ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: ADMISSIBILITY, AUTHENTICITY AND THE CHALLENGES OF DIGITAL MANIPULATION

Lakshya Sharma, Law Student, Dr. Ram Manohar Lohiya National Law University

ABSTRACT

The increasing reliance on electronic records in judicial proceedings has made the reliability of digital evidence a significant concern for Indian evidence law. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), establishes a statutory framework for the recognition and proof of electronic and digital records, particularly through Sections 61 to 63 and the certificate prescribed under Section 63(4) and its Schedule .However, the formal requirements governing admissibility raise a broader question: to what extent do statutory certification and technical safeguards establish the authenticity and evidentiary reliability of digital material? This paper examines the statutory framework under the BSA alongside the judicial development of electronic evidence under the former Indian Evidence Act, 1872, with particular reference to State (NCT of Delhi) v. Navjot Sandhu, Anvar P.V. v. P.K. Basheer, Shafhi Mohammad v. State of Himachal Pradesh, and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. It also considers the Supreme Court's order in Pune Bar Association v. Union of India (2026) in relation to the certification requirements under Section 63(4).The paper argues that admissibility, authenticity, integrity, contextual accuracy and evidentiary weight are distinct questions that should not be conflated. Although certification and hash values can contribute to procedural accountability and the detection of subsequent alteration, they cannot independently establish a record's original provenance, exclude prior manipulation or prove the truth of its contents. These limitations become particularly significant in cases involving selective editing and artificial intelligence generated Deepfakes. Adopting a doctrinal and analytical approach, the paper proposes clearer certification guidance, accessible forensic assistance, documented chains of custody, proportionate judicial scrutiny of disputed records and specialised training for legal professionals. It concludes that an effective evidentiary framework must combine statutory compliance with

technically informed, context sensitive evaluation to protect both the integrity of judicial proceedings and the fair administration of justice.

Key Words: - *Electronic Evidence, Bharatiya Sakshya Adhiniyam, 2023, Digital Authentication, Admissibility of Electronic Records, Artificial Intelligence-Generated Deepfakes.*

Introduction

The increasing use of digital technology has significantly changed the manner in which evidence is created, stored, communicated and presented before courts. Electronic records such as emails, WhatsApp conversations, CCTV footage, call recordings, photographs, social media posts and other digital files have become important sources of evidence in both civil and criminal proceedings. Their ability to preserve and communicate information makes them valuable for the administration of justice. However, the same technology also creates concerns regarding alteration, fabrication, selective editing and the use of artificial intelligence to generate misleading audio, images and videos. In India, the law governing the admissibility of electronic evidence has developed through statutory amendments and judicial interpretation. The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on 1 July 2024, replaced the Indian Evidence Act, 1872 and introduced a revised statutory framework for electronic and digital records. Sections 61 to 63 of the BSA address the legal recognition, proof and admissibility of such records. In particular, Section 63 and its accompanying Schedule prescribe requirements relating to the production and certification of electronic records. These provisions seek to facilitate the use of digital evidence while providing safeguards against questions concerning its integrity and authenticity.

Against this background, the present research examines the legal framework governing electronic evidence under the BSA, with particular emphasis on the relationship between admissibility, authenticity and evidentiary value. It also considers the challenges posed by digital manipulation and AI-generated material, while exploring whether existing statutory and procedural safeguards are sufficient to ensure a fair and reliable evaluation of electronic evidence. The central argument of this paper is that statutory compliance is an essential safeguard, but it should not be confused with conclusive proof of authenticity or reliability. A balanced approach must preserve the legal requirements for admitting electronic records while

allowing appropriate scrutiny of their source, integrity and contents. Such an approach is necessary to ensure that digital evidence contributes to the discovery of truth without creating unnecessary barriers to the fair administration of justice.

Statutory Framework Governing Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 (BSA), which came into force on 1 July 2024, provides the principal statutory framework governing electronic and digital evidence in India. It replaced the Indian Evidence Act, 1872, while introducing provisions that address the growing significance of digital records in judicial proceedings. Emails, electronic messages, digital photographs, CCTV footage, call recordings and other forms of electronically stored information are increasingly relied upon to establish facts in civil and criminal cases. The BSA recognises the importance of such material while prescribing specific requirements for proving its contents and securing its admissibility. The principal provisions governing this subject are Sections 57 to 63, particularly Sections 61–63[1], which must be read together to understand the legal treatment of electronic evidence. The distinction between primary and secondary evidence remains relevant to the statutory framework. Section 57 of the BSA defines primary evidence and includes specific explanations concerning electronic and digital records. It recognises that electronic information may exist simultaneously or sequentially in multiple files and that recordings stored or transmitted through different systems may qualify as primary evidence in the circumstances described by the provision. Section 58 deals with secondary evidence, while Sections 59 and 60 address proof by primary evidence and the circumstances in which secondary evidence may be given. These provisions reflect the practical reality that digital information is often stored, copied and transferred across multiple devices rather than preserved in a single physical document.

Section 61 establishes the legal recognition of electronic and digital records by providing that a record cannot be denied admissibility merely because it is electronic or digital in nature, subject to the requirements of Section 63. It also recognises such records as having the same legal effect, validity and enforceability as other documents, in accordance with the statutory provision. Section 62 complements this recognition by providing that the contents of electronic records may

[1]Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 61–63.

be proved in accordance with Section 63. These provisions establish that electronic records are not excluded from the evidentiary process merely because of their digital form, but their proof and admissibility remain subject to the applicable statutory conditions.

Section 63 is central to this framework because it prescribes the conditions under which electronic records and electronic outputs may be admitted in evidence. Section 63(1) addresses the admissibility of qualifying electronic output, while Section 63(2) sets out conditions relating to the regular use of the relevant computer or communication device, the ordinary-course feeding of information, the proper functioning of the device and the relationship between the information produced and the information originally supplied to the system. Section 63(3) addresses situations in which information is processed or stored through multiple computers or communication devices, allowing the relevant systems to be treated as a single computer or communication device for the purposes of the provision when its conditions are satisfied. These requirements are significant because electronic information may be generated, processed and stored through interconnected systems rather than a single device. An important feature of the current framework is the certificate requirement under Section 63(4)[2], read with its Schedule. The provision prescribes requirements relating to the submission of electronic records, while the Schedule specifies particulars concerning the record, its source or device, the manner of production and hash-value information, along with the prescribed certification components. The certificate is intended to provide information about the production of the record and the relevant technical circumstances under which it is presented. This is particularly important when a party relies upon an electronic output or copy rather than producing the original source device itself.

The wider statutory framework also recognises the importance of technical expertise in the evaluation of electronic evidence. Section 39[3] of the BSA, which deals with expert opinion on specified matters, may become relevant where specialised technical questions arise. In addition, Section 79A [4]of the Information Technology Act, 2000 provides for the notification of an Examiner of Electronic Evidence. These provisions form part of the broader legal context within which courts may evaluate technical questions relating to digital material. Depending on the

[2]Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63(4) read with the Schedule thereto.
[3]Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 39.
[4]Information Technology Act, 2000 (Act 21 of 2000), s. 79A.

nature of the dispute, expert examination may assist in assessing whether a file has been altered, whether particular technical information supports a claim about its origin, or whether the methods used to examine it justify the conclusions drawn. Expert opinion, however, must itself be evaluated on the basis of the material examined, the methods employed and the reasons supporting the opinion. The statutory framework under the BSA therefore represents an attempt to balance the practical use of electronic records with the need for procedural and technical safeguards. Sections 61–63 establish the legal recognition, proof and admissibility of electronic evidence, while the certificate requirements seek to provide a structured method of presenting such records before courts. At the same time, digital evidence presents challenges that cannot always be resolved through formal compliance alone. A source device may be inaccessible, a record may have been manipulated before collection, or an apparently unchanged file may still be misleading because of its context or contents. Advances in artificial intelligence have further increased the importance of examining claims concerning the authenticity of digital material.

Judicial Evolution of Electronic Evidence in India

The judicial approach to electronic evidence in India has developed alongside changes in technology and the growing use of digital records in litigation. The principal challenge has been to determine how electronic records should be proved without compromising the reliability of judicial proceedings or creating unnecessary obstacles to the use of relevant evidence. Under the former Indian Evidence Act, 1872, the Supreme Court gradually established a specialised framework for the admissibility of electronic records through Sections 65A and 65B. These decisions continue to provide important background for understanding the corresponding provisions of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), although their application must be considered in light of the wording of the new legislation.

In ***State (NCT of Delhi) v Navjot Sandhu***[5],the Supreme Court adopted a relatively flexible approach to electronic evidence. The case arose from the prosecution relating to the attack on the Indian Parliament and involved the use of telephone records and other electronic material. The Court permitted electronic records to be proved through the general provisions governing secondary evidence, even where the requirements of Section 65B had not been satisfied. This

[5](2005) 11 SCC 600.

approach allowed electronic material to be considered through established evidentiary methods, but it also created uncertainty about whether the special statutory requirements for electronic records could be bypassed. The position changed significantly in ***Anvar P.V. v P.K. Basheer***[6]. The case concerned an election petition in which electronic recordings were relied upon to establish allegations of corrupt electoral practices. The Supreme Court held that secondary electronic evidence had to satisfy the specific requirements of Section 65B of the former Evidence Act. It rejected the approach in *Navjot Sandhu* insofar as that decision permitted the ordinary rules governing secondary evidence to substitute for compliance with the special electronic-evidence provision. The Court emphasised that the statutory framework governing electronic records had to be followed when such records were tendered as secondary evidence. The decision therefore strengthened procedural certainty and clarified the importance of certification in the admissibility of electronic records. The significance of *Anvar* lies in its recognition that electronic evidence requires a specific statutory method of proof. Digital information can be copied, transferred and reproduced without the visible physical changes associated with conventional documents. The certificate requirement was intended to provide a structured means of establishing the circumstances in which computer-generated material was produced.

A further dimension emerged in ***Tomaso Bruno v State of Uttar Pradesh***[7]**.**The case arose from a criminal prosecution in which the non-production of relevant CCTV footage became an important issue. The Supreme Court discussed the significance of scientific and electronic evidence and observed that the failure to produce available electronic material could affect the evaluation of the prosecution's case. The decision illustrates that electronic evidence is not important only when it is produced but the absence of relevant digital material may also raise questions about the completeness of the evidence available to the court. The difficulty faced by parties who do not control the device or system containing the relevant information was considered in ***Shafhi Mohammad v State of Himachal Pradesh*****, (2018)**[8]**.**The Supreme Court adopted a more flexible approach to the certificate requirement in circumstances where the party seeking to rely upon the electronic record was unable to obtain the necessary certificate. The

[6](2014) 10 SCC 473.
[7](2015) 7 SCC 178.
[8](2018) 2 SCC 801.

judgment reflected a practical concern: a litigant may need to rely on information stored on a device or system controlled by another person and may not have direct access to the technical information required for certification.

This approach was subsequently reconsidered by a larger Bench in ***Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020)[9]**.The case concerned video recordings relating to the filing of nomination papers in an election dispute. The Supreme Court reaffirmed the mandatory nature of the certificate requirement for secondary electronic evidence under Section 65B of the former Evidence Act and overruled the contrary approach adopted in *Shafhi Mohammad*. The Court also clarified that, where the required certificate could not be obtained from the person or authority controlling the relevant device or system, the court could assist in securing it through the appropriate legal process.The decision in *Arjun Panditrao* is particularly significant because it attempted to balance procedural certainty with practical fairness. It maintained that statutory requirements could not simply be disregarded because obtaining a certificate was inconvenient, while recognising that a party should not necessarily be deprived of relevant evidence merely because the necessary information was controlled by another person.

A major contemporary development is ***Pune Bar Association v Union of India[10]***, Writ Petition (Civil) No. 599 of 2026, decided on 22 May 2026. The petitioner challenged the constitutional validity of Section 63(4) of the BSA and its Schedule, arguing that the certificate requirements imposed an excessive burden on ordinary litigants. The challenge particularly concerned the disclosure of hash values in Part A of the prescribed certificate and the expert certification contemplated in Part B. The Supreme Court declined to entertain the challenge and held that the prescribed requirements could not be regarded as manifestly arbitrary or unreasonable merely because they imposed additional obligations on parties relying on electronic evidence. The Court reasoned that the inclusion of hash-value information had a rational connection with the objective of verifying the identity and integrity of digital data. It also considered expert certification an additional safeguard for secondary electronic evidence. The order is therefore important to the current constitutional position of the certificate framework under Section 63(4). However, the Court expressly refrained from giving a conclusive opinion on whether the expert

[9](2020) 7 SCC 1.
[10]W.P. (C) No. 599 of 2026 (Supreme Court of India, order dated 22 May 2026).

signing Part B must be a person notified under Section 79A of the Information Technology Act, 2000.The decision is significant because it demonstrates the continuing importance of procedural safeguards in the presentation of electronic evidence. At the same time, its reasoning must be understood within its proper scope. The Court's acceptance of the rational connection between certification, hash values and evidentiary integrity does not mean that every certified electronic record is conclusively authentic or that a hash value establishes the truth of its contents. A hash value can assist in determining whether data has changed relative to a reference value, but it does not necessarily establish whether the file was manipulated before that reference value was generated. Similarly, expert certification may assist in verifying technical aspects of a record without necessarily proving that the event depicted actually occurred.

Critical Analysis and Proposed Reforms

The Bharatiya Sakshya Adhiniyam, 2023 represents an important step towards adapting Indian evidence law to the increasing use of electronic records in judicial proceedings. By expressly addressing electronic and digital records and prescribing a structured certification process under Section 63, the legislation seeks to improve the manner in which such evidence is presented and verified. However, the effectiveness of this framework must be assessed not merely by the safeguards it prescribes, but by whether those safeguards adequately address the different ways in which digital evidence can be created, altered, presented and interpreted. The central concern is that a procedure designed to establish the admissibility and integrity of an electronic record cannot, by itself, establish that the record accurately represents the event it purports to depict.

One of the principal strengths of Section 63 is that it introduces a more structured process for producing secondary electronic evidence. The certificate prescribed under Section 63(4) and its Schedule, including hash-value disclosure and expert certification[11] can improve accountability and make it easier to identify subsequent changes to a digital file. Nevertheless, the statutory process should not be mistaken for a complete test of authenticity. A hash value is generated from the digital data supplied to the hashing process. It can help establish whether that data has changed when compared with a reliable reference hash, but it cannot independently establish

[11]Barbara Guttman, Douglas R. White, Shannan Williams and Tracy Walraven, Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387 (National Institute of Standards and Technology, 2022),

who created the file, whether the file had already been manipulated before the hash was generated, or whether the contents accurately represent the underlying event. For instance, if an altered video is submitted for certification and its hash is recorded only after the alteration, a matching hash at a later stage may demonstrate that the submitted file has remained unchanged since that point. It does not establish that the video was genuine before certification. A related concern is the distinction between the statutory certificate and the chain of custody. The certificate provides prescribed information about the electronic record and its production, while the chain of custody documents how the record was collected, transferred, stored, accessed and preserved. A certificate cannot automatically cure gaps in that history. Consider CCTV footage obtained from a commercial establishment: even if a copy is accompanied by the required certificate, questions may remain about whether the correct recording was extracted, whether the relevant time period was omitted, whether the system clock was accurate, or whether the footage was altered before it reached the person certifying it.

The certification framework also raises concerns about accessibility and procedural fairness.[12] Although expert scrutiny is important, obtaining technical assistance may be more difficult for individual litigants than for parties with substantial financial and institutional resources. A person seeking to rely on a private message, a recording or other electronic material may not possess the original device or have the technical ability to extract and preserve the data. The difficulty may be greater when the relevant record is held by a service provider, employer, financial institution or public authority. If access to the necessary certificate or expert assistance depends on resources beyond a litigant's control, a legitimate claim may be weakened by procedural barriers unrelated to the merits of the dispute. The Supreme Court's order in *Pune Bar Association v Union of India* is significant in this context. The Court rejected the challenge to the constitutional validity of the requirements under Section 63(4), reasoning that the hash-value requirement and expert certification have a rational nexus with authenticity and integrity. The Court left the wider issue concerning the application of Section 79A of the Information Technology Act, 2000 open, while clarifying that the Madras High Court's restrictive view should not be treated as binding precedent. The decision consequently supports the legitimacy of procedural safeguards, but it

[12]Vaibhav Chadha and Janani Sivaraman, "Critical Analysis of the Law on Admissibility of Electronic Evidence in India" 15 Jindal Global Law Review 119–132 (2024).

does not eliminate the need for clear guidance on expert competence, access to forensic services and the evidentiary significance of a certificate.

Another limitation concerns the treatment of authenticity as a question distinct from the admissibility of electronic evidence. A record may satisfy the applicable statutory conditions and still be disputed on substantive grounds. A screenshot may be incomplete; a message may be presented without the surrounding conversation; an audio recording may lack relevant context; and a video may be genuine in its individual frames but misleading because of selective editing or omission. The challenge becomes more serious with the development of deepfake technology and generative artificial intelligence[13]. Conventional digital-forensic safeguards are primarily concerned with identifying, preserving and examining a particular file. Yet an artificially generated video or voice recording may be created in a form that appears convincing from the outset. The difficulty is therefore not simply one of detecting post-creation tampering; it is also one of determining whether the content itself is trustworthy. The problem is not limited to the statutory text. Effective safeguards depend on the capacity of institutions to preserve and examine electronic evidence. Poor collection practices, inadequate storage facilities, inconsistent documentation and delays in forensic examination can weaken a case before the evidence reaches court. A reform programme should therefore include standardised evidence-handling protocols, secure storage, controlled access, documented transfers, appropriate hash-generation practices and the preservation of original data wherever legally and practically possible.

In light of these concerns, several reforms are warranted. First, practical guidance should clarify the operation of Section 63(4) and the Schedule, including the information expected in the certificate, the manner of recording hash values, and the distinction between certification and substantive authentication. The guidance should also address situations in which the proponent does not control the device or system from which the record originated. In such cases, courts should have clear procedures for directing the relevant custodian or authority to assist in obtaining the necessary information, consistent with the applicable law. Second, accessible and independent forensic assistance should be strengthened. Public institutions should develop

[13]Abhishek Dalal, Chongyang Gao, Paul W. Grimm, et al., “Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases” 2024 University of Chicago Legal Forum 75–113 (2024).

adequate capacity to examine disputed electronic records, while maintaining appropriate safeguards for impartiality and technical competence. Where a party cannot reasonably obtain the necessary expertise, courts should be able to consider proportionate directions for examination or assistance, having regard to the nature of the dispute, the importance of the evidence and the interests of justice. Courts should adopt a clearer approach to assessing the evidentiary weight of electronic records. Where authenticity is specifically disputed, the court should record the nature of the objection and evaluate the available material, including the source, chain of custody, surrounding context, signs of alteration and any relevant expert opinion.

A certificate may support the admissibility and integrity of a record, but it should not create an irrebuttable presumption that the contents are true. Equally, a general allegation of manipulation should not, without more, automatically displace electronic evidence that is otherwise supported by reliable material. A reasoned, casespecific assessment would promote fairness to both the party relying on the record and the party challenging it. The distinction between admissibility and authenticity also requires a proportionate approach to judicial scrutiny. A challenge to an electronic record should be assessed by reference to its specific grounds rather than accepted or rejected merely because a certificate has been produced. Where the objection concerns an identifiable issue, such as an unexplained break in the chain of custody, inconsistent metadata or an alleged alteration, the court may consider whether further technical examination or corroborative material is necessary. This approach would avoid two competing risks: excessive reliance on formal certification and the indiscriminate rejection of electronic material because of the possibility of manipulation. The objective should be to ensure that the degree of scrutiny corresponds to the nature of the challenge, the significance of the record and the available means of verification.

Fourth, a more specialised response is required for suspected deepfakes and AI-generated material[14]. Courts should be equipped to seek relevant forensic assistance where a concrete dispute arises about synthetic generation, voice cloning, face replacement or material editing. The inquiry should focus on verifiable indicators and the available technical evidence rather than

[14]Felipe Romero-Moreno, “Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights” 58 Computer Law & Security Review 106162 (2025).

on the visual or auditory persuasiveness of the recording alone. Detection methods may have limitations and can produce errors; their results should therefore be assessed alongside the source of the material, its history, relevant metadata, contextual evidence and the conclusions of competent experts. This would allow courts to respond to technological developments without creating an unrealistic expectation of perfect detection.

Finally, legal education and judicial training should keep pace with the growing technical complexity of electronic evidence. Judges, advocates, investigators and other relevant personnel should understand the basic functions and limitations of hash values, metadata, digital extraction, chain of custody and AI-generated content. Its purpose should be to enable them to ask the right questions, recognise the limits of technical claims and distinguish between procedural compliance and proof of authenticity. A technically informed judicial process is particularly important where sophisticated-looking digital material may be persuasive despite unresolved questions about its origin or meaning.

Conclusion

The Bharatiya Sakshya Adhiniyam, 2023 marks an important development in the treatment of electronic evidence under Indian law. Its recognition of electronic and digital records, together with the certification framework under Section 63, reflects the need to adapt evidentiary rules to an increasingly digital society. The judicial evolution from *State (NCT of Delhi) v Navjot Sandhu* to *Anvar P.V. v P.K. Basheer* and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* demonstrates the judiciary's effort to establish procedural certainty in the production of electronic evidence. The Supreme Court's order in *Pune Bar Association v Union of India* further highlights the legitimate role of safeguards designed to protect the integrity of digital records. However, the effectiveness of these safeguards depends on recognising their limitations. Compliance with certification requirements and the preservation of a file's integrity do not conclusively establish its origin, authenticity or truthfulness. This distinction has become increasingly significant with the emergence of deepfakes and AI-generated content, which may appear convincing even when they do not represent genuine events.

The appropriate response is not to weaken statutory safeguards or to treat electronic evidence with general suspicion, but to strengthen the process through which it is collected, preserved,

examined and evaluated. Clearer certification procedures, accessible forensic assistance, documented chains of custody, proportionate judicial scrutiny and specialised training can help ensure that procedural requirements do not become unnecessary barriers to justice. At the same time, courts must remain willing to examine credible challenges to authenticity rather than treating formal compliance as conclusive proof. Ultimately, the credibility of electronic evidence depends on more than the integrity of a digital file; it depends on the reliability of the process through which that file is brought before the court and the care with which its contents are evaluated. The objective should not be to demand technical perfection from every electronic record, but to ensure that material disputes concerning its origin, integrity and context receive appropriate scrutiny. Such an approach would preserve the evidentiary value of digital technology while reducing the risk that procedural compliance is mistaken for conclusive proof.The long-term success of the BSA will therefore depend on its practical implementation as much as on its statutory design. By combining procedural safeguards with technically informed and context-sensitive judicial assessment, India can develop an evidentiary framework that responds to technological change while protecting fairness, reliability and the administration of justice.

References

1. Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).
2. Information Technology Act, 2000 (Act 21 of 2000).
3. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
4. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
5. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
6. *Pune Bar Association v. Union of India*, W.P. (C) No. 599 of 2026 (Supreme Court of India, order dated 22 May 2026).
7. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
8. *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 SCC 178.
9. Chadha, Vaibhav, and Janani Sivaraman, "Critical Analysis of the Law on Admissibility of Electronic Evidence in India" 15(1) *Jindal Global Law Review* 119–132 (2024).Available at: https://doi.org/10.1007/s41020-024-00219-1.
10. Dalal, Abhishek, Chongyang Gao, Paul W. Grimm, Maura R. Grossman, Daniel W. Linna Jr., Chiara Pulice, V.S. Subrahmanian, and John Tunheim, "Deepfakes in Court: How

Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases" *University of Chicago Legal Forum* 75 (2024). Available at: https://chicagounbound.uchicago.edu/uclf/vol2024/iss1/3/.

11. Guttman, Barbara, Douglas R. White, Shannan Williams, and Tracy Walraven, *Digital Evidence Preservation: Considerations for Evidence Handlers*, NISTIR 8387 (National Institute of Standards and Technology, 2022). Available at: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf.
12. Romero-Moreno, Felipe, "Deepfake Detection in Generative AI: A Legal Framework Proposal to Protect Human Rights" 58 *Computer Law & Security Review*, article 106162 (2025). Available at: https://www.sciencedirect.com/science/article/pii/S2212473X25000355