the person against whom it is used. Third, that person must be given a proper opportunity to cross-examine the opponent's witnesses. Fourth, no material should be relied upon against a party unless they are given a fair chance to explain it or produce rebuttal evidence. These requirements ensure that the inquiry remains just, transparent, and consistent with the principles of natural justice.

Common Misunderstanding:

A common misunderstanding is to treat the strictly non-application of the Evidence Act as a license to ignore basic fairness. This leads to incorrect practices, such as denying cross-examination on the ground that the Evidence Act does not apply, relying on untested hearsay or rumours, considering irrelevant materials, using secret evidence, or refusing to allow parties to present their case. The correct approach is different. The right to cross-examine is a core principle of natural justice and must be given where the evidence is adverse. Hearsay evidence can be considered, if it is logically relevant and only after assessing its reliability and weight. A photocopy of paper document can be relied; unless its original, preparation and authenticity are established by proper procedure. Therefore, decisions must be based on relevant material, and all evidence relied upon must be disclosed to the parties. Above all, each party must be given a fair opportunity to present evidence and respond to the case against them.

Bareilly Electricity v. Workmen [2] the Hon'ble Court held that, 'The application of the principle of natural justice does not imply that what is not evidence can be acted upon. On the other hand, what it means is that no material can be relied upon to establish a contested fact which are not spoken to by persons who are competent to speak about them and are subject to cross-examination by the party against whom they are sought to be used''.

Note: In reality, the extent of inapplicability of evidence Act varies depending on the enabling statute. Some tribunals are expressly excluded from the Evidence Act by their parent legislation, while others are only partly exempt. Ex**.** Section 19(1) of the Arbitration and Conciliation Act, 1996 explicitly states that an arbitral tribunal is not bound by the Indian Evidence Act, 1872, Ex. Section 14 of the Family Courts Act, 1984.

Note: In a civil court the standard is preponderance of probabilities, meaning the evidence must show that authenticity and integrity are more probable than not, and judicial scrutiny of the technical proof is rigorous and exacting. In a quasi-judicial proceeding the standard is preponderance of evidence on the record, meaning the finding must rest on some credible and reliable evidence that a reasonable person could act upon, but the forum retains flexibility in the method and degree of proof it demands. However, the substantive requirements of authenticity, integrity, reliability and accuracy remain non-negotiable and must be established through credible means before the electronic record can be safely relied upon.

The difference lies in the degree of scrutiny and the method of proof, not in the obligation to prove the substantive requirements at all.

Note: In State of U.P. v. Saroj Kumar Sinha, [6] the Hon'ble Supreme Court held that if material is relied upon without proof, or without giving the employee an opportunity to respond, the enquiry is vitiated as being contrary to principles of natural justice.

Applicability of Section 63 of BSA:

Section 1 of the BSA limits their application to "judicial proceedings before a court,". Therefore, the BSA is not applicable to quasi-judicial forums like tax authorities or all tribunals or arbitrator. The Hon'ble Madras High Court in the case of The Assistant Commissioner of Income Tax vs Vetrivel Minerals [3] pleased to held that,'' Section 65B of the Indian Evidence Act and Section 63 of the Bharatiya Sakshya Adhiniyam (BSA) do not apply to such quasi-judicial forums''.

Although above Vetrivel Minerals case arose in a tax context, its reasoning applies with equal force to quasi-judicial authority, because when tribunals themselves are not bound by the technical provisions of the law of evidence, it is too obvious that quasi-judicial authorities cannot also be bound.

As the Section 63 of the BSA is held not to be applicable to quasi-judicial forums (such as tax authorities, tribunals, or departmental enquiries), it does not mean that electronic record can be produced casually or accepted without scrutiny. It only means that the rigid, technical mode of proof prescribed by the statute is relaxed, not that proof itself is dispensed with.

In quasi-judicial proceedings, electronic evidence can be produced in any reasonable form, such as a CD, pen drive, hard disk, mobile phone, printout, transcript, or screenshot. The authority may accept the record, if it is placed on record openly and the opposite party is given access to it. However, simply producing electronic device or filing the electronic record is not sufficient; the party relying on it must still prove that it is trustworthy and relevant.

Since the technical rules are relaxed, proof is to be established by evidentiary discipline through substantive and credible material. This may include oral evidence from the person who created, recorded, seized, or extracted the data, or from the custodian who handled or stored it. The party should also explain the process, such as the device from which the data came, how it was copied or transferred, and whether it remained unchanged. Some form of chain-of-custody material should be shown, even if informal, such as seizure notes, office records, registers, or details of sealed storage. But, when the integrity of the record is disputed, the process becomes technically complex, or the opposing party raises a serious challenge, expert or technical evidence may be required.

The standard is not proof beyond reasonable doubt, but proof that reasonably inspires confidence. Therefore, when the party relying on electronic evidence must still prove the four basic substantive requirements. First, authenticity i.e. the record must be shown to be what it claims to be and to come from the stated source. Second, integrity i.e. there must be proof that the record has not been altered, manipulated, or tampered with. Third, reliability i.e. the method by which the record was created, recorded, or extracted must be shown to be dependable. Fourth, accuracy i.e. the contents must correctly

reflect the original information. These requirements are mandatory because they flow from the principles of natural justice, the requirement of fair play, and the rule that findings cannot be based on no evidence.

Even in quasi-Judicial proceedings, the opposite party must be given a fair chance to meet the electronic evidence. This includes access to the electronic record, the opportunity to cross-examine the relevant witnesses, and the right to raise objections or produce a contrary expert opinion. If such an opportunity is denied, the proceedings become unfair and may be set aside.

The authority still has a positive duty to examine the electronic evidence with care. It should record reasons for relying upon it. It must satisfy itself that the record appears trustworthy and reliable, and it should record reasons for relying upon it. The authority cannot accept or act upon electronic material blindly merely because it has been produced; it must first be satisfied about its credibility and fairness to both sides.

In quasi-judicial proceedings, physical devices that store or generate electronic records are often produced as evidence. These can include mobile handsets, pen drives, compact discs, hard drives, memory cards, laptops, computers, iPads, tablets, DVRs or NVRs, digital cameras, GPS devices, and smartwatches. The authority must ensure that the device was functioning properly at the relevant time and that the data extracted from it is genuine and untampered. Custodians or witnesses should explain how the device was used, how the data was stored, and how it was preserved until production. Experts may examine the device to verify technical reliability, confirm that the data has not been altered, and ensure that any extraction or copying methods are sound. The authority must be satisfied that the evidence is authentic, accurate, reliable, and intact before relying on it in the proceedings.

In quasi-judicial proceedings, different types of electronic records are produced depending on the forum and nature of the dispute:

Family Courts commonly deal with WhatsApp chats, SMS, call detail records (CDRs), emails, audio and video recordings, CCTV footage, digital photographs, social media posts, bank account statements, GPS locations, screen recordings, and records linked to Aadhar or PAN.

Labour or Industrial Tribunals often handle biometric attendance data, electronic salary slips, CCTV footage, emails, WhatsApp messages, payroll Excel sheets, ERP software records, audio/video recordings, bank statements, digital appointment letters, and electronic show-cause notices.

Disciplinary or Departmental Enquiries may involve pen drives with audio/video files, mobile handsets, emails, CCTV footage, WhatsApp chats, computer logs, digital photographs, biometric records, GPS tracking, CDs or DVDs, electronic financial transactions, and Aadhar/PAN-linked records.

Arbitration proceedings frequently see emails, electronic contracts, ERP records, WhatsApp messages, Excel sheets, digital photographs, CCTV footage, bank statements, digital invoices, GPS logs, audio/video recordings, work orders, and records of digital signatures.

In each case, the quasi-judicial authority must ensure the records are genuine, untampered, and properly linked to the person, device, or event they relate to, with custodians and experts confirming authenticity, integrity, reliability, and accuracy before the evidence can be relied upon.

Note: Points to check prima facie: Authenticity – Where did the file come from? Firstly, check the source of the file. The user can also open the file properties to see the author's name, last modified by, and date created. If the author's name does not match the claimed source, or the file was created much later than the event it refers to, it may not be genuine. **Integrity – Has the file been changed?** Check this by looking at the file's creation and modification dates. Normally, a file is created first and then modified later. In scanned documents or PDFs, visible signs such as sudden font changes, uneven lines, blurred areas, or misaligned text may suggest editing. In logs or lists, missing dates or sudden jumps in serial numbers may show that some entries were deleted or inserted. If the file shows signs of unnatural changes, its integrity is doubtful. **Reliability:** Was it made by a system or typed by a person? Check whether the record was automatically generated by a machine or manually typed by a person. It is also important to see whether the same information appears in other related records. **Accuracy:** Does the information make sense? Check whether the record shows something that could not have happened. If the facts in the document are impossible or clearly inconsistent with known events, the document cannot be considered accurate or trustworthy. **Additional Points to Consider: Chain of Custody:** Document the complete path of the file from creation to presentation. Record who had access, when, and what actions were taken. Verify storage methods and backup procedures. Check for any gaps in custody that could allow tampering. **Technical Metadata Analysis:** Examine EXIF data, document properties, and hidden metadata. Check file signatures and hash values for integrity verification. Analyze embedded objects, hyperlinks, or references. Review version history and track changes (if available). **Cross-Reference Verification:** Compare with contemporaneous records from independent sources. Check against official databases or repositories. Verify with witnesses or parties who were present during document creation. Look for corroborating evidence in related systems or files. **Legal Admissibility Requirements:** Verify if proper foundation has been laid for admission. Check if opposing party has been given opportunity to examine. **Context and Circumstances:** Evaluate the business process or system that generated the document. Consider the purpose for which the document was originally created. Assess whether the document was created in the ordinary course of business. Review the technological environment and standard practices at time of creation.

Note: It is noticed that in some quasi-judicial proceedings the authority is an administrative or technical officer. Such officers may accept photocopies or electronic records without checking their authenticity. At times, CCTV footage, emails, or system logs are used without giving copies to the delinquent employee. In some cases, material evidence is disclosed too late. As a result, the opponent does not get a fair opportunity to examine or challenge that material. Malini Jain Versus Pankaj Bhutad and others[9], even in the trial where 65-B is applicable, due to this unexplained delay, lack of prior disclosure, and absence of voice identification, the court refused to accept the pen drive as evidence.

Admissible Compliance:

Admissible compliance requires the party producing an electronic record to satisfy the substantive requirements of proof. This means the party must establish the authenticity of the source, the integrity of the record, the reliability of the device or process, and the accuracy of the data. These elements may be proved through reliable methods such as oral testimony of relevant witnesses, expert forensic reports, chain-of-custody records, metadata analysis, or effective cross-examination that supports the credibility

of the evidence. The authority will then examine whether these substantive conditions are satisfied i.e. integrity and authenticity of the record are otherwise convincingly established.

Sr No	Substantive	Action
A	Device was functioning properly	Reliability must be shown in some manner
B	Information accurately reproduced	Accuracy must be proved
C	Record not tampered or altered	Integrity must be established
D	Source is authentic	Authenticity must be proved

Illustrations: -

[a] Device was functioning properly:

Example 1: Pen drive with audio files: The person who recorded the audio must testify that the recording device (mobile phone or recorder) was working properly at the time of recording.

Example 2: Photocopies of Excel sheets: The person who generated or maintained the Excel data must show that the computer system was functioning normally when the entries were made and when the sheets were printed.

[B] **Information accurately reproduced:**

Example 1: Pen drive with audio files: The person who transferred the audio to the pen drive must show that the file is an exact copy of the original recording. This may be done by stating that the file was directly copied without editing, and that it plays in the same form as the original recording.

Example 2: Photocopies of Excel sheets: The witness must prove that the printed or photocopied Excel sheets are exact reproductions of the original electronic data. This can be shown by testifying that the sheets were printed directly from the system without changes and that the figures match the original entries.

[C] Record not tampered or altered:

Example 1: Pen drive with audio files: The party must show that the audio recording was not edited, cut, or manipulated after it was made. This may be proved by the testimony of the person who recorded and preserved the file, a chain of custody showing who handled the pen drive, or a forensic report confirming that the file has not been altered.

Example 2: Photocopies of Excel sheets: The party must show that the electronic data in the Excel file was not changed before printing. This can be proved by testimony from the person maintaining the records, system logs, backup records, or expert analysis showing no alteration.

[D] Source is authentic:

Example 1: Pen drive with audio files: The party must prove who made the recording, on what device, and in what circumstances. For instance, the person who recorded the conversation may testify that they

personally made the recording on their phone at a particular time and later copied it to the pen drive including the voice sample verification.

Example 2: Photocopies of Excel sheets – The party must show where the Excel data originated, who entered the information, and in what system it was maintained. This may be proved by the employee or officer responsible for maintaining those records.

[E] Secure Hash Value:

Example 1: Pen drive with audio files: Where no secure hash value is produced, the party must still prove that the audio file is genuine and untampered. This may be done by calling the person who recorded the audio to testify about when, where, and how the recording was made and stored. The party may also produce a forensic expert who examines the audio file on the pen drive, generates its secure hash value, and confirms that the file shows no signs of editing or alteration. Chain of custody evidence, showing who handled the pen drive from the time of recording until production before authority, can further support its integrity.

Example 2: Photocopies of Excel sheets: Where no secure hash value is produced, the party must still prove that the data in the photocopies accurately reflects the original electronic records and has not been altered. This can be done by examining the person who maintained the Excel data and printed the sheets, who can testify that the printouts were taken directly from the system without changes. A forensic expert may also examine the original electronic file, generate a secure hash value, and confirm that the data is intact and consistent with system backups or logs.

Quasi-Judicial Authority- Pen drive with audio files: Examine the testimony of the person who recorded the audio, confirming that the device (mobile phone or recorder) was working properly and that the recording was made in the ordinary course without errors or malfunctions. The witness must also show that the file transferred to the pen drive is an exact copy of the original, and that it has not been edited, cut, or otherwise manipulated. Chain of custody evidence should be considered to track who handled the pen drive from recording to production. Expert testimony may be relied upon to verify the technical reliability of the device, the integrity of the audio file, and the absence of tampering, including forensic checks and hash values where available. The authority must satisfy itself that the recording is authentic (who recorded it and on what device), accurate (faithful reproduction of events), reliable (the device and process functioned properly), and intact (no alteration after creation). Even if a secure hash value is not produced, the substantive proof through witness testimony, forensic examination, and chain of custody must establish confidence in the record.

Quasi-Judicial Authority- Photocopies of Excel sheets: The authority must ensure that the printed or photocopied Excel sheets accurately reflect the original electronic data. The witness who generated or maintained the Excel file should explain that the computer system was functioning normally when the entries were made and when the sheets were printed, and that the printouts are exact reproductions of the original records. The authority should examine evidence that the electronic data was not tampered with before printing, including system logs, backup records, or forensic expert reports. Expert testimony may be considered to verify the integrity of the Excel file, confirm that the printed copies match the original entries, and explain the reliability of the system and printing process. The authority must satisfy itself that the record is authentic (source of data and responsible employee), accurate (figures and information

match the original), reliable (system and process worked correctly), and intact (no post-generation changes). In the absence of a secure hash value, testimony from the custodian and expert, along with corroborating records, should provide confidence in the integrity of the evidence.

Illustration: CDR (Call Detail Record) produced through Telecom Nodal Officer

What the Telecom Nodal Officer should prove: Telecom Nodal Officer must explain in simple terms how the record was created and why it can be trusted. The officer should state that the CDR was generated from the company's regular switching or billing system, which was functioning normally at the relevant time, and that such records are maintained in the ordinary course of business. The officer must confirm that the CDR is a true extract from the company's official servers, relating to the specific subscriber number and period in question, and that the data was taken directly from the secure system without any manual alteration. It should also be explained that the record was printed or transferred through the standard internal process and, after extraction, remained in official custody without being modified. Finally, the witness must identify himself as the authorised Nodal Officer and affirm that the data originates from the telecom company's official systems and accurately reflects the call events recorded there.

Expert To Prove: Expert should explain the reliability of the telecom system and the integrity of the data. The expert should state that the telecom network uses an automated process to log call details, and that this process is standard, dependable, and not dependent on manual input. The expert should confirm, after examining the electronic file or server extract, that there are no signs of tampering or manipulation. The metadata and system logs should be shown to be consistent with the call events mentioned in the record. The expert must also explain that the method used to extract the CDR is technically sound and follows accepted procedures. Finally, the expert should confirm that the produced record corresponds exactly with the data stored in the original telecom system.

Quasi-Judicial Officer: In quasi-judicial proceedings, the authority must ensure that electronic evidence, such as a CDR, is credible, reliable, and trustworthy. It cannot rely merely on the fact that the record is produced; it must satisfy the four core substantive requirements. Authenticity is established by confirming that the record originates from the claimed source, such as the telecom system or subscriber. Integrity is proved by showing that the record has not been altered, deleted, or tampered with after creation. Reliability requires verifying that the device, system, or process used to generate the record functioned normally and consistently. Accuracy is ensured by confirming that the record correctly reflects the events, transactions, or communications it claims to document. To satisfy these requirements, the authority examines the testimony of the custodian or officer who generated, extracted, or preserved the record, considers expert evidence about technical reliability and integrity, and reviews supporting records or corroborating material linking the evidence to the correct subscriber, device, or period. The opposing party must be given a fair opportunity to test the evidence, including cross-examination, filing contrary expert opinions, or inspecting the original device if feasible. The authority must act fairly, record reasons for admitting or rejecting evidence, and base findings on credible proof rather than assumptions. The substantive requirements of authenticity, integrity, reliability, and accuracy must always be met before the evidence can form the basis of a finding.

Note: If the charge refers to CDRs, it should be verified that the CDRs were issued by the authorised nodal officer. If other records, such as movement files or raw data, are produced, the legality of the source from which they were obtained must be checked. Since such data may differ when accessed from different locations or when reverified from a reliable source, there is a possibility of errors. Actual exclusive use of mobile handset at relevant time is also factor needs to be considered. Therefore, in all circumstances, the opponent should, as far as possible, be allowed to verify the supplied electronic record through his own expert to defend the case.

Note: CDRs mainly contain technical details such as the calling and called numbers, time of the call, duration, and the cell tower to which the phone was connected. This information as showing only an approximate location, not the exact position of the handset. CDR must be supported by subscriber records, lawful seizure of the handset or SIM, forensic linkage, witness testimony, or other independent proof. Cell towers are divided into sectors, and identifying the specific sector used by the phone can reduce the area of uncertainty. Handover patterns between towers may indicate movement during a call, helping to reconstruct a person's path. Technical parameters such as Timing Advance can estimate the distance between the handset and the tower within a limited radius. Internet Protocol Detail Records track data sessions and may provide more frequent location indications.

Note: Voice identification reliability depends on a proper chain of custody, clear recording quality, lawful collection of voice samples, and scientific comparison by a qualified expert. The speaker be properly identified, and the accuracy of the recording be proved by eliminating the possibility of tampering. An acoustic comparison, experts may also consider linguistic features such as dialect, speech habits, pronunciation patterns, and distinctive word usage, which can help in identifying the speaker. The conditions under which the voice sample is taken are also important, because stress, unwilling participation, or deliberate voice disguise can affect the reliability of the comparison. Experts must further account for environmental and technical factors, such as background noise or differences between recording devices, since these "channel effects" can distort the voice signal.

Illustration: Mobile phone handset produced

The witness or custodian to prove: The witness or custodian should explain that the mobile handset was in proper working condition at the relevant time and was regularly used for calls, messages, or recordings, without any known malfunction affecting the data. The witness should state that the messages, recordings, or other data shown from the handset are the same as originally stored, and that the display, extraction, or transcription was done correctly without any changes. It should also be explained that the handset remained in the custody of the concerned person or authority, that no editing, deletion, or insertion of data was done after the relevant events, and that the device was kept safely until it was produced. Finally, the witness should confirm that the handset belonged to or was used by the concerned person, that the phone number or user account is correctly identified, and that the data originated from that handset.

Expert: The technical or forensic expert should state that the handset was functioning normally at the relevant time and that its operating system and applications were working properly. The expert should explain that, on forensic examination, there are no signs of tampering, editing, or manipulation of the data. The metadata and system logs should be shown to be consistent with the claimed events. The

expert should also confirm that the method used to extract or copy the data was technically sound and reliable, and that the extracted files match the data stored in the handset.

Quasi-Judicial Authority: In quasi-judicial proceedings, when a mobile handset is produced as evidence, the authority must ensure that the data it contains is credible, reliable, and trustworthy. The authority should examine the testimony of the witness or custodian, who must confirm that the handset was in proper working condition at the relevant time, that it was regularly used, and that no malfunction affected the data. The witness should also verify that messages, recordings, or other data are the same as originally stored, that extraction, display, or transcription was done correctly, and that no editing, deletion, or insertion occurred after the relevant events. Custody of the device should be shown to have been properly maintained, and the handset must be linked to the concerned person and their account or phone number. The authority should also consider expert evidence confirming that the handset functioned normally, that forensic examination shows no signs of tampering or manipulation, and that metadata and system logs are consistent with the claimed events. The expert should explain that the extraction or copying process was technically reliable and that the extracted data matches what is stored in the handset. The opposing party must be given a fair opportunity to test the evidence, including cross-examination of the witness or expert, filing a contrary opinion, or inspecting the handset if feasible. The authority must be satisfied that the substantive requirements of authenticity, integrity, reliability, and accuracy are met before relying on the data for findings.

Illustration: WhatsApp account shown from a produced mobile phone handset

Witness or Custodian: The witness or custodian should state that the mobile handset was working normally at the relevant time and that WhatsApp was installed and functioning properly on the device. The messages were sent and received in the ordinary course of use. The messages shown are exactly as stored in the phone, and the screenshots, printouts, or transcripts correctly reflect the conversation without any alteration or omission. The witness should also confirm that the handset remained in the custody of the concerned person or authority, that no deletion, editing, or insertion of messages was done after the relevant events, and that the device was kept safely until it was produced. Finally, the witness should identify that the WhatsApp account belongs to the concerned person, that the linked mobile number is correctly identified, and that the conversation took place between the stated parties.

Expert: The expert should state that the mobile handset and the WhatsApp application were functioning normally at the relevant time and that there is no indication of any system malfunction affecting the messages. The expert should explain that, upon forensic examination, there are no signs of message editing, deletion, or fabrication. The metadata and system records are consistent with the claimed timeline of the conversation. The expert should also confirm that the method used to extract or copy the WhatsApp data is technically reliable and that the extracted data matches what is actually stored in the handset.

Quasi-Judicial Authority: The authority must ensure that the evidence is credible, reliable, and trustworthy. The authority should examine the testimony of the witness or custodian, who must confirm that the handset and WhatsApp application were working normally, that messages were sent and received in the ordinary course, and that the messages shown, whether screenshots, printouts, or transcripts, accurately reflect the conversation without any alteration or omission. The witness must also

verify that the device remained in proper custody, that no editing, deletion, or insertion of messages occurred after the relevant events, and that the WhatsApp account and linked mobile number belong to the concerned person, with the conversation taking place between the stated parties. Expert evidence should be considered to confirm technical reliability: the expert must state that forensic examination shows no tampering, editing, or fabrication, that metadata and system records align with the claimed timeline, and that the method used to extract or copy the data is technically sound, with the extracted data matching what is stored in the handset. The opposing party must be given a fair opportunity to test the evidence, including cross-examination, filing contrary expert opinions, or inspecting the handset if feasible. Even if technical formalities such as a hash value is not produced, the authority must ensure that the substantive requirements of authenticity, integrity, reliability, and accuracy are satisfied before relying on the messages for findings.

Illustration: Photograph taken by a digital device. [The defence is that it is AI-generated].

Witness or custodian: The witness or custodian should state that the camera or mobile phone used to take the photograph was working normally at the relevant time and that the photo was taken in the ordinary course without any technical problem. The witness should confirm that the photo produced is the same as originally captured by the device and that the printout or digital copy accurately represents the original image. The witness should also state that the photo was not edited, manipulated, or enhanced after it was taken, and that the device or storage media remained in safe custody. Finally, the witness should identify that the photo was taken by the stated person or device and that the place, time, and persons shown in the photo are correctly identified.

Photographer or Custodian: The photographer or custodian should state who took the photograph and when and where it was taken. The witness should confirm that the image was captured in the ordinary course and was not edited, manipulated, or created using AI or other tools. The original device or memory card should be produced, and it should be shown that the photograph exists in the device's gallery or storage in its original form. The witness should also point out the date, time, and device information embedded in the image file, and confirm that this metadata is consistent with the claimed circumstances of the photograph.

Expert: The forensic expert's role is to examine the photograph or digital image for any signs of manipulation, editing, or AI generation. The expert analyzes the file for inconsistencies, traces of alteration, unusual compression patterns, metadata anomalies, or other technical indicators that could suggest the image has been modified or artificially created. Their report helps establish the integrity and authenticity of the photograph.

Quasi-Judicial Authority: The authority must ensure that the evidence is credible, reliable, and trustworthy. The authority should examine the testimony of the witness or custodian, who must confirm that the camera or mobile device was functioning normally, that the photograph was taken in the ordinary course without technical problems, and that the image produced accurately reflects the original photo without any editing, manipulation, or AI generation. The custodian should also confirm that the device or storage media remained in proper custody, that the photograph was captured by the stated person or device, and that the place, time, and persons shown are correctly identified. Expert evidence should be considered to verify technical integrity and authenticity; the forensic expert must examine the

image for signs of alteration, manipulation, or AI generation, including reviewing metadata, file properties, compression patterns, and other technical indicators, and confirm that the photograph has not been tampered with. The opposing party must be given a fair opportunity to test the evidence, including cross-examining the custodian or expert and inspecting the original device if feasible. The substantive requirements of authenticity, integrity, reliability, and accuracy are satisfied before relying on the photograph in its findings.

Note: In Nirmaan Malhotra vs Tushita Kaul [7], the husband contended that wife was living in adultery with another man and produced photographs of his wife and the adulterer. The Court observed that it was unclear whether the person in the photograph was the wife and took judicial notice that it was an era of deepfakes and the burden of proof was on the husband.

Note: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, [updated as on 10.02.2026] [8] , The amended Information Technology Rules impose specific duties on online intermediaries such as social media platforms and AI services to prevent unlawful or misleading digital content, especially deepfakes and other synthetically generated information. Platforms must publish clear user guidelines, warn users about illegal content, and send reminders at least every three months about legal obligations and possible penalties. The rules define unlawful synthetic content to include impersonation deepfakes, non-consensual intimate images, fake electronic documents, and fabricated videos. Intermediaries must use technical tools to detect and remove such high-risk content while ensuring fairness, accuracy, and user privacy. Routine edits like cropping, brightness adjustment, translation, or accessibility changes are allowed if they do not distort the original material. The government also has the power to block specific online content on grounds such as national security or public order, including emergency blocking subject to later review. Overall, the framework is regulatory and compliance-oriented, rather than focused on courtroom evidence law.

Since India does not yet have codified legal standards for deepfake detection, the task of identifying such content largely depends on forensic experts. They examine indicators such as synthetic-generation signatures, metadata inconsistencies, and AI-generation markers to decide whether a file is genuine or fabricated. Therefore, in quasi-judicial proceedings where a formal certificate is not mandatory, the safer and fairer approach is to follow a hybrid method [as per U.S. system}. Hybrid method involves relying on a combination of forensic validation, expert opinion, platform or custodian records, and witness identification to assess the authenticity, integrity, and accuracy of the digital material. In any circumstances, the administrative justice must remain open to reliable forensic evidence, especially when it shows that a procedure may have been affected by fraud. Where electronic records formed the basis of charges and credible forensic evidence questions their authenticity, the authority generally cannot ignore this without examining it.

Illustration: Electronic Ticket Issuing Machines (ETIMs)

Custodian / Operator / Witness: The custodian or operator of the ETIM device must confirm that the machine was functioning normally at the relevant time and that tickets were issued in the ordinary course of business. They should verify that the printouts or digital records accurately reflect the transactions stored in the device and that these records have not been altered, deleted, or manipulated after generation. The ETIM must have remained in official custody and been handled according to

standard procedures, and the device should be properly assigned to the concerned operator or station. The custodian should be able to confirm that the ticket numbers, dates, times, fares, and other transaction details are correct, that any logs or memory cards storing the data were preserved securely, and that they can explain the process of ticket issuance, storage, and transfer of data.

Expert: The expert examines the ETIM records or printouts to ensure they have not been tampered with or manipulated. They verify that the device was functioning properly during the relevant period and confirm that the ticketing logs stored in the machine match the issued tickets. The expert checks system metadata, transaction logs, and memory records to confirm integrity, and ensures that any extraction or copying of data was done using a technically reliable method. Finally, the expert confirms that the ETIM data corresponds to the claimed operator, location, and time of the transactions.

Quasi-Judicial Authority: The authority must ensure that the evidence is credible, reliable, and trustworthy. The authority should examine the testimony of the custodian or operator, who must confirm that the ETIM device was functioning normally, that tickets were issued in the ordinary course of business, and that the records accurately reflect the transactions without any alteration, deletion, or manipulation. The custodian must also confirm that the device and any memory cards or logs were kept in official custody, handled according to standard procedures, and properly assigned to the concerned operator or station. Expert evidence should be considered to verify the technical integrity and reliability of the ETIM data. The expert must confirm that the machine was working correctly, that the ticketing logs match the issued tickets, and that any extraction or copying of data was technically sound. The authority should ensure that the records correspond to the claimed operator, location, and time, and that the opposing party has a fair opportunity to test the evidence, including cross-examining witnesses or experts. The authority must be satisfied that the substantive requirements of authenticity, integrity, reliability, and accuracy are met before relying on the ETIM records in its findings.

Illustration: Emails and Digital Correspondence (official, personal, or business)

Party relying: The party must show that the computer, phone, or email server used was functioning normally. The emails were sent or received in the ordinary course of business, personal, or official communication. Any printout or digital copy produced accurately reflects the original content, including text, attachments, date, time, and sender/receiver details. The emails have not been altered, fabricated, or manipulated after creation. The account or storage system must have been under proper control, and the emails must originate from the claimed sender's account. The person who sent or received the emails should confirm that the account belongs to them, the emails were actually sent or received, and the contents are genuine. Additional proof can include that, Email headers showing sender, receiver, date, time, and routing details. Company server logs or IT department records (for official emails). The original device where emails are stored or access to the original mailbox/application. Explanation of how the emails were extracted, copied, or printed. Documentation of who handled the device or data and how it was preserved.

Witness/Custodian: The custodian (e.g., IT officer, employee) can confirm the original storage, access, and handling of the device or mailbox. They may explain how the emails were extracted or printed, who handled them, and how they were preserved to ensure they remained unchanged.

Expert: The expert examines email headers, server logs, or metadata. They check for any signs of spoofing, tampering, or fabrication. The expert also validates that the extraction method was reliable and that the digital copy matches the original stored emails.

Quasi-Judicial Authority: The authority must ensure the evidence is credible, reliable, and trustworthy. The authority should examine the testimony of the custodian or party relying on the record, who must confirm that the device or server was functioning normally, that the emails were sent or received in the ordinary course, and that the digital copies or printouts accurately reflect the original content, including text, attachments, dates, times, and sender/receiver details. The custodian or party must also confirm that the accounts or devices were under proper control and that no alteration, deletion, or manipulation occurred after creation. Expert evidence should be considered to verify the technical integrity and authenticity of the emails, including examination of headers, server logs, metadata, and extraction methods. The authority must ensure that the evidence corresponds to the claimed sender, receiver, and time, and that the opposing party is given a fair opportunity to test the evidence, such as cross-examination, filing contrary expert opinion, or inspecting the original mailbox or device. The substantive requirements of authenticity, integrity, reliability, and accuracy are met before relying on the emails for findings.

Illustration: Biometric or Attendance Logs (fingerprint, access card, facial recognition systems)
Party relying: The party producing the attendance record must show that the biometric machine, access card reader, or facial recognition system was working properly at the relevant time. The system was used in the normal course of business. The attendance report or printout accurately reflects the data stored in the system, including dates, times, and user identification. The data was not edited, deleted, or tampered with after recording. The system was under proper administrative control, and access was restricted to authorized personnel. The biometric template, access card, or facial record belongs to the concerned person, and the entries correspond to their actual presence or access.

Witness/Custodian: The system administrator or HR officer explains how the system works, how data is recorded and stored, and confirms that the system was functioning properly. They may present enrolment records showing registration of fingerprints, facial data, or access cards. System logs, attendance registers, or software reports may be produced. The custodian can demonstrate the original data in the system and explain how the attendance report was generated, including who accessed the system and when.

Expert: A technical or forensic expert may examine the system logs and other data. The expert can confirm that the attendance entries are genuine and show no signs of tampering or manipulation.

Quasi-Judicial Authority: The authority must ensure the records are credible, reliable, and accurate. The authority should examine the testimony of the party producing the record, who must confirm that the biometric machine, access card reader, or facial recognition system was functioning normally at the relevant time, that it was used in the ordinary course, and that the attendance report accurately reflects the data stored in the system. The custodian or system administrator should explain how the system works, confirm that the data has not been altered, deleted, or manipulated, and provide supporting records such as enrolment data, system logs, or attendance registers. Expert evidence should be considered to verify technical integrity, including examination of system logs or software records to

ensure there are no signs of tampering. The authority must also ensure that the entries correspond to the person claimed and that the opposing party has a fair opportunity to challenge the evidence through cross-examination, inspection, or filing a contrary expert opinion. The authority must satisfy itself that the substantive requirements of authenticity, integrity, reliability, and accuracy are met before relying on the records for findings.

Illustration: Digital Financial Records (bank statements, e-wallet logs, online transaction records)

Party Relying: The bank or e-wallet system was working normally at the relevant time. The records were generated in the ordinary course of business. The statement or transaction log produced accurately reflects the data stored in the system. Dates, amounts, account numbers, and transaction details are correctly shown. The records were not edited, manipulated, or fabricated after generation. The statement is a true extract from the original system, originating from the concerned bank, financial institution, or e-wallet provider. The account or wallet belongs to the person to whom it is attributed.

A nodal officer, bank manager, or authorized representative explains how the records are generated and stored, confirms that the system functions normally, and certifies that the statement is a true extract from the system. Supporting documents may include certified bank statements, official transaction reports, account opening forms, and KYC records linking the account to the person. The original records can be produced if required. The officer also explains who accessed, downloaded, or printed the records.

Expert: A forensic or technical expert may examine the digital file or transaction logs, including metadata and system details. The expert can confirm that the records are genuine and show no signs of tampering or manipulation.

Quasi-Judicial Authority: In quasi-judicial proceedings, when digital financial records such as bank statements, e-wallet logs, or online transaction records are relied upon, the authority must ensure that the records are credible, authentic, and accurate. The authority should examine the testimony of the party producing the records, who must confirm that the financial system was functioning normally, that the records were generated in the ordinary course of business, and that the statement or transaction log accurately reflects the data stored in the system. Custodians or authorized representatives should explain how the records are generated, stored, and accessed, and provide supporting documents such as certified statements, account opening forms, KYC records, or official transaction reports. Expert evidence should be considered to verify technical integrity, ensuring that the files, logs, or metadata show no signs of tampering or manipulation. The authority must also ensure that the account or wallet belongs to the person claimed and that the opposing party has a fair opportunity to challenge the records through cross-examination, inspection, or filing a contrary expert opinion. The substantive requirements of authenticity, integrity, reliability, and accuracy are met before relying on the records for its findings.

Illustration: CCTV / Video Surveillance Footage

(a) General Security Footage:

Security Officer / System Operator: The CCTV system was working properly on the relevant day. Cameras were installed at the correct locations, and recordings were automatic and continuous. The footage was taken from the official system and preserved without alteration.

Expert: Examine the video for signs of editing or manipulation. Verify timestamps, metadata, and overall file integrity to confirm authenticity.

(b) Incident in Building Corridor:

Building Manager / CCTV Operator: The cameras were operational at the relevant time. Footage was copied from the building's official system and handed over without tampering. **Expert:** Check for alterations, verify continuity and timestamps, and examine file properties to confirm genuineness.

(c) Retail Store Surveillance:

Store Manager / CCTV Operator: Cameras were installed at the relevant locations and the system functioned normally. Footage was automatically recorded from the original system and preserved without any changes.

Expert: Verify that the video was not edited, check frame continuity, timestamps, and overall file integrity.

(d) Absent-on-Duty Evidence:

CCTV Operator / Supervisor: Cameras covered the relevant area and were working normally. Recording was automatic and sourced from the official system without alteration. **Expert:** Examine whether any selective editing occurred, check continuity of recording, and verify timestamps and integrity of the video file.

Quasi-Judicial Authority: The authority must ensure that the recordings are authentic, accurate, and reliable before using them for any findings. The authority should consider the testimony of the security officer, system operator, building manager, or store personnel, who must confirm that the cameras and recording system were functioning properly at the relevant time, that the recordings were automatic and continuous, and that the footage was preserved without alteration. Custodians should also explain how the footage was copied, transferred, or stored, and that the original system remained under proper control. Expert evidence must be considered to verify technical reliability, integrity, and authenticity, including examination of timestamps, metadata, frame continuity, file properties, and signs of editing or manipulation. The authority must also ensure that the opposing party has a fair opportunity to test the evidence, such as by inspecting the original recordings or filing a contrary expert opinion. The substantive requirements of authenticity, integrity, reliability, and accuracy are met before relying on the footage.

Illustration: Computer / Server Logs- Unauthorized Office Login

System Administrator / IT Officer: The server was working properly at the relevant time. Login and logout entries were recorded automatically by the system in the ordinary course of business. The logs were stored securely and were not altered. The entries correspond to the official server and the employee's user account.

Expert: Examine whether the logs were tampered with, deleted, or fabricated. Verify that timestamps, system configuration, and log continuity are consistent with normal operation to confirm authenticity.

Quasi-Judicial Authority: In quasi-judicial proceedings, when computer or server logs are relied upon, the authority must ensure the records are credible, reliable, and accurate before acting on them. The authority should consider the testimony of the system administrator or IT officer, who must explain that the server was functioning properly, that login and logout entries were automatically recorded in the ordinary course of business, and that the logs were securely stored without any alteration. Custodians should also confirm that the entries relate to the correct server and user account. Expert evidence should be used to verify that the logs were not tampered with, deleted, or fabricated, and to ensure that timestamps, system configuration, and log continuity are consistent with normal operation. The opposing party must be given an opportunity to inspect the logs or present contrary expert evidence. The authority must satisfy itself that the logs meet the substantive requirements of authenticity, integrity, reliability, and accuracy before relying on them for findings.

Note: When two different electronic versions of the same order; one allowing and the other rejecting the same application, are produced, then the main issue is to identify which version is the authentic record. This can be determined only by retrieving the order directly from the official electronic system, including the local office server where it was first uploaded and the central servers where it is stored and made available for download. The system audit logs must be checked to show the exact date and time of creation and upload, whether any modification or replacement took place, and the user responsible for those actions. The metadata of both soft copies, such as their creation and modification dates and author details, should also be compared to verify their integrity. If only printed copies are produced and no soft copies are filed, in such a case, the original electronic record must be obtained from the official servers, along with download logs showing when and by whom the order was accessed and which version existed at that time, and the audit trail of the case file showing when the order was passed and whether it was later modified or replaced.

Illustration: Memory Card

Relying Party: The party producing the memory card must show that the card contains the original electronic record (e.g., photos, videos, audio files, documents) relevant to the proceedings. He should explain how the data was recorded or created, confirm that the memory card has been securely stored, and that no tampering, deletion, or modification occurred after the relevant events. If possible, he should provide a chain of custody showing who handled the card from the time of recording to production.

Custodian / Witness: The custodian or witness should testify that the memory card was in proper working condition at the relevant time and was used in the ordinary course. He must confirm that the files stored on the card are identical to the originals, and that the card was safely preserved until production. The witness should explain how the card was handled, transferred, or copied and affirm that no data was altered, inserted, or deleted.

Expert: A forensic or technical expert examines the memory card to check for signs of tampering, editing, or manipulation. The expert verifies metadata, file properties, timestamps, and continuity of records. He confirms that the method used to extract or copy the data is technically sound and reliable, and that the files on the memory card correspond exactly to the originals.

Quasi-Judicial Authority: The authority must ensure that the memory card and its contents are credible, authentic, and reliable. He should examine the testimony of the custodian and the expert to

confirm the card's integrity, authenticity, and accuracy. The authority must also ensure that the opposing party has a fair opportunity to inspect the card, cross-examine the witnesses or expert, and raise objections. The authority must satisfy itself that the record can be trusted before relying on it for findings.

Note: Where a hash value is not disclosed, the party relying on the electronic record must prove its integrity and chain of custody through other reliable evidence. This generally requires proof of how and by whom the device or data was first seized or collected, the manner of extraction, and a clear record showing who handled the device or storage media at each stage. Seizure memos, custody registers, transfer records, sealing details, and oral testimony of the persons who seized, extracted, or prepared the record are commonly used to establish continuity and authenticity. If the electronic record is disputed, or the circumstances of its creation or handling raise doubt, the authority may require technical or forensic evidence to confirm that the extraction process was reliable and that there are no signs of tampering. Even where no technical objection is raised, the adjudicating authority must still be satisfied that the record appears trustworthy and properly preserved. However, expert evidence [a person with specialised technical or forensic knowledge, appropriate to the nature of the electronic evidence and the dispute involved] is not automatically mandatory in every case; its necessity depends on the nature of the record, the level of dispute, and the overall reliability of the supporting evidence.

Note: If a secured hash value is not produced, the opponent is not deprived of the opportunity to test the electronic evidence. The opponent can still adopt several lawful methods to verify its authenticity and integrity. He may seek production of the original device or storage medium from which the data was created or stored. The opponent may also demand supporting technical material such as metadata, system logs, backup records, or chain-of-custody documents. In addition, they can seek comparison with independent sources, such as server records, third-party backups, or the other party's device, to check whether the contents match. Finally, the opponent can rely on cross-examination of the person who created, handled, or produced the electronic record, and through such questioning, expose any gaps, inconsistencies, or signs of alteration in the process of recording, storage, transfer, or preservation.

Note: If the opponent receives only a copy-paste version of an electronic record [without secure hash value] and files an independent expert opinion, the situation becomes critical. The burden of proving that the record is genuine and untampered remains on the producing party, and the absence of a secure hash value or expert testimony weakens their position. The opponent's expert report, which may highlight possible alterations, inconsistencies, or integrity issues, becomes material evidence that the authority must consider. If the producing party had the means to provide proper technical proof, such as a secure hash value, expert examination, or the original device, but failed to do so, the authority may draw an adverse inference regarding the reliability of the record. Where only a copy-paste version is produced without technical support, secure hash value, and the opponent's expert raises doubts, the authority may refuse to rely on the record. However, the producing party still has an opportunity to rebut the opponent's expert opinion by producing the original device, presenting their own expert, or providing other credible technical evidence to establish the integrity of the record.

Note: There is no specific judicial pronouncement / Judgment stating that a secure hash value or hash value need not be disclosed in disciplinary proceedings or before tribunals where the Evidence Act is not applicable [[Toman Lal Sahu S/o Panth Ram Sahu vs State of Chhattisgarh [4]]. The case law instead

focuses on the broader requirement that electronic evidence must be shown to be authentic, reliable, and untampered, and that the opposing party must have a fair opportunity to test it and it is based on natural justice.

Power to Review:

Pravin Kumar v. Union of India [5] to reaffirm that,' judicial review of administrative action is limited to checking if the process was fair, not re-evaluating the evidence like an appellate court'. It has also held for grounds of "gross unreasonableness" and "manifest error of law" are the independent review grounds.

From the above view, the court does not re-appreciate the evidence like an appellate authority. Its role is limited. It only examines whether there was some credible material before the authority, whether the basic substantive safeguards were followed, and whether the process was fair and rational. If the electronic evidence lacks authenticity, integrity, or reliability, or if the opposing party was not given a fair opportunity to test it, the finding becomes vulnerable. In such a situation, the court may interfere on the ground that the decision is contrary to natural justice, based on no evidence, or so unreasonable that no rational authority could have reached it. Therefore, if substantive compliance and proof is absent, the electronic record cannot be safely relied upon, and any decision based on such unproved evidence is considered unsustainable under judicial review principles, as reaffirmed in Pravin Kumar v. Union of India.

Conclusion:

Where the BSA is not applicable like quasi-judicial proceedings or Tribunal, in that situation, the substantive principles cannot be ignored by authority. The substantive requirements like integrity, authenticity, reliability, and accuracy, remain mandatory and must always be proved by some credible means. Therefore, in all circumstances, whether device is produced or electronic record is produced, integrity, authenticity, reliability, and accuracy are always mandatory substantive requirements and decision of the authority must always rest on credible and trustworthy electronic evidence.

Recommendations and Limitations: As per Part I to Part III

References:

1. Union of India v. T.R. Varma https://indiankanoon.org/doc/1478450/
2. Bareilly Electricity v. Workmen https://indiankanoon.org/doc/244446/
3. The Assistant Commissioner of Income Tax vs Vetrivel Minerals https://www.casemine.com/judgement/in/681234eb3565bc4ff53809ee
4. Toman Lal Sahu S/o Panth Ram Sahu vs State of Chhattisgarh, WPS No. 5287 of 2012, 26.03.2021 https://www.indianemployees.com/judgments/details/toman-lal-sahu-versus-state-of-chhattisgarh, the Hon'ble court dealt only with supply of the CD for fair defence. It did not discuss hash values at all.
5. Pravin Kumar v. Union of India https://indiankanoon.org/doc/108065727/
6. State of U.P. v. Saroj Kumar Sinha, https://indiankanoon.org/doc/1064026/
7. Nirmaan Malhotra v. Tushita Kaul, 2024 SCC OnLine Del 4326

8. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 20211 [updated as on 10.02.2026] https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf
9. MALINI JAIN Versus PANKAJ BHUTAD AND OTHERS https://www.livelaw.in/pdf_upload/2026/02/11/trtrtrtrt-655337.pdf

Other Reference:

1. Supply of copy of electronic evidence - Suggested system for District Courts, Advanced International Journal for Research, Volume 7, Issue 1 (January-February 2026), https://www.aijfr.com/papers/2026/1/3213.pdf
2. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach--[Part-III], Advanced International Journal for Research, Volume 7, Issue 1 (January-February 2026), https://www.aijfr.com/papers/2026/1/3405.pdf
3. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach--[Part-II], Advanced International Journal for Research, Volume 7, Issue 1 (January-February 2026), https://www.aijfr.com/papers/2026/1/3276.pdf
4. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approachhttps://www.academia.edu/150287956/Trial_Court_as_Guardian_of_Electronic_and_Digital_Record_Under_Section_63_of_the_Bharatiya_Sakshya_Adhiniyam_2023_A_Modern_Approach