ELECTRONIC EVIDENCE AND WRONGFUL CONVICTION: JUDICIAL CAUTION IN DIGITALLY DRIVEN PROSECUTIONS

Dr. Mamta Kumari, Assistant Professor, Faculty of Law, ICFAI University

Yashpreet Kaur, LL.M., Faculty of Law, ICFAI University

ABSTRACT

In Indian criminal trials, debates focus on the validity of electronic evidence and wrongful convictions as a matter of complexity, justice, and restraint. This paper discusses the Indian judiciary's position on prosecutions based on mobile data, call logs, and other digital evidence. The greatest risk is the over-reliance on modern technology by the judiciary, rather than the technology itself. The author employed a doctrinal approach to the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023, and leading cases from the Supreme Court of India to assess the jurisdictions of the admissibility of evidence, custody, and the disclosure of evidence as part of the judicial reasoning. The new laws recognize the existence of electronic material and evidence produced during the discovery process, but also acknowledge the process and require certificates, identifiers, and restrictions to the recordings of the search and seizure in the evidence collection process. The author has noted the dual approach to reasoning drafting employed by the courts in this area. The courts are addressing the issue of electronic evidence and determining the admissibility of evidence to decide the relevant value of the evidence in the case. Mohd. Arif alias Ashfaq, Rahil, Chandrabhan Sudam Sanap, and Pooranmal, are cases that critique the lack of evidence, defunct CCTV systems, and unproven claims regarding mobile communication network data. This paper relies on evidence from the 2021 to 2023 cybercrime case data from the courts, and the available cyber-policing resources, illustrating the expanding scope of digital prosecutions. The judicial system prioritizes constitutional protections over technological advancements that may lead to false convictions. In order to protect the rights of the accused, judicial procedures demand the lawful origination, substantive legal access to defend, minimal reliance on, and reasoned corroboration to electronic material that may lead to criminal convictions.

Keywords: Electronic evidence; wrongful conviction; admissibility; Section 63 certificate; proper custody; cloned copy; call detail records; cell tower location; digital forensics.

1.1 INTRODUCTION

The digital world has drastically changed the way Indian criminal courts conduct their investigations, prosecutions, and adjudications. Even the prosecutorial case file has changed; courts must now rely on mobile phone investigations, social media platform records, and video recordings along with other telecommunication case files. With the shift in available evidence, courts are faced with the need to assess the integrity, reliability, and fairness of the evidence that is being presented.[1]

Because of the perceived neutrality of electronic evidence, it is seen as more persuasive than other types of evidence. However, this perceived neutrality is a danger in and of itself. A call log cannot be taken at face value, nor can a video file, and a device extraction cannot just be assumed to be complete, untampered, and non-selective. Digital technologies are shaping the potential outcomes of criminal prosecutions; the apprehension of technology creates the possibility of wrongful convictions. The need to treat digital evidence as powerful, and to reign in the necessary overestimation of technology, is required by the constitutional guarantees of equality and justice.

The Bharatiya Sakshya Adhiniyam 2023 and Bharatiya Nagarik Suraksha Sanhita 2023 mark a new legislative milestone for Indian criminal law. These laws recognize the reality of the importance of electronic and digital records, while maintaining a legal framework for authenticity, custody, certification, and fairness. Their importance is not in how things become simpler with the use of digital evidence, but in managing the circumstances with respect to the digital evidence and the trust placed on it. In a situation where liberty is at stake, the law must recognize the difference between the data and the lawful, just, and plausible evidence of the data.[2]

This paper defends the position that the reluctance of judges to embrace digital evidence in criminal cases is not due to an archaic view of evidence but is a response to the problem of digital data, and that the nature of that data is ephemeral, digital data leading to evidence can be reconstructed and is not always the final instance of data. There appears to be a consolidated

[1] Stephen Mason, Daniel Seng, *Electronic Evidence and Electronic Signatures* 74 (University of London Press, London, 5th edn., 2021).
[2] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* 112 (Academic Press, Orlando, 3rd edn., 2011).

principle emerging in the Indian legal framework. First, the judge must examine whether that particular piece of evidence is deemed to be legally present or not. Second, the judge assesses whether that particular piece of evidence, legally or not, is sufficiently reliable to warrant a conviction. This distinction is arguably the most critical in minimizing wrongful convictions in the age of electronic evidence.

1.2 CONCEPTUAL FRAME

The doctrine of electronic evidence is highly problematic, and it is this aspect that lawyers and judges must begin to study in order to understand the doctrine of electronic evidence. Indian judiciary is not just looking at the new types of documents; they are looking at new types of reasoning documents and evidence.[3]

1.2.1 Electronic Evidence as a Composite Category

Evidence that is electronic in nature is about more than just an electronic document in the narrow sense. In criminal practice, evidence can include Closed Circuit Television footage, Digital Video Recorders exports, instant message conversations, app data, recoveries of deleted files, server logs, temporal and special data, Call Detail Records, social media images, electronic signatures, cloud storage backups, and forensic images of storage media. What unites these items is not the technology they employ; rather, the point of view of the court is that they see only the end output or end presentational form of an intricate digital chain. Because of this, legal evaluation must be tuned to the issues of authenticity, provenance, completeness, and contextuality, rather than just evaluating the document in a typical sense.[4]

It is important to distinguish the ultimate original source, the electronic output, and what the prosecution is purporting. A source may be original, yet the prosecution is relying on a copy of that source. A portion or segment may be a copy and may even be technically verifiable, but it can be misleading due to missing contextual data. A video can be true but can lack the criterion to make a conclusive identification. A location record may be genuine but may not be sufficient to demonstrate an actual presence. Flattening these distinct layers into a single assertion that 'the device is evidence of guilt' is usually the starting point of wrongful convictions. Judicial

[3] Orin S. Kerr, "Digital Evidence and the New Criminal Procedure", 105 *Columbia Law Review* 279 (2005).
[4] Digital Evidence, *available at:* https://www.nist.gov/digital-evidence (last visited on April 9, 2026).

conservatism begins by avoiding such a flattening.[5]

1.2.2 Wrongful Conviction in the Digital Setting

A conviction based on digital evidence does not require fully fabricated schemes. It can develop in a more subtle manner, one that can, in isolation, be justifiable, like seizing evidence without a documented chain of custody, an investigator who is careless in how they export evidence, a witness being led over the course of several images to choose the accused during identifications, or a judge presuming that being near a cell tower implies being near a crime. Errors of this kind, when viewed in isolation, seem inconsequential, but when put together, they can transform an assumption of guilt into a conviction in an advanced technological environment.[6]

Errors in digital evidence can spread through a case in a different manner when compared to traditional evidence. With digital evidence, a judge or lawyer may assume the digital evidence is more accurate than an eyewitness identification, when in fact the evidence is digital and the output is flawed. This may be a result of a more digital output than a more open and straightforward contentious circumstance with an identification. A digital output is often described with an extensive technical language, which discourages further questioning and, therefore, a more digital output tends to be less scrutinized than an eyewitness identification, which may also be hindered by bias or the time of the event. Digital evidence is a constructed version of reality, made by devices and software. It is less than the reality. A digital output may be so inherently flawed and may be so less representative of the reality that digital evidence can be more easily scrutinized than non-digital evidence.[7]

1.2.3 The Meaning of Judicial Caution

Judicial caution should not be confused with hostility to electronic evidence. It means more than discipline. The court must ask who controlled the device, how the data was generated, whether the output is original, secondary, or even electrical, whether statutory conditions were

[5] Electronic Evidence in Focus: Navigating Legal Shifts in the Law on Electronic Evidence Under the BSA, 2023, *available at:* https://www.scconline.com/blog/post/2024/10/23/electronic-evidence-in-focusnavigating-legal-shifts-in-the-law-on-electronic-evidence-under-the-bsa-2023/ (last visited on April 8, 2026).

[6] Brandon L. Garrett, *Convicting the Innocent: Where Criminal Prosecutions Go Wrong* 96 (Harvard University Press, Cambridge, 1st edn., 2011).

[7] C. Ronald Huff, Arye Rattner, et.al., *Convicted But Innocent: Wrongful Conviction and Public Policy* 141 (Sage Publications, Thousand Oaks, 1st edn., 1996).

met, whether the defence had meaningful access to evidence, whether the chain of custody is documented, and whether the evidence is secondary and the inference invoked by the prosecution exceeds the actual data. In criminal adjudication, caution is not optional prudence.

It is the structure of proof itself. Guilt must be proven beyond reasonable doubt, not beyond technological confidence.[8]

This idea of caution has both an evidential dimension and a constitutional dimension. The evidential dimension is caution against manipulation, incompleteness, and overstatement. The constitutional dimension is caution against unfair surprise, asymmetry of access, and a trial where the accused does not face an open and disclosed case, but a technologically curated and edited narrative. The right to fair procedure under Articles 14 and 21 is pertinent because the digital case is capable of overwhelming the defence's ability to test prosecution claims. Where the State possesses the devices, the software environment, the extraction history, and the witness infrastructure, judicial passivity can become a source of wrongful conviction.[9]

1.2.4 Why Digital Traces Are Inferential, Not Self-Proving

Usually, a digital trace on its own does not demonstrate a legally relevant fact. It proves a smaller claim from which further reasoning is expected. A call log may prove communication, but not conspiracy. A location record may demonstrate an association with a network cell, but not a physical location. A video may demonstrate movement, but not a person or purpose. A chat log may show a message, but not a person if ownership of the device and the account is in dispute. There are no digital traces in legal guilt, and each digital trace requires an inferential bridge. Judicial caution is the mechanism by which a court assesses whether those bridges exist in law and logic.[10]

The gap between authenticity and evidential weight is particularly relevant here. A record may comply with the rules of formal admissibility, but remain anaemic in its proof. On the other hand, a narrative may be technically convincing, but not meet the legal proof requirements.

[8] Gary C. Kessler, "Judges' Awareness, Understanding, and Application of Digital Evidence", 6 *Journal of Digital Forensics, Security and Law* 54 (2011).

[9] Eric Van Buskirk, Vincent T. Liu, "Digital Evidence: Challenging the Presumption of Reliability", 1 *Journal of Digital Forensic Practice* 19 (2006).

[10] New NIST Forensic Tests Help Ensure High-Quality Copies of Digital Evidence, *available at:* https://www.nist.gov/news-events/news/2017/12/new-nist-forensic-tests-help-ensure-high-quality-copiesdigital-evidence (last visited on April 7, 2026).

When a record's admissibility is confused with reliability or when digital records are sufficient to prove reliability, wrongful convictions thrive. Recent Indian case law has placed significant emphasis on the need to separate these concepts. This is the primary defence against the technologically overreached prosecution.[11]

1.3 STATUTORY FRAMEWORK

Although the new Indian statutory framework does not remove judicial discretion, it offers a clearer design. The Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023, address digital realities, but instituting procedural safeguards.[12]

1.3.1 The Bharatiya Sakshya Adhiniyam, 2023

As of July 1, 2024, the Bharatiya Sakshya Adhiniyam, 2023, is the primary legislative document governing the handling of electronic and digital records in Indian courts. The statute provides for the integration of digitally stored evidence into the Indian legal framework, and while it addresses the digital format of evidence, the statute also provides for the legal basis of evidence in a digital format. The provision is important as it rejects the law's technological exceptionalism; however, it also retains a degree of technical protection. The provision recognizes the digital reliability of records while maintaining the need for the reliability of the records to withstand legal scrutiny.[13]

While Section 57's provision on proper custody, particularly in relation to primary evidence, is appreciative, the electronic or digital record produced from proper custody is primary evidence unless discredited, which speaks to the uncertainty that was previously associated with evidence produced from the original device and its relation to the outputs of the original device. The phrase 'unless discredited' is, however, crucial. There is no presumption of trust, and if custody, integrity, or ownership, as well as extraction, and completeness are challenged, the court must still delve into the underlying factors to assess the record. Proper custody of the

[11] When Artificial Intelligence Gets It Wrong, *available at:* https://innocenceproject.org/news/when-artificialintelligence-gets-it-wrong/ (last visited on April 6, 2026).

[12] Avtar Singh, *Principles of the Law of Evidence* 88 (Central Law Publications, Prayagraj, 24th edn., 2023).

[13] Shivam Kumar Pandey, Mahammad Anas Abbashbhai Umatiya, "A Study on Admissibility of Electronic Evidence with Reference to the Provisions of the Bhartiya Sakshya Adhiniyam, 2023", 2 *Lex Scripta Magazine of Law and Policy* 1 (2024).

record is the beginning point for proof and not the endpoint.[14]

This provision also has an institutional consequence because it depends on investigators thinking about documentation at the time of seizure and not at the time of the trial. In case the prosecution wants to argue that a record was a product of proper custody, it has to prove who the custodian was, when the record was seized, the condition it was in when seized, how it was controlled, how it was prevented from being altered, and how access was restricted. For a judge who weighs matters carefully, a courtroom assertion of proper custody, without evidence, should not suffice to satisfy a claim of a diligent judge. In wrongful conviction analysis, custody failures matter because they foster the potential for change to go undetected, and leave the defendant in the position of challenging events that transpired completely within the State's controlled domain.

1.3.2 Section 63 and the Certificate Regime

Section 63 preserves the formal regime for the admissibility of electronic records where the law requires the electronic output to be certified. It requires identifying the record, describing how it was produced, specifying the device used, and addressing whether the statutory requirements were met. This is not sterile paperwork. In the digital context, the certificate plays the role of a legal translator with certificate that tells the court what the electronic output is, where it came from, and why it should be considered a reliable reflection of the underlying data.[15]

When the prosecution relies on secondary electronic evidence such as printouts, Compact Discs, pen drives, server exports, and other derived outputs (as opposed to the original device environment), the certificate requirements become critical. Without that structure, courts would be asked to accept a chain of technical transformation on mere assertion. The certificate, at least in theory, pins responsibility on a person in a position to speak about the device and the process. That responsibility is one of the limited legal mechanisms that can, in a modest way, prevent the cavalier treatment of copied digital information. For cases that rely on such technological outputs, the discipline of identification is itself a safeguard against wrongful

[14] Soni Lavin Valecha, Sonika Bharadwaj, "Admissibility of Electronic Evidence under the Indian Evidence Act, 1872", 4 *International Journal of Management and Humanities* 15 (2020).

[15] The Bharatiya Sakshya Bill, 2023, *available at:* https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023 (last visited on April 5, 2026).

conviction.[16]

The Schedule to the Bharatiya Sakshya Adhiniyam, 2023 is equally significant in that it provides a template for the certificate and specifically mentions device identifiers and hash values. This point illustrates a recognition of the fact that, while it is impossible to check the digital integrity of a device, the physical integrity of a document can be verified. A file may appear to remain unchanged, when in fact it has been modified. The statutory template relates to hash values, and in doing so, it demands a greater forensic culture of proof. The consistency of this culture may conflict with the intent of the statute, but the design of the statute is unambiguously correct. In a situation where the prosecution claims a controlled extraction or cloning framework, the careful judge should see the absence of such integrity indicators as a significant deficit.

1.3.3 Search, Seizure, and Procedural Recording under the Bharatiya Nagarik Suraksha Sanhita, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023, outlines how digital materials enter case files, affecting law on the evidence. Section 105 requires audio-video documentation of the entire search and seizure process, including preparation and signing of the seizure list, to be recorded, ideally by mobile phone, and to be sent to the Magistrate without undue delay. This is particularly relevant in case of mobile phones, storage devices, and surveillance devices as the legal and evidentiary status of digital evidence hinges on what was seized, from where, in what state, and in whose presence.[17]

Serious implementation of audio-video recording can, to an extent, eliminate a number of repeated wrongful conviction causes. It can demonstrate whether a device was switched on, whether seals were used, whether a number of devices of the same kind were present, whether there were bystanders/witnesses during the process, and whether the seizure memo was consistent with the items recorded. It allows trial courts to go beyond the oral testimonies of the investigating officers, which tend to be vague and unreliable. However, the statutory provision will be of little consequence unless courts regard unexplained non-compliance or

[16] How To Fulfill Requirements of Admissibility of Electronic Evidence Under Section 63 Bhartiya Sakshya Adhiniyam, 2023, *available at:* https://www.livelaw.in/articles/electronic-evidence-admissibility-section-63bhartiya-saksha-adhiniyam-2023-261511 (last visited on April 4, 2026).

[17] Yatindra Singh, *Cyber Laws* 157 (Universal Law Publishing, New Delhi, 1st edn., 2003).

incomplete compliance as a reason to diminish the weight of the digital evidence. A provision that is accompanied by no evidentiary impact is little more than window dressing.[18]

1.3.4 Disclosure, Defence Access, and Meaningful Contestation

Digital prosecutions fundamentally fail in fairness when the defence has limited opportunity to access the evidence the State is relying on. This is the primary disconnect concerning the wrongful conviction critique of the disclosure doctrine. When defendants receive only screen shots, transcripts, or selective exports, as opposed to fully underling electronic materials, the opportunity for independent testing diminishes. In that situation, the defence is forced to contest technical aspects without the ability to examine metadata, chain of custody, time stamps, related communications, or file properties. Such asymmetry in the process distorts the adversarial system and increases the chances the court is only presented the prosecution's version of the electronic evidence.[19]

The cloned copy phenomena in Indian laws is not a procedural perk; it is an element of structural fairness. A clone preserves the possibility of the defence considering the same material in a given state, making objections prior to charge, and exposing omissions and manipulations that would otherwise be invisible. It is almost self-evident in instances when the digital material is not merely corroborative but central. In cases that almost exclusively rely on some memory card, device extraction, or stored videos, lack of access to usable material effectively transforms the prosecution into the sole decider of the evidence, which in wrongful conviction terms is an extremely problematic monopolization of the evidence.[20]

1.4 JUDICIAL DOCTRINE

The Indian case law has evolved from a mostly interested stance to a much more responsible position in regard to digital evidence. Most of the leading decisions demonstrate a single judicial conviction; the risk is not so much in accepting the technology but in equating the technological form with the sufficient proof. This conviction is the source of the modern

[18] Farooq Ahmad Mir, *Cyber Law in India (Law on Internet)* 119 (Allahabad Law Agency, Faridabad, 7th edn., 2026).

[19] Michael Losavio, Julia Adams, et.al., "Gap Analysis: Judicial Experience and Perception of Electronic Evidence", 1 *Journal of Digital Forensic Practice* 13 (2006).

[20] Tejas Karia, Akhil Anand, et.al., "The Supreme Court of India Re-Defines Admissibility of Electronic Evidence in India", 12 *Digital Evidence and Electronic Signature Law Review* 33 (2015).

expression of caution.[21]

1.4.1 Anvar P.V. v. P.K. Basheer and the Structure of Admissibility

The most significant doctrinal turning point is *Anvar P. V. v. P. K. Basheer*[22], the case treats the proof of electronic records as a separate area regulated by specific statutory provisions as opposed to a boundless area governed by the law of secondary documentary evidence. The case is important, not just in requiring a certificate for certain types of electronic outputs, but in requiring the courts to ask a preliminary question, before not being able to see the contents, relating to whether the record before the court has been legally journeyed; The case, in that sense, reintroduced evidentiary humility in a domain that is characterized by technological overconfidence.

Anvar's deeper significance lies in the fact that it refused to permit convenience to compromise the proof of the case. Electronic records can be easily copied, edited, segmented, reformatted, and transmitted. If courts were able to receive such outputs without the specialized threshold, the prosecution would be allowed to circumvent the important questions regarding the source of the evidence, the integrity of the evidence, and the circumstantial evidence as it paved the way for the proof path. This is fundamental to wrongful conviction analysis. A person should not have their liberty severely restricted merely because the state finds it convenient to provide a print out or storage device without determining, legally, what that output is and how it came to be.

1.4.2 Shafhi Mohammad v. State of Himachal Pradesh and the Temporary Relaxation

The subsequent ruling in *Shafhi Mohammad v. State of Himachal Pradesh*[23], shows greater latitude by stating that, in some circumstances, the certificate requirement may be removed as a matter of form, especially when the certificate is a matter of the party's control. While the pragmatic response is reasonable, it risks turning a carefully crafted admissibility rule into a discretionary afterthought. When exceptions are made, investigators and prosecutors are provided less incentive to obtain the necessary certification at the proper time.

[21] Changing Facades of Law on Admissibility of Electronic Evidence, *available at:* https://www.scconline.com/blog/post/2021/03/13/electronic-evidence/ (last visited on April 3, 2026).
[22] (2014) 10 SCC 473.
[23] (2018) 2 SCC 801.

The Shafhi Mohammad case is problematic for wrongful conviction cases not because of a lack of consistency, but because it communicates the idea that the courts might overlook a problematic evidentiary basis for some degree of judicial activism. In criminal cases, this ambiguity works in favour of the prosecution. The accused seldom has control over the device, the service provider, or the extraction process. Relaxing the standard requirements in the name of practicality creates an unbalanced burden. Imposing an incomplete case on the defendant, after the process has shaped the judicial view, is clearly contrary to the interests of justice.

1.4.3 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Doctrinal Consolidation

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[24], the three-judge bench reinstated doctrinal clarity by reaffirming *Anvar P. V. v. P. K. Basheer*[25] and nullifying the opposing direction of Shafhi Mohammad. The Court stated that where the original device itself is produced, the need for a certificate may not arise in the same way, but when the court is asked to rely on secondary electronic output, the statutory path must be followed. This clarity is necessary as it blurs two different evidentiary situations rather than just looking at the electronic modernity aspect.

The Court's view that a judge may, in an appropriate case, be able to assist in the making of a certificate where the individual trying to rely on the material has, in good faith, requested it from the appropriate authority and has been denied is of equal importance. This dimension retains the practicality of the doctrine without unworking its essence. The judgment preserves practical difficulty as an informal proof. The outcome is a judicious mix of equity and practicality. In wrongful conviction terms, Arjun Panditrao Khotkar is significant because it upholds that the State's technological case must be legally sound.

1.4.4 Sonu Alias Amar v. State of Haryana and the Timing of Objection

The case of *Sonu alias Amar v. State of Haryana*[26], is mostly described as a case about the law's procedural aspects. However, it is also very relevant for issues about fairness in the criminal justice process. The Supreme Court was prepared to consider the absence of a certificate as a

[24] (2020) 7 SCC 1.
[25] (2014) 10 SCC 473.
[26] (2017) 8 SCC 570.

challenge to the 'mode of proof', which is an objection that is usually taken when the electronic record is submitted and marked. Positive proof is served when the objection is taken at the correct time. This means that the trial judge is able to insist on this compliance and the prosecution is not able to complain later that the case was not given the opportunity to correct a deficiency of obedience to a rule.

The rule also has a learning consequence for trial judges. Judges must not simply sit back, as they do in other types of court process, and regard the marking of electronic records in serious criminal cases to be case closure, then leave below the foundation of issues to be debated later, possibly years, on an appeal. The prosecution being able to tender a record that is primarily reliant on digital technology means that there is a need for the judge's control and active supervision at the time of filing. Judges should be asking questions about whether the record is an original or secondary one, whether a legal foundation exists, and whether the defence has an opportunity to address the questions. When these questions are not addressed, it is likely that the trial proceeds on the basis of assumptions that are inappropriately evidential, and that is how the problem of wrongful convictions becomes institutionally embedded before we commence further appellate control.

1.4.5 Tomaso Bruno v. State of Uttar Pradesh and the Best Evidence Principle

In the case of *Tomaso Bruno v. State of Uttar Pradesh*[27], the Supreme Court doe notice the importance of electronic and scientific evidence and suggests that an adverse inference could occur if one fails to produce the best evidence available in an electronic form. It is true that later developments have sought to limit aspects of this decision to the certificate issue. However, the case still maintains commendable breadth and importance regarding the instinct of the evidence. It buttresses the courts in saying that the absence of electronic technological evidence should have some substantial meaning. If a prosecuting or investigating agency is sure of something but fails to obtain or show the equally important electronic evidence, like a video tape recording of the incident, the absence of that evidence should determine a case with respect to the degree of judicial confidence.

The importance of Tomaso Bruno should still be about the case as one of the primary sources of the importance of the investigation that goes together with the verification of the electronic

[27] (2015) 7 SCC 178.

evidence. The judgment in relation to the later cases should be more in line with the restriction to reject the electronic evidences that might be available, but to appreciate the fact the needed electronic evidence should have been collected and, where appropriate, to deducted to demonstrate the importance of the evidence in relation to the case. In relation to wrongful conviction, this case goes both ways. It speaks against conviction in the absence of the best available evidence, and it also speaks against evidence that is digitally available as a substitute to the evidence that is missing.

1.4.6 P. Gopalkrishnan v. State of Kerala and Defence Access to Digital Material

The case *P Gopalkrishnan v. State of Kerala*[28] highlights the electronic evidence components of the fair trial. The Court noted that while the prosecution seeks to prove evidence through electronic means such as a memory card or a pen drive, the accused must, with some safeguards, be provided the content in a cloned copy. This is a crucial decision because it moves the discussion from the question of the abstract admissibility to the question of the concrete adversarial fairness. If a digital case is to be fairly contested, both sides must be able to access the evidence in the usable form.

This principle is directly linked to the fight against wrongful convictions. In the absence of cloned access, the accused loses the opportunity to analyse the evidence in terms of the continuity, metadata, timestamps, sequencing, and the omitted surrounding contexts. The narrative of the prosecution becomes the record by default. That is not a trial in adversarial form, but a recital of technological outcomes in a controlled manner. P. Gopalkrishnan should be viewed as more than a case of disclosure. It is about the principle that digital evidence should be contestable. In a trial system that also seeks to safeguard the rights of defendants, contestability must not be viewed as an add-on after evidence is presented.

1.4.7 Mohd. Arif Alias Ashfaq v. State (National Capital Territory of Delhi) and Capital-Level Caution

An important statement of caution can be found in *Mohd. Arif alias Ashfaq v. State (National Capital Territory of Delhi)*[29], review proceedings decided on November 3, 2022. In this case, the Supreme Court remarked that, in the review of the death sentence, evidence in the form of

[28] (2020) 9 SCC 161.
[29] 2014 (9) SCC 737.

uncertified Call Detail Records should be avoided. This review is important because it shows that the Supreme Court in this case review Deficient Legislation, regarding the use of electronic evidence, which is all the more important in the case of irreversible legal consequences. This case shows that, when a person's freedom is at stake, the technical correctness of the proof becomes irrelevant.

This case illustrates the most important aspect of wrongful conviction. The essence of wrongful conviction is not in the wait, but in review proceedings where uncertified electronic evidence has already been interpreted as guilt. By instructing to keep such materials out of consideration, the Court recognizes the fact that electronic evidence, even when it is established, should not be used to substantiate illegal conclusions. The case has a very clear message. Where the digital infrastructure is illegal, the charge is not justified by the wrongful conviction. On the contrary, the weight of the charge is a justification for more caution, not less.

1.4.8 Rahil and Another v. State (Government of National Capital Territory of Delhi) and the Limits of Location Inference

The 2025 decision in *Rahil and another v. State (Government of National Capital Territory of Delhi)*[30], is a good example of a decision illustrating the perils of inferential overreach. The Supreme Court held that secondary electronic records pertaining to Rahil were not admissible where there were trial objections and the prosecution left the objections unrectified. The Court went further to advise that cell tower records show only the approximate operational area of a tower, not the specific location of the device. The Court cautioned that connection to a single tower is dangerous evidence to demonstrate presence.

For purposes of assessing wrongful conviction, this line of reasoning is particularly valuable, as it describes a typical prosecutorial tendency. Location records are often described in imprecise language, as though network connectivity fuses presence with cartographic accuracy. The Court rejected that narrative. Importantly, the Court noted that the range of a tower is subject to many variables and that triangulation is more precise, whereas singular tower inference is a less precise method. As a result, the decision demands that judges be careful to differentiate approximate technological evidence from legal evidence of presence to a standard of beyond reasonable doubt. This is a distinction that should be adopted in all location-based

[30] 2025 INSC 858.

prosecutions.

1.4.9 Chandrabhan Sudam Sanap v. State of Maharashtra and the Fragility of Closed Circuit Television Identification

In *Chandrabhan Sudam Sanap v. State of Maharashtra*[31], the Supreme Court dealt cautiously with Closed Circuit Television footage. Even while dealing with arguments about admissibility, the Court was concerned with the prosecution's chances of securing a conviction and, therefore, whether the footage, if it were copiable, added some value. The answer was de facto negative. The Court described the unclear circumstances of the seizure of the footage, the use of the footage, the witnesses not seen, the absence of the footage, forensic proof, and the evidence which could not establish that the dead and the accused were in the same frame of the footage, and could not establish that they were both dead.

Judgments in other legal systems should separate visual suspicion from legal proof. The Court noted that psychological force about video material, as opposed to other materials, is that it presents the event 'live' to the judge, in the courtroom. The Court, however, acknowledged the absence of video footage from actively demonstrating accountability and responsibility. For wrongful conviction scholarship, Chandrabhan Sudam Sanap is a case of video not selfauthenticating, self-narrating, and self-interpreting.

1.4.10 Sameer Sandhir v. Central Bureau of Investigation and the Limits of Procedural Accommodation

The *Sandhir v. CBI*[32], sets out the parameters of procedural accommodation without evidentiary relaxations. The Supreme Court, in this case, allowed the late filing of case-related Compact Discs, which were referred to in the case records but were not previously filed. The Court, however, left the questions of authenticity and validity of the certificate unaddressed and permitted the recall of prosecution witnesses for the limited purpose of cross-examination on that digital issue. The unaddressed questions are important. One procedural issue in this case demonstrates that the Court can deal with procedural intricacies without conferring presumptive evidentiary value on electronically stored information simply by virtue of being

[31] 2025 INSC 116.
[32] 2025 SCC OnLine SC 776.

filed late.

For the purpose of wrongful conviction, the case illustrates the point that the unfairness of a case should not be determined by the digital information present in the case, whether it should be filed or disregarded completely. The fairness of the case should be assessed by the opportunity it provides to the defence to independently verify and challenge the information after it has been produced. In this case, the Court differentiated between the filing of the Compact Discs and an assumption that they were authentic and legally verifiable; thus, that distinction should be adopted in all similar cases. In information technology-related cases, the lack of digital information should not be confused with procedural unfairness, nor should the presence of digital information be taken as an automatic endorsement of the case. Otherwise, the mere presence of digital information could lead to presumed evidentiary value, without thorough scrutiny of the information.

1.4.11 Pooranmal v. State of Rajasthan and the Refusal to Replace Statutory Proof with Oral Narrative

Pooranmal v. State of Rajasthan and another[33], is an important recent case on the issue of strict caution. The Supreme Court stated that in the case of the appellant, the prosecution was based on recoveries and Call Detail Records. It reiterated that electronic evidence is easily manipulatable and that oral evidence does not replace evidence that is not mandated by the legal requirements of admissibility. Legally, the digital evidence was not sufficient to uphold the conviction. The consequence was that the accused was acquitted. This judgment applies valid criticism to the prosecution's criticism of an absence of documentary proof.

The most important aspect of Pooranmal is that it does not allow the seriousness of the charge to stand behind evidential informality. It is common for courts to overlook evidential deficiencies of technicalities in cases where the context is disturbing. The judgment does not yield to that instinct. It is not ornamental to have compliance in criminal justice. It is one of the things that stand to protect against wrongful convictions. When the State wants to use technological records to presuppose guilt, it must legally satisfy the requirements of those records. The oral account of defective evidence cannot convert suspicion to conviction.

[33] 2026 INSC 217.

1.4.12 The Emerging Doctrine

When analysed collectively, these decisions demonstrate a level of doctrinal maturity. Courts recognize the digital materials offer evidence, but are less tolerant of reductive reasoning. The law differentiates original devices from secondary outputs, admissibility from probative value, communication from conspiracy, approximate range from exact presence, suspicion from identification, and other such distinctions. Each of these distinctions reduces the scope within which wrongful convictions can occur. The concern here is straightforward. The restraint shows a concern which digital evidence must be lawfully proven and rationally constructed.[34]

The latest method is proof. The nature of digitally enabled prosecution is that it is unlikely to recede. With every new prosecution, there is increased pressure on the courts to regard electronic records as the best or most objective evidence. These cases illustrate the point. Digital records, themselves, should be treated as contestable, contextual, and corroborated. The fact of their digital form does not exempt them from the criticism of the criminal law that conviction should result only from the combination of lawful proof, rational inference, and an adequate degree of determination.[35]

1.5 WRONGFUL CONVICTION RISKS, DATA

The conviction risk does not stem from a singular doctrinal shortcoming. It arises from the amalgamation of a culture of disclosure, evidentiary elements, police behaviour, courtroom behaviour, and the institutional aura of reverence to technology, especially, the 'poor technologies' in the domain of criminal law. Any meaningful consideration of electronic evidence must therefore explore the intersection of the various elements in play.[36]

1.5.1 Chain of Custody and the Problem of Invisible Alteration

The exposure in a traditional evidence system, is quite the reverse. A technology evidence file may have been altered in many ways, but the lapses may not be obvious and there may be a

[34] From Anvar To Arjun - A Tale of Two "Anys" & Other Stories, *available at:* https://www.livelaw.in/columns/from-anvar-to-arjun-a-tale-of-two-anys-other-stories-157264 (last visited on April 5, 2026).

[35] Rahil and Another v. State (Govt. of N.C.T. of Delhi), *available at:* https://www.supremecourtcases.com/rahil-and-another-v-state-govt-of-n-c-t-of-delhi-3/ (last visited on April 4, 2026).

[36] C. Ronald Huff, Martin Killias, *Wrongful Convictions and Miscarriages of Justice: Causes and Remedies in North American and European Criminal Justice Systems* 187 (Routledge, London, 1st edn., 2013).

swift avoidance of accountability. The nature of digital evidence is that there can be obvious lapses and it is thinner than the traditional evidence. For this reason, the chain of custody should not be a formality. The nature of digital evidence is that custody should rather be the main concern because it should indicate to the court that the evidence should be what it is. It, therefore, is the concern that should lead the court to a guilty outcome and not a justice outcome if the evidence is lives.[37]

The risk increases when investigators interact with the device prior to applying forensic aids to the device. For example, investigators potentially impact questions of completeness and integrity by accessing the device, viewing content, sending files, taking screenshots, or replaying videos. The court should be concerned if there is a lack of clarity about the condition of the device, the chain of access, the method of extraction, and the documented steps taken to secure the device. If these elements are absent, the prosecution's version of the technology is likely to be unverifiable. The risk of wrongful conviction increases because the court relies on a dataset with unknown transformation history. Digital evidence that lacks provenance is often a feigned technical obfuscation.[38]

1.5.2 Selective Extraction and Narrative Curation

Selective extraction is another common risk. Investigators may be biased in producing only certain chats, snippets, images, or entry logs that align with their theory of the case, omitting other material that's crucial to understand the context. A message may seem incriminating when taken out of context, and a video clip may seem threatening without the earlier footage that reveals the context. The architecture of digital storage allows such selection, and the architecture of criminal suspicion makes it a temptation. Therefore, judicial caution must include an awareness that prosecution exhibits, as a rule, may be edited and cut exhibits rather than complete records.[39]

Closed-copy principle becomes significate in lessening curation and contestation asymmetry. For the Defence, having access to the material in use means that selective extraction becomes

[37] Eoghan Casey, "Error, Uncertainty, and Loss in Digital Evidence", 1 *International Journal of Digital Evidence* 1 (2002).
[38] Catherine L. Bonventre, "Wrongful Convictions and Forensic Science", 3 *WIREs Forensic Science* 1 (2021).
[39] Best Practices for Digital Evidence Collection, *available at:* https://www.swgde.org/documents/publishedcomplete-listing/18-f-002-best-practices-for-digital-evidence-collection/ (last visited on April 3, 2026).

easier to demonstrate through cross examination and expert assistance. If not, the prosecution's selective presentation may become the only reality that the court sees. Within the context of wrongful conviction, selective extraction is the most insidious as it rarely appears to be fabrication. Rather it appears to be organised, efficient, focused on the evidence. Yet, it may, in substance, distort meaning as much as an outright falsehood. Therefore, the court must examine the electronic exhibit not only for the possibility of alteration, but also for the possibility of omission.[40]

1.5.3 Overclaim from Location, Identity, and Device Association

Judges in India have become more alert to the fact that digital evidence supports only certain propositions but there is appreciable evidence of over claiming in the investigations and prosecutions. A recurring assumption is that, a person who is in possession of a mobile phone at the relevant time is the user of the phone, and a user of a mobile phone is located in a given area is present at that location, and that an image of a person in a television picture is the person that an investigator is searching for. All these assumptions collapse an entire chain of evidence into a single proposition. This may have the unintended and dangerous consequence of exaggerating the evidence.[41]

The problem will not be resolved simply by saying that the court will "consider the totality of circumstances". Meaningful totality only happens when each of the individual circumstances is assessed in a reasonable manner. A weak location inference does not become a strong one just because it is accompanied by a weak visual identification and a weak association claim. Three uncertainties do not automatically equate to a certainty. In the digital cases, they may in fact just reinforce one another through a false sense of convergence. Judicial restraint necessitates a more rigorous approach. Each digital connection should be scrutinized as to

whatever it proves. Only then can the court consider whether the rest of the chain is sufficiently complete to warrant a conviction.[42]

---

[40] Digital Evidence Preservation: Considerations for Evidence Handlers, *available at:* https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-programme-cftt/digitalevidence (last visited on April 2, 2026).

[41] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 73 (New York University Press, New York, 1st edn., 2004).

[42] Stephen Mason, Daniel Seng, *Electronic Evidence* 97 (Institute of Advanced Legal Studies for the SAS Humanities Digital Library, London, 4th edn., 2017).

The following table presents an official all-India cyber-crime case flow snapshot for the years 2021 to 2023. While it does not measure wrongful convictions, it illustrates the increasing scale of prosecutions based on electronic investigations, digital records, and case-building in contemporary India.

Year	Cases Registered under Cyber Crimes	Cases Charge-Sheeted under Cyber Crimes	Cases Convicted under Cyber Crimes
2021	52,974	18,744	491
2022	65,893	18,925	1,118
2023	86,420	20,526	886

Table 1: All-India cyber-crime case flow, 2021 to 2023.

The table is appropriate for a bar chart, line chart, clustered column chart, or a pie chart depicting the distribution by years. Its primary purpose should be to illustrate the increasing scale of digital prosecutions, although the numbers should not be interpreted as the conviction rate for the respective years.

In India's criminal justice system, the number of registered cyber-crimes increased from 52,974 in 2021 to 86,420 in 2023. This speaks to the growing entrenchment of the criminal justice system into electronic technologies. This expansion of recorded crimes is consequential for the justice system's reliance on the same investigative ecosystem, consisting of device seizure, digital tracing, platform coordination, extraction reports, and electronic documentation, that is influencing more routine criminal cases. As digitally mediated evidence carves out more space within multiple case categories, the demand on courts to handle the authenticity and inferential scrutiny becomes acute. A more active use of digital technologies for prosecution does not ipso facto result in enhancements of justice. Without the appropriate scaling, the nature of systemic error can be aggravated.

The gap between registered cases and cases that resulted in a conviction is significant, but caution is warranted. These numbers are not a straight conviction ratio, as registration,

chargesheeting, and conviction fall under different case types. Nonetheless, this is another case large front-end digital case generation compared to a recorded conviction. Courts should be concerned with early-stage digital suspicion claims from prosecutors. If a system is based on extensive electronic allegations, the risk is that tech-infused investigations will outrun the actual evidence required to support a conviction.

Digital caution is easier to preach than to practice, which is why institutional capacity is important. The next table analyzes official state-level data on cyber-crime police stations, focusing on the top ten states with the most stations. The numbers serve as a general indicator of the density of digital investigation infrastructure.

Rank	**State**	**Number of Dedicated Cyber Crime Police Stations**
1	Uttar Pradesh	75
2	Tamil Nadu	54
3	Maharashtra	47
4	Bihar	44
5	Gujarat	39
6	West Bengal	36
7	Rajasthan	34
8	Haryana	29
9	Kerala	20
10	Odisha	15

Table 2: Top ten states by dedicated cyber-crime police stations, as on 1 January 2024.

The data in this table could be presented as a bar chart or a proportional share chart. In terms of analysis, the purpose is minor but significant. It points out the geography of digital policing capacity, which in turn affects the quality of evidence collection, data extraction, case

preservation, and prosecution support available to criminal cases in different jurisdictions.

Capacity tables create illusions. More specialized police stations do not make better evidence, and fewer stations do not make weaker investigations. Still, institutional distribution matters. Where specialized capacity is limited, officers may workaround interpretation, incomplete documentation, or ad hoc stream device handlings. Where capacity is strong, the danger may shift from reinforcement to overconfidence in technical process. Either way, the risk of wrongful conviction is present. What changes is its form. In one setting, the problem may be simple processing. In another, it may be polished but under-scrutinized digital assertions that the court regards as professionally infallible.

The risk is that judicial scepticism can be too reliant on the evident self-assurance of the investigative agency. There must be a suitable process verifying the agency's digital claims, which is a domain of certainty. A specialized unit may still fail to preserve continuity. A certified output may still prove too little. A professionally presented extraction may still omit exculpatory context. It is not the data on the institutional expansion of the evidence that matter, but the framework within which such evidence is certain, or better, the institutional setting that is lacking. As India continues to expand its digital policing, the courts must, in turn, expand their digitally grounded legal scepticism.

1.6 CONCLUSION

The outcome of this debate should not be that all electronic evidence untrustworthy. There is a larger issue of electronic evidence being susceptible to untrustworthy evidence. Because evidence is perceived to be exact, it can be forgotten that evidence is handled by people throughout the processes of collection, storage, certification, extraction, and interpretation. The evidence can also be subject to the influence of advocates. The courts should be cautious because of the illusion of infallibility.[43]

The Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023 demonstrate how Indian Law has progressed. They address the evidence and its electronic form, but they also maintain a balance between the right to proof and the integrity of the

[43] Jon B. Gould, Richard A. Leo, "One Hundred Years Late: Wrongful Convictions After a Century of Research", 100 *Journal of Criminal Law and Criminology* 825 (2010).

process. In the case of *Anvar PV v. PK Basheer*[44], and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[45], the Supreme Court has insisted that evidence should be electronically assessed, but with moderate and cautious approaches.

This doctrinal trend should be viewed from an anti-wrongful conviction perspective. It imposes on the courts the responsibility to ascertain whether the record has been proven lawfully, whether the record's integrity is certified, whether the defence had available effective access, whether the inference is reasonable and logical, and whether the technological indicator is approximate, fragmentary, or corroborated, and other corroborated elements. None of those questions obstruct justice. They make justice attainable. A digital prosecution that lacks the strength to withstand those questions is not a strong digital prosecution that is unfairly burdened by the so-called technicality. It is a prosecution that has not yet earned a conviction.[46]

The final normative observation is brief. Judicial prudence is not anti-technology in the digital era. It is pro-precision, pro-fair trial, and pro-constitutional criminal law. A judge who carefully examines electronic evidence is not anti-technology; he or she is pro-law. When judges succumb to the prestige of the data, there is a high likelihood of wrongful convictions. When judges do not succumb to the prestige of data, wrongful convictions become unlikely. Every digital record should be scrutinized so that the consequences of losing someone's life or liberty are not taken lightly.

1.7 SUGGESTIONS

The issues addressed in this paper show that prosecutions that rely on digital traces demand a higher standard of control by the judiciary from the time of seizure to the time of final judgment.[47]

1. There ought to be a uniform digital-seizure record, detailing the description and condition of the device, whether it is locked, cellular SIM card information, the time and location of the seizure, sealing information, and all officers who have interacted

[44] (2014) 10 SCC 473.
[45] (2020) 7 SCC 1.
[46] Samuel R. Gross, Barbara O'Brien, "Frequency and Predictors of False Conviction: Why We Know So Little, and New Data on Capital Cases", 5 *Journal of Empirical Legal Studies* 927 (2008).
[47] Chain of Custody, *available at:* https://www.swgde.org/glossary/chain-of-custody/ (last visited on April 1, 2026).

with the device, to support a chain of custody assertion, along with contemporaneous documentation. Custody claims should be testable with contemporaneous documentation.

2. The trial courts should consider the absence of the BNSS audio-video recording as an evidentiary weakness, especially when unrecorded search and seizure took place. Where an unrecorded search and seizure took place, the trial courts should lower the evidentiary weight of the digital exhibit.

3. Prosecutors should provide the cloned copies, extraction logs, and hash reports relating to electronic evidence, even before the charges are laid. This is particularly important, as evidence relating to the electronic data is crucial, and the defenses ability to challenge the evidence is often limited because of issues relating to voluntary screenshots, transcripts, and edited clips.

4. The courts should conduct a preliminary hearing, especially if the prosecution heavily relies on secondary electronic evidence. This hearing should clarify whether the record is original, whether the Section 63 certificate is complete, who created the record, and whether the defence has had an opportunity to access the record.

5. When adjudicating digital cases, steps should be followed in this order: admissibility, integrity, how precise the proposition proves, and last the inferential weight. If this order is maintained in judgments, it will be impossible for a judge to justify the existence of a file and conclude the accused is guilty without further justification.

6. The legal process is most accurate in making pinpoint evaluations on call detail records and cell-site evidence where the qualification is done by a technology expert on the dataset's scope. Presence claims that rely solely on a location record should be assessed much more cautiously, especially where the state fails to sufficiently justify the method and its scope of the inferences of the case.

7. The credibility of identification by means of CCTV should be given utmost consideration. Courts should ensure that the image quality is acceptable, the continuity of the sequence is maintained, the exposure is correct, the footage itself is preserved, and the footage underwent forensics analysis. If there's no witness able to situate the

accused and the victim in the sequence, the footage is not entitled to take the prime place; it should only be treated as corroborative.

8. The rule makers should consider a uniform approach that links the digital evidence certification and witnessing modules to device identifiers and hash values. A model is needed to ease the judge's burden of dissecting a digital evidence preservation and certification that, despite the police's diverse units, lacks depth and fall more on the side of being a generic certificate.

9. Experts of digital forensics should be included in tunnels of state legal-aid system to assist in serious prosecutions, especially at the early stages. If only the investigatory body understands the technical descriptions, tools, workflows, and design that produced the evidence, the rights to stand and cross-examine become meaningless.

10. The judiciary and the NCRB should collaborate on the study of acquittals and appellate reversals in cases which involved electronic evidence. A systematic database of mistakes with the certification, evidence custody, faulty location data, and video identification defects would allow the judiciary to transform recurrent issues into training, practice directions, and reforms of a measurable scope.

BIBLIOGRAPHY

PRIMARY SOURCES

1. Statutes

- The Bharatiya Nagarik Suraksha Sanhita, 2023
- The Bharatiya Sakshya Adhiniyam, 2023

SECONDARY SOURCES

2. Books

- Garrett, B. L., *Convicting the Innocent: Where Criminal Prosecutions Go Wrong* (Harvard University Press, Cambridge, 1st edn., 2011).
- Huff, C. R., Rattner, A., et al., *Convicted But Innocent: Wrongful Conviction and Public Policy* (Sage Publications, Thousand Oaks, 1st edn., 1996).
- Huff, C. R., Killias, M., *Wrongful Convictions and Miscarriages of Justice: Causes and Remedies in North American and European Criminal Justice Systems* (Routledge, London, 1st edn., 2013).
- Mason, S., Seng, D., *Electronic Evidence* (Institute of Advanced Legal Studies for the SAS Humanities Digital Library, London, 4th edn., 2017).
- Mason, S., Seng, D., *Electronic Evidence and Electronic Signatures* (University of London Press, London, 5th edn., 2021).
- Mir, F. A., *Cyber Law in India (Law on Internet)* (Allahabad Law Agency, Faridabad, 7th edn., 2026).
- Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Academic Press, Orlando, 3rd edn., 2011).
- Singh, A., *Principles of the Law of Evidence* (Central Law Publications, Prayagraj, 24th edn., 2023).
- Singh, Y., *Cyber Laws* (Universal Law Publishing, New Delhi, 1st edn., 2003).
- Solove, D. J., *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, New York, 1st edn., 2004).

3. Articles

- Bonventre, C. L., "Wrongful Convictions and Forensic Science", 3 WIREs Forensic Science 1 (2021).
- Casey, E., "Error, Uncertainty, and Loss in Digital Evidence", 1 International Journal of Digital Evidence 1 (2002).
- Gould, J. B., Leo, R. A., "One Hundred Years Late: Wrongful Convictions After a Century of Research", 100 Journal of Criminal Law and Criminology 825 (2010).
- Gross, S. R., O'Brien, B., "Frequency and Predictors of False Conviction: Why We Know So Little, and New Data on Capital Cases", 5 Journal of Empirical Legal Studies 927 (2008).
- Karia, T., Anand, A., et al., "The Supreme Court of India Re-Defines Admissibility of Electronic Evidence in India", 12 Digital Evidence and Electronic Signature Law Review 33 (2015).
- Kerr, O. S., "Digital Evidence and the New Criminal Procedure", 105 Columbia Law Review 279 (2005).
- Kessler, G. C., "Judges' Awareness, Understanding, and Application of Digital Evidence", 6 Journal of Digital Forensics, Security and Law 54 (2011).
- Losavio, M., Adams, J., et al., "Gap Analysis: Judicial Experience and Perception of Electronic Evidence", 1 Journal of Digital Forensic Practice 13 (2006).
- Pandey, S. K., Umatiya, M. A. A., "A Study on Admissibility of Electronic Evidence with Reference to the Provisions of the Bhartiya Sakshya Adhiniyam, 2023", 2 Lex Scripta Magazine of Law and Policy 1 (2024).
- Valecha, S. L., Bharadwaj, S., "Admissibility of Electronic Evidence under the Indian Evidence Act, 1872", 4 International Journal of Management and Humanities 15 (2020).
- Van Buskirk, E., Liu, V. T., "Digital Evidence: Challenging the Presumption of Reliability", 1 Journal of Digital Forensic Practice 19 (2006).

4. Websites

- Best Practices for Digital Evidence Collection, available at: https://www.swgde.org/documents/published-complete-listing/18-f-002-bestpractices-for-digital-evidence-collection/ (last visited on April 3, 2026).

- Chain of Custody, available at: https://www.swgde.org/glossary/chain-of-custody/ (last visited on April 1, 2026).

- Changing Facades of Law on Admissibility of Electronic Evidence, available at: https://www.scconline.com/blog/post/2021/03/13/electronic-evidence/ (last visited on April 3, 2026).

- Digital Evidence Preservation: Considerations for Evidence Handlers, available at: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testingprogramme-cftt/digital-evidence (last visited on April 2, 2026).

- Digital Evidence, available at: https://www.nist.gov/digital-evidence (last visited on April 9, 2026).

- Electronic Evidence in Focus: Navigating Legal Shifts in the Law on Electronic Evidence Under the BSA, 2023, available at: https://www.scconline.com/blog/post/2024/10/23/electronic-evidence-in-focusnavigating-legal-shifts-in-the-law-on-electronic-evidence-under-the-bsa-2023/ (last visited on April 8, 2026).

- From Anvar To Arjun - A Tale of Two "Anys" & Other Stories, available at: https://www.livelaw.in/columns/from-anvar-to-arjun-a-tale-of-two-anys-other-stories157264 (last visited on April 5, 2026).

- How To Fulfill Requirements of Admissibility of Electronic Evidence Under Section 63 Bhartiya Sakshya Adhiniyam, 2023, available at: https://www.livelaw.in/articles/electronic-evidence-admissibility-section-63-bhartiyasaksha-adhiniyam-2023-261511 (last visited on April 4, 2026).

- New NIST Forensic Tests Help Ensure High-Quality Copies of Digital Evidence, available at: https://www.nist.gov/news-events/news/2017/12/new-nist-forensic-testshelp-ensure-high-quality-copies-digital-evidence (last visited on April 7, 2026).

- Rahil and Another v. State (Govt. of N.C.T. of Delhi), available at: https://www.supremecourtcases.com/rahil-and-another-v-state-govt-of-n-c-t-of-delhi3/ (last visited on April 4, 2026).

- The Bharatiya Sakshya Bill, 2023, available at: https://prsindia.org/billtrack/thebharatiya-sakshya-bill-2023 (last visited on April 5, 2026).

- When Artificial Intelligence Gets It Wrong, available at: https://innocenceproject.org/news/when-artificial-intelligence-gets-it-wrong/ (last visited on April 6, 2026).