INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 11 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

RELEVANCE OF EVIDENCE IN INDIA'S DIGITAL ERA: INNOVATIONS, LEGAL CHALLENGES, AND SDG ALIGNMENT

AUTHOR - ANJALI YADAV, STUDENT AT LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY

BEST CITATION – ANJALI YADAV, RELEVANCE OF EVIDENCE IN INDIA'S DIGITAL ERA: INNOVATIONS, LEGAL CHALLENGES, AND SDG ALIGNMENT, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (11) OF 2025, PG. 161-169, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

In an age where bytes often speak louder than witnesses, India's courts find themselves at the crossroads of tradition and innovation. Digital footprints, from blockchain-etched timestamps to AI-decoded voiceprints, are increasingly the linchpin of legal narratives, yet they carry both the promise of crystalline transparency and the peril of algorithmic obfuscation. This paper embarks on a journey through India's evolving evidence landscape, tracing the contours of recent statutory overhauls (the Bharatiya Sakshya Adhiniyam, 2023; Digital Personal Data Protection Act, 2023) and landmark judgments (from *Anvar P.V.* to *Arjun Panditrao Khotkar*) that oscillate between procedural rigor and pragmatic flexibility. We spotlight cutting-edge forensic infrastructure, from blockchain-backed chain-of-custody apps in Delhi to National Cyber Forensic Laboratories born of the Nirbhaya initiative, and interrogate how AI-driven analysis both accelerates investigations and raises new questions of bias and "black-box" opacity. By weaving comparative threads from U.S. Daubert criteria to UK accreditation standards, and aligning our findings with Sustainable Development Goals, especially the quest for just, inclusive institutions (SDG 16) and resilient innovation ecosystems (SDG 9), we propose a roadmap for a "forensically enabled" justice system. Our recommendations blend legislative clarity, judicial tech-literacy, and cross-border data pacts into a cohesive blueprint: one that ensures digital evidence illuminates truth rather than obscures it, safeguarding both the scale of technological progress and the sanctity of due process.

Introduction

India's legal system is undergoing a profound transformation as digital evidence replaces traditional artifacts of truth. Today, disputes are often decided not by physical documents or eyewitnesses alone, but by algorithms, metadata, and encrypted logs. This "digital adjudication" raises a core question: can Indian courts keep pace with the speed and complexity of electronically generated evidence? The urgency is stark: over 50 million cases are pending across India's courts, straining an antiquated framework that relies on colonial-era statutes. In response, India recently overhauled its evidence law (the *Bharatiya Sakshya Adhiniyam, 2023*) and enacted a new data-protection statute, signaling a push toward modernization. Yet, practical adaptation lags. Indian courts continue to grapple with issues like cross-border data access, privacy safeguards, and the authenticity of AI-generated media (deepfakes).

In this context, technological innovations, from blockchain to artificial intelligence to advanced digital forensics, promise both solutions and new dilemmas. For example, immutable blockchains and cryptographic hashes could render evidence tamper-proof, but courts must still decide the evidentiary weight of such logs. Similarly, AI can expedite legal research and forensic analysis, but it also embeds hidden biases and raises "black box" concerns. This paper offers an integrated analysis of these developments. We examine how technology is reshaping evidence law in India, survey major legal and judicial trends, assess the state of forensic infrastructure, and explore how these changes align with India's Sustainable Development Goals (SDGs), especially SDG 16 (justice and institutions). By referencing comparative models (e.g., U.S. Daubert standards, UK forensic protocols) and recent policy measures, we propose a path toward a "forensically enabled" legal system, one that embraces innovation without sacrificing fundamental fairness.

Technological Dimensions

The digital revolution is reconfiguring the very nature of evidence. In the Indian context, we identify three key technological dimensions:

Blockchain as a Trust Framework. Blockchain's primary promise in evidence is immutability. When each forensic record or custody chain event is hashed and linked in a distributed ledger, it becomes computationally infeasible to alter past entries without detection. India's law enforcement is already piloting blockchain for evidence management: Delhi's Forensic Science Laboratory, for instance, is developing a blockchain-based "e-forensic" app so that each piece of evidence (tagged with QR codes) remains "free of any tampering" from collection through analysis. This system creates clear audit trails across multiple stages. In practice, blockchain could thus bolster the *chain of custody* by digitally stamping each transfer of data. It also underpins other tools, like smart contracts that automate evidentiary certification or decentralized registries (for example, land records) that courts can tap as sources of truth. However, integration is still nascent. Most Indian courts currently lack the infrastructure to verify cryptographic hashes or smart-contract logs. Judges will soon face questions like: what probative weight to give a blockchain entry compared to sworn testimony? Until standards emerge, blockchain evidence may boost transparency, but it cannot alone resolve disputes.

Artificial Intelligence in Forensics and Legal Research. AI is reshaping Indian justice on two fronts. On the one hand, courts are adopting AI tools for efficiency: for example, the Supreme Court's AI portal (SUPACE) helps summarize case law, and many practitioners use software to search precedents or predict sentence ranges. Judges in higher courts have noted the scale of this shift. By April 2022, about 19.2 million cases across India had been heard virtually (via video conferencing), with 17.8 million disposed, highlighting how AI-enabled docket management and remote hearings are operational. On the other hand, AI is deeply entering evidence analysis: police now use facial-recognition systems, predictive-policing models, and data-mining algorithms to detect fraud and criminal networks. Novel forensic AI tools can parse terabytes of data (chat logs, CCTV feeds, banking records) far faster than humans. For example, speech-recognition and deep-learning algorithms help authenticate voice messages or match images from crime scenes.

These AI advances raise ethical and evidentiary concerns. Many systems operate as "black boxes": their logic is opaque even to experts. Studies (e.g., Buolamwini & Gebru) show facial-recognition tools misidentify minorities at higher rates, and global reports note similar biases in predictive policing. If Indian police or courts rely on AI outputs (say, a probability score that a suspect's face matches a watchlist), how can they verify that output? Current Indian law has no standards for AI explainability. To uphold due process, any AI-derived evidence must be auditable and contestable. India might look to international models: for instance, the EU's proposed AI Act would require synthetic images to be watermarked and algorithms to be transparent. In sum, while AI can accelerate investigations and legal workflows, unchecked deployment risks entrenching existing biases and undermining equality before the law. Courts will need protocols to interrogate AI-generated evidence and remain cautious about substituting human judgment with algorithmic outputs.

*Digital Forensics and Metadata***.** Digital forensics, the science of retrieving data from devices, is both a tool and a chokepoint. Techniques like bitstream imaging, file carving, memory analysis, and metadata reconstruction allow investigators to recover emails, browsing histories, GPS logs, and even fragments of deleted files. Properly done, these techniques yield compelling digital traces: for instance, obtaining the geolocation metadata from a phone's photos can corroborate a suspect's alibi. However, forensic work is extremely sensitive to the process. Even minor errors (a wrong tool, or reading from a live hard drive without a write-blocker) can alter data. In India, recent reports have highlighted systemic gaps: many police units lack certified cyber-forensic labs and trained personnel. Without uniform accreditation (unlike ISO/IEC standards in the US/EU), labs use varying methods, raising questions about evidentiary integrity. Moreover, emerging data types complicate the field: encrypted cloud storage, ephemeral messaging (like WhatsApp or Snapchat), Internet-of-Things logs, and even AI-generated "synthetic" data fall outside traditional procedures.

Maintaining data integrity demands rigorous procedure: investigators should create bit-for-bit copies of drives (using hardware write-blockers) and hash both the original and copy. Matching hashes guarantee the copy's exactness. Courts and agencies now understand this in theory: the new Evidence Act explicitly mandates documentation "for every stage of evidence handling". In practice, though, implementation lags. Many agencies still seize devices without imaging them, or chain-of-custody logs go unrecorded. Weaknesses here can doom evidence; Indian courts have overturned crucial forensic reports (e.g., DNA) due solely to sloppy logging. Until India closes these gaps, the reliability of digital evidence will hinge on the discipline of investigators and the availability of modern forensic technology.

Legal Framework

India's statutory regime is catching up with the digital era, but with tensions. Two recent laws are especially relevant: the *Bharatiya Sakshya Adhiniyam* (2023) replaces the Indian Evidence Act of 1872, and the *Digital Personal Data Protection Act* (2023) overhauls privacy law.

The new Evidence Act embraces technological neutrality. It broadly defines "document" and "electronic record," treating e-records on par with paper documents. However, it retains a strict admissibility regime: e-records are still "primary evidence" and generally require an official certificate of authenticity (akin to the old Section 65B of 1872) when produced secondarily. In cases like *Anvar P.V. v. P.K. Basheer (2014)*, India's Supreme Court had previously held that any electronic evidence must accompany a Section 65B(4) certificate, essentially confirming the record's origin and integrity. That precedent survives. The new law even codifies Section 65B as Section 65: to admit digital evidence, a responsible officer must describe how the data was generated, which machine produced it, and sign off on its integrity. In effect, procedural formalities still guard digital proof. Critics note this focus on compliance can paradoxically exclude truth – a securely stored WhatsApp message might be deemed inadmissible simply because the custodian lost the "certificate" paperwork.

Privacy and consent also feature in the framework. The *Digital Personal Data Protection Act, 2023,* establishes consent-based rules for processing personal data, but carves out broad national-interest exemptions. Enforcement and surveillance laws (like the IT Act and Telegraph Act) still permit warrantless access in many cases. Article 21 of the Constitution, after *Puttaswamy (2017)*, protects privacy as a fundamental right. Yet present rules give law enforcement sweeping powers. For instance, agencies often rely on internal authorizations to search digital evidence without judicial oversight, raising due-process questions. India's new data law introduces user rights (e.g., data correction, erasure) and mandates consent for collection, but it still allows blanket exceptions (such as for security or "public order" purposes). Thus, evidence-gathering is caught between two imperatives: courts demand procedurally perfect digital proof, even as privacy safeguards can be weak. Policymakers and courts are now debating how to reconcile these goals – for example, whether an independent judiciary should regulate cyber-surveillance and whether the certificate regime should be relaxed when data is retrievable only from a reluctant private server abroad.

In practical terms, Indian law still struggles to define the chain of custody for e-evidence. The new Evidence Act calls for logs at every handling stage, but gives limited guidance on enforcement. If a police officer pockets a seized phone for a week without logging it, there is no automatic sanction; judges may exclude such evidence at their discretion. This underscores a legal-technical gap: India has laws recognizing digital records, but not yet a culture of forensic rigor. Strengthening the framework will likely require both clearer statutes (e.g., penalties for chain-of-custody violations) and procedural rules (for instance, guidelines on using forensic imaging). Some model laws (forensic protocols of the UNODC or ISO standards) could help. Until then, the admissibility of digital proof in India will depend heavily on case-by-case judicial interpretations and on the professionalism of investigators rather than on a unified code.

Judicial Trends

The Supreme Court and High Courts have navigated digital-evidence issues through a series of landmark cases, illustrating shifting judicial philosophy. Early on, judges were eager to admit e-records subject to certification. In *Suhas Katti v. Tamil Nadu (2004)*, the first cyber-harassment case, a district court admitted an email printout under Section 65B even though the formal certificate was "informally" issued by a private expert. This set a precedent that authenticated digital copies (even from a remote server) could be treated as primary evidence if properly certified.

However, just a year later, *State v. Navjot Sandhu (2005)* introduced caution. The Supreme Court held that illegally intercepted phone call records could be admitted without strict 65B certificates, as a kind of "secondary evidence" under general rules. Navjot effectively lowered the bar: call-detail records were admitted like ordinary documents, as long as officers attested to their source. While pragmatic, this approach alarmed critics for sidestepping Section 65B's safeguards against tampering.

A decade later, *Anvar P.V. v. P.K. Basheer (2014)* reversed Navjot's laxity. A three-judge bench declared Sections 65A–B a "complete code" for electronic records. From then on, any digital evidence not accompanied by a valid 65B (4) certificate was inadmissible. Anvar underscored strict formality: it even barred oral testimony to validate an uncertified digital record. In practice, these tightened standards have changed dramatically. For instance, uncertified CDs of recorded speeches were excluded, forcing prosecutors to scramble for paperwork. Critics noted that Anvar's rigidity failed to consider realities, how to get certificates from foreign tech platforms, or when devices are destroyed, but the Court insisted on procedural precision for the sake of reliability.

The pendulum swung again shortly after. In *Tomaso Bruno v. State of U.P. (2015)*, another bench sidestepped Section 65B entirely for CCTV footage: it allowed the video content as secondary evidence under the general provisions. Effectively, Tomaso Bruno revived a Navjot-style exception, at least for certain kinds of data. The Court later admitted it did not follow Anvar (calling those decisions "per incuriam"). This created confusion: two parallel rules (Anvar's strict code vs. Tomaso's relaxed approach) left lower courts uncertain which to follow.

The conflict continued with *Shafhi Mohammad v. State of H.P. (2018)*. A bench carved out a narrow "safety valve": if an accused truly has no control over the device holding evidence (for example, call data held only by a telecom), then insisting on the certificate could be harsh. Shafhi allowed courts to admit such evidence under general law, framing 65B (4) as procedural rather than jurisdictional. In other words, certificates weren't mandatory in every circumstance, a compromise aimed at fairness.

Finally, in *Arjun Panditrao Khotkar v. Gorantyal (2020)*, the Supreme Court resolved the split. A full bench overruled both Tomaso and Shafhi, reaffirming Anvar's strict rule. It held that Sections 65A–B exclusively govern all electronic evidence and that a 65B (4) certificate is a "condition precedent" for any secondary digital record. The Court stressed that without the certificate, no amount of oral testimony or alternative proof can substitute. This effectively cemented the Anvar regime: post-2020, lower courts resumed excluding uncertified e-evidence. (The majority did acknowledge one concession: judges can now summon a certificate from a recalcitrant custodian under India's procedural codes, but this is rarely practical.)

Taken together, these cases illustrate an oscillation in judicial attitude. Early on (2004), the courts were willing to admit electronic records with basic certifications. The mid-2000s saw a liberal turn (Navjot) followed by a return to formality (Anvar). The late 2010s saw confusion (Tomaso/Shafhi) as courts tried to balance technical rules with substantive justice. And finally, Khotkar (2020) restored rigidity, albeit with some sighs that the law might need future amendment. Throughout, a theme emerges: technology keeps outpacing law, so judges swing between form and substance and vice versa, often erring on the side of caution in evidence law.

Despite this turbulence, a clear trend is visible: Indian judges recognize the importance of digital evidence but struggle with it. There is no uniform lower-court approach. In one city, a WhatsApp screenshot may be admitted; elsewhere, the same data is thrown out. This procedural roulette erodes predictability. The only way to achieve consistency is either through new legislation (to clarify the statute) or through higher court guidance. Meanwhile, an emerging model is hybrid: courts increasingly allow technology-driven submissions, but still scrutinize them with traditional safeguards.

Forensic Infrastructure

Robust evidence requires robust institutions. In recent years, India has dramatically expanded its forensic infrastructure, but gaps remain. The Ministry of Home Affairs (MHA) has linked 117 forensic science laboratories across states through an "e-Forensics" IT platform. This network centralizes data and speeds up requests between labs. The MHA has also established three new Central Forensic Science Laboratories (CFSLs) in Bhopal, Guwahati, and Pune, and upgraded Kolkata's lab to high-end standards. Additionally, six new *National Cyber Forensic Laboratories* (NCFLs) have been approved at major CFSLs (e.g., Delhi, Chandigarh) under a Women's Safety scheme, tapping the Nirbhaya Fund. These specialized cyber units focus on technology-intensive crimes and gender-related offenses.

On the academic front, the National Forensic Sciences University (NFSU) has expanded rapidly. Originally set up in Gujarat, NFSU now has several satellite campuses. In late 2024, in-principle approval was granted for five more off-campuses (in Goa, Agartala, Bhopal, Dharwad, and Guwahati). Moreover, a new National Forensic Infrastructure Enhancement Scheme provides ₹1,309 crore to establish nine additional NFSU campuses (2024–29). This investment signals India's long-term commitment to training forensic scientists and standardizing lab procedures nationwide.

Despite these strides, implementation is uneven. Many state labs still lack accreditation and standardized protocols. In practice, police units often have to send devices to distant centers, causing delays. India's criminal code does not independently define "chain of custody," so procedures vary by jurisdiction. Some courts admit digital evidence despite custody gaps, treating lapses as excusable; experts warn this "don't ask, don't tell" approach risks admitting contaminated data. To remedy this, Indian agencies have begun issuing formal guidelines: the DUS (Directorate of Forensic Science Services) has released quality manuals for lab accreditation and evidence-handling SOPs. Training programs have also expanded, over 32,000 officers (investigators, prosecutors, medical examiners) have been trained in forensic procedures, and tens of thousands of sexual assault evidence collection kits have been distributed.

Still, human capital remains a bottleneck. The ratio of forensic examiners to cases is low, and many police stations lack basic digital forensics skills. Even with modern labs, evidence goes unused if no expert can testify about it. In this sense, forensic infrastructure is a double-edged sword: India has massively increased its labs and budgets, but without uniform standards and personnel, quality can't keep pace. Experts call for national accreditation programs (with legal backing) and for embedding independent forensic scientists in investigative teams. The goal is to mirror best practices: for instance, Interpol's digital-evidence guidelines or the U.S. NIST frameworks, which require strict chain-of-custody logs and tool validation. If adopted nationally, such standards would ensure that Indian digital evidence is as reliable and scientifically credible as physical evidence.

SDG Alignment

Digital evidence management intersects surprisingly closely with India's Sustainable Development Goals. SDG 16 (Peace, Justice, and Institutions) emphasizes accountable, inclusive justice systems. Digital tools can advance these targets. For example, India's Aadhaar biometric ID now covers 95.5% of the population, providing nearly universal digital identity. This broad coverage helps certify electronic records; when a police report or court filing is linked to an Aadhaar-verified identity, it gains credibility. Moreover, judicial technology initiatives expand access to justice: India's e-Courts mission approved 1,150 new virtual courts, allowing more litigants to attend hearings remotely. By reducing travel costs and hearing backlogs (19.2 million virtual hearings by April 2022), these innovations help "access to justice for all" (SDG 16.3). In practical terms, remote hearings and e-filing mean rural citizens can participate in legal processes without long journeys.

Improved forensic capacity also serves SDG 16. Faster, more reliable evidence examination strengthens institutions (SDG 16.6). For instance, expanding CFSLs and deploying mobile forensic vans directly bolsters law enforcement's ability to solve crimes efficiently. In 2022, India's charge-sheeting rate for IPC crimes was 71.3%, below ideal, reflecting cases filed v. cases closed. Enhanced digital evidence handling (like quicker DNA matches or digital tracking) could raise this metric by enabling more prosecutions. Women's safety initiatives are further tied to SDG 5 (Gender Equality). The Union has allocated Nirbhaya funds to establish dedicated cyber-forensics units focusing on crimes against women. By ensuring gender-based crimes are investigated with modern tech, India advances its target SDG 5.2 ("eliminate violence against women") through forensic innovation.

SDG 9 (Industry, Innovation, and Infrastructure) is echoed in India's approach to legal-tech. Incorporating AI and blockchain into the justice system is itself an act of industrial innovation. AI-powered analytics (automating data review, anomaly detection) boosts investigators' capacity, while blockchain applications demonstrate homegrown tech solutions. Delhi's blockchain e-forensics app exemplifies this: it is a cutting-edge infrastructure project within the public sector. Such projects also signal to international observers that India is cultivating a tech-forward justice ecosystem. Moreover, India's commitment to digital inclusion (e.g., 95% 4G connectivity nationwide) dovetails with the SDG 9 goals. In short, modernizing evidence law not only serves justice, it contributes to India's broader development agenda by fostering transparency, innovation, and inclusion.

Conclusion

India stands at a crossroads in evidence law. On one hand, courts and legislatures have acknowledged the pivotal role of digital evidence. New statutes (the 2023 Evidence Act and Data Protection Act) recognize electronic records and aim to integrate them. Judges have repeatedly stressed reliability and technical integrity in recent rulings. On the other hand, evolving jurisprudence has been inconsistent: strict rules (as in *Anvar* and *Khotkar*) have alternated with practical exceptions (*Shafhi*, *Tomaso*). Our review finds that this inconsistency undermines certainty. The draft Evidence Act 2023, for example, still ties its reform to the old certificate regime, a contradiction that critics note could confuse investigators.

To move forward, India needs both doctrinal and institutional clarity. Legally, the new evidence law should reconcile formality with reality, for instance, by specifying how digital signatures, timestamps, or third-party data requests can fulfill authentication requirements. Statutory provisions might also be updated to address AI-specific issues (e.g., requiring disclosure of algorithmic methods when AI-derived evidence is used). Judges, in the meantime, should receive specialized training in cyber-forensics and AI so they can independently assess digital evidence. Educational initiatives (in bar councils and judiciaries) are crucial; as one expert notes, judges must grasp emerging tech to make informed rulings.

Internationally, India should seek better cross-border evidence mechanisms. Its mutual legal assistance (MLAT) processes are currently slow. We suggest India evaluate models like the U.S. CLOUD Act (bilateral data-sharing pacts) or the EU's emerging e-Evidence framework, possibly negotiating frameworks that allow faster access to data held by global tech companies. In the era of transnational cloud storage, India's courts cannot wait months for foreign cooperation. Improved treaties and direct channels will enable investigators to retrieve emails, logs, and other critical evidence in time to prosecute crime effectively.

Finally, India must incorporate safeguards against new threats. As AI blurs reality, evidence law must adapt. Indian courts have begun "taking judicial notice" of deepfakes in some cases, and the government has urged online platforms to label synthetic media. Going further, India could mandate that AI-generated images and videos carry embedded metadata indicating their origin, a practice similar to upcoming EU regulations. Forensics labs should be equipped with deep fake-detection tools, and legislation could require watermarks for certain AI outputs.

In summary, digital evidence law in India has been oscillating between technical formality and practical necessity. The path forward lies in stability and integration: a clear legal code that embraces technology, robust forensic infrastructure, and continual judicial education. By doing so, India can ensure that its courts remain capable of discovering truth in a data-driven era, while safeguarding fairness and liberty.

References

- Anbarasi, G., & Sankar, D. (2025). *Greening the justice system: Assessing the legality, feasibility, and potential of artificial intelligence in advancing environmental sustainability within the Indian judiciary*. Frontiers in Political Science, 7, Article 1553705.
- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- Bharatiya Sakshya Adhiniyam, No. 47, Gazette of India (2023).

- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1–15.
- Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)* (ETS No. 185).
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
- Department of Justice, Government of India. (2025). *National Judicial Data Grid (NJDG).*
- Digital Personal Data Protection Act, No. 22, Gazette of India (2023).
- E-Committee, Supreme Court of India. (2023). *e-Courts Mission Mode Project Phase III.*
- E-Committee, Supreme Court of India. (2025). *e-Courts Project Report* (status as of June 2025).
- Government of India. (1872). *Indian Evidence Act, 1872* (Act No. 1 of 1872).
- Government of India. (2000). *Information Technology Act, 2000* (No. 21 of 2000).
- Government of India. (2023). *Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023).
- Government of India. (2023). *Digital Personal Data Protection Act, 2023* (No. 22 of 2023).
- Handa, S., & Thakur, S. (2024). Role of artificial intelligence in the admissibility of electronic evidence. *International Journal of Research Publication and Reviews, 5*(11), 1323–1328.
- Indian Evidence Act, 1872 (Act No. 1 of 1872) (India).
- Information Technology Act, 2000 (Act No. 21 of 2000) (India).
- Interpol. (2020). *Global guidelines for digital forensics laboratories.*
- Interpol. (2020). *Guidelines for Digital Forensics Laboratories*. Lyon: Interpol Cybercrime Directorate.
- ISO/IEC. (2012). *27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence*. International Organization for Standardization.
- Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).
- Ladoia, P., Sharma, T., & Mukhija, N. (2024). *Changes introduced under the Bharatiya Sakshya Adhiniyam, 2023.*
- Ministry of Home Affairs. (2024). *Annual Report 2023–24*. Government of India.
- Mittal, R., & Jha, P. (2021). Automated evidence and algorithmic accountability in India. *Indian Journal of Law and Technology, 17*(1), 36–55.
- National Crime Records Bureau. (2023). *Crime in India – 2022 Statistics*. Government of India.
- National Forensic Sciences University. (2024). *Institutional Expansion Brief*. Retrieved from
- Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data. *Forensic Science International, 338*, Article 111565.
- Puttaswamy v. Union of India, (2017) 10 SCC 1.
- Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
- Sharma, A., & Srivastava, R. K. (2023). Digital justice: Analyzing the role and legal admissibility of digital forensic evidence in India. *Indian Journal of Law and Legal Research, 7*(1), 2691–2709.
- Singh, S., & Chahar, V. (2025). Legal admissibility and evidentiary value of electronic evidence in criminal proceedings. *International Journal of Research Publication and Reviews, 6*(4), 8237–8245.
- Singh, S., & Mishra, V. (2022). Digital forensics and legal admissibility in India. *International Journal of Cyber Law & Forensics*, 4(2), 91–104.

- State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
- Suhas Katti v. State of Tamil Nadu, CC No. 4680/2004 (Metropolitan Magistrate, Chennai).
- Tomaso Bruno v. State of U.P., (2015) 7 SCC 178.
- United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. UN General Assembly.
- UNODC. (2019). *Cybercrime Module 6: Key issues in handling digital evidence*. United Nations Office on Drugs and Crime.
- UNODC. (2019). *Digital Evidence and Chain of Custody: A Training Manual*. United Nations Office on Drugs and Crime.
- Vidhi Centre for Legal Policy. (2021). *Strengthening forensic and legal infrastructure for electronic evidence in India*.
- Wang, X., Wu, Y.C., & Ma, Z. (2024). *Blockchain in the courtroom: evidentiary significance and procedural implications in U.S. judicial processes*. Frontiers in Blockchain, 7, Article 1306058.
- Wang, X., Wu, Y.C., & Ma, Z. (2024). *Blockchain in the courtroom: evidentiary significance and procedural implications in U.S. judicial processes*. Frontiers in Blockchain, 7, Article 1306058
- World Bank. (2018). *Doing Business 2018: Reforming through Difficult Times.*

GRASP - EDUCATE - EVOLVE