CHALLENGES IN DIGITAL FORENSICS AND CYBER EVIDENCE IN INDIAN COURTS

Mr Ashish Shahi, Assistant Professor, Khwaja Moinuddin Chisti Language University Lucknow.[1]

Introduction

The digital age has transformed the criminal justice landscape by making electronic data ubiquitous in investigations. Crime today often involves computers, smartphones, cloud services and social media, producing vast amounts of "cyber evidence." In response, India's legislature and judiciary have struggled to adapt 19th-century laws to 21st-century technology. The Information Technology Act, 2000 introduced legal recognition of electronic records, and in 2023 the Bharatiya Sakshya Adhiniyam (BSA) replaced the Evidence Act, 1872 to explicitly include digital evidence. However, the legal framework remains fraught with ambiguities and gaps. As one recent study notes, "Digital evidence is defined vaguely, there are no established standards for its preservation or analysis, and no set protocols for its presentation in court".[2] The courts and legislature have repeatedly noted that without clear procedures, proof based on electronic records is vulnerable to manipulation. For instance, the Supreme Court warned that relying on unsafeguarded electronic records could lead to a "travesty of justice".[3] This chapter examines the principal legal challenges in admitting and handling digital evidence in India, focusing on admissibility under the Evidence Act, chain-of-custody and authenticity concerns, compliance with procedure, judges' technological capacity, and specific issues under the IT Act, Evidence Act/BSA and CrPC. Throughout, we cite key Indian cases and recent legal reforms (up to 2025) relevant to cyber forensics and electronic proof.

Legal and Statutory Framework

Indian Evidence Act (and Bharatiya Sakshya Adhiniyam)

Prior to the digital era, the **Indian Evidence Act, 1872** did not contemplate electronic records.

[1] Assistant Professor, Khwaja Moinuddin Chisti Language University Lucknow.

[2] International Journal of Law, Legal challenges and lacunas in the digital forensics jurisprudence in India

[3] Legislative Brief, PRSIndia

The Information Technology Act, 2000 amended the Evidence Act to include electronic evidence: it defined an "electronic record" and declared that documents could include data produced by computers. In particular, the Act added Sections 65A and 65B (now Sections 62–63 of the BSA), creating a special scheme for electronic evidence. Section 65B(1) states that any information printed, stored or recorded by a computer (a "computer output") is "deemed to be also a document" and is admissible if certain conditions are met.[4] These conditions (in clause (2) and (4)) require, among other things, a **certificate of authenticity** from a responsible official identifying the device and verifying that the record was produced by it.[5] The statutory scheme thus treats certified electronic output much like the original document itself, subject to the safeguards in the sections. The Supreme Court has held that this regime (Sections 65A–65B) is a "complete code" for electronic evidence, meaning that general Evidence Act provisions yield to it when secondary electronic evidence is offered.[6] In short, the Evidence Act (as amended) provides that a printout or data copy of an electronic record is admissible if accompanied by a proper certificate of authenticity.

Presumptions: The Act (and now the BSA) also includes presumptions relating to electronic data and digital signatures. For example, Section 90A (IEA) presumes that an electronic signature on a record older than five years is genuine if the record came from a proper source. Section 73A (IEA) deals with verification of a digital signature by a certifying authority. Sections 85A–85C create rebuttable presumptions that an electronic agreement is valid and that an electronic signature or certificate belongs to the purported person. These presumptions are meant to ease the prosecution of electronic evidence, but they apply only when the basic admissibility criteria are met.

Information Technology Act, 2000

The IT Act itself defines many of the building blocks of cyber evidence. It introduced the concept of a **digital signature** (secure electronic signature) and set up certifying authorities to authenticate them. It amended Evidence Act definitions so that "electronic form" and "electronic record" have statutory meaning. The Act also gave law enforcement new investigative powers over digital devices. For instance, Section 69 authorizes a magistrate or

[4] Drishti Judiciary, Impact of Information Technology Act on Indian Evidence Act
[5] *ibid*
[6] *ibid*

designated officer to order interception of computer content; Section 69A allows blocking of websites; Section 70 allows search and seizure of computers or data, and Section 72A provides for penalties for violating privacy by theft of data. (These provisions raise their own constitutional and procedural issues, but at minimum they validate police powers to seize devices or compel data from them.)

The IT Act introduced **safe harbor** for intermediaries (Section 79, originally 79A) but carved exceptions (Section 85B, 85C) for offline evidence standards and certification. It also inserted Sections 47A and 45A in the Evidence Act (before becoming BSA sections) to provide that expert opinions on digital signatures and electronic evidence are admissible. In short, the IT Act underpins the admissibility framework by defining key terms and authorizing evidence collection, but it did not itself resolve practical evidentiary issues which have been left to judicial interpretation.

Code of Criminal Procedure (CrPC)

The Code of Criminal Procedure (1973) governs the gathering of evidence by police. It generally treats electronic items like other "movable property" that can be searched and seized. For example, a search warrant under Section 96–98 may authorize taking possession of computers or drives. In 2009 the CrPC was amended (Criminal Law Amendment Act 2008) to clarify that courts can order seizure and custody of digital evidence (for example, under Sections 91 and 92 regarding summoning records). However, no specific provisions were added at that time exclusively for electronic devices; they fall under the general seizure laws.

The interplay of CrPC and IT Act also raises questions. Notably, in *Virendra Khanna v. State of Karnataka* (2021) the Supreme Court held that compelling a suspect to divulge a password or biometric to unlock a device does not violate the right against self-incrimination (Article 20(3) of the Constitution).[7] This means that once police have lawful access to a person or premises, they may legally demand encryption keys or fingerprints to access evidence. The court emphasized that such compulsion is different from forcing a person to speak about guilt; producing a password is like producing a key for a locked safe. This ruling has streamlined investigations, but it also underscores that strict procedural compliance (like obtaining proper

[7] Virender Khanna vs State of Karnataka (Device Seizure) • Page 1 • CYRILLA: Global Digital Rights Law

warrants) is required before using these powers.

Admissibility of Digital Evidence

A central challenge in cyber-forensic trials is simply getting digital evidence admitted in court. The legislature's special provisions (Section 65B and related sections) aim to ensure authenticity, but their application has been contentious. In practice, judges often must decide whether a given digital item is **primary evidence** (the original document itself) or **secondary evidence** (a copy or output). Under Section 62 of the Evidence Act (now Section 57 of the BSA), all documents are prima facie primary evidence of the facts in them, unless they fall under exceptions for secondary evidence. However, Section 65B creates a special rule for electronic documents: any printed copy or recording of an electronic record (a computer output) is deemed a document only if the certification conditions are met.[8]

- *Conditions for admissibility:* Under Section 65B, the prosecution must normally produce a **certificate** that identifies the electronic record, describes the device that produced it, and states that the device was working properly, among other points. This certificate (signed by a person in charge of the device) is intended to authenticate the record. In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court held that Section 65B's requirements are mandatory: the word "may" in 65B(4) is to be read as "shall," and electronic evidence without the prescribed certificate is inadmissible. In other words, Anvar confirmed that Sections 65A–65B are a complete code:

  secondary electronic evidence can only be admitted if 65B's conditions are satisfied.[9]

- *Judicial guidance:* These requirements led to conflicting case law. In *State (NCT of Delhi) v. Navjot Sandhu* (2005) – the "Parliament attack" case – the Court admitted an electronic record without a 65B certificate, treating it under general hearsay provisions. This was later overruled. In *Anvar* (2014) the Court explicitly overruled Navjot, emphasizing the need for certification. Later cases briefly muddied the waters: *Shafi Mohammad v. State of Himachal Pradesh* (2018) suggested that a certificate might not be required when the record came from a device not in the party's control. Ultimately, a three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*

[8] D Judiciary, Impact of Information Technology Act on Indian Evidence Act
[9] *ibid*

(2020) reaffirmed Anvar's rule and overruled Shafi. It held that a certificate is **not needed** if the "original electronic record" itself is produced (for example, the actual computer or phone).[10] If the original cannot practically be brought (e.g. a networked system), then a certificate is required for secondary evidence. In short, Arjun Panditrao said: original digital records (by their owner) can be shown in court without a certificate, but otherwise, follow Section 65B.[11]

- *Recent developments:* This principle was recently applied again in *Kum. Shubha v. State of Karnataka* (July 2025). There the Supreme Court explicitly endorsed Arjun Panditrao, confirming that Sections 65A–65B of the old Act (Sections 62–63 of the BSA) form a complete code on electronic evidence.[12] Importantly, the court observed that the new BSA recognizes electronic records as primary evidence in a prescribed form (Section 57 BSA), but still requires compliance with Section 63 (65B) for admissibility. The legislative Standing Committee also emphasized this point: it recommended that electronic records be proven in accordance with the certification provision.

In practice, these rulings mean that any photocopy of a chat log, email, or phone memo must be presented with a Section 65B certificate. Without it, the court should exclude the evidence. However, if the police bring the original computer or device and the person who used it, the contents can be admitted directly. This has sometimes confused trial courts, but higher courts now stress that the certificate is a **mandatory safeguard** for secondary electronic evidence. The BSA (2023) retains this structure, effectively keeping the certification regime in place.[13]

Authenticity and Integrity of Digital Evidence

Electronic data's ease of alteration makes authenticity a key concern. Unlike a paper letter, a digital file can be changed without visible marks. Courts have repeatedly noted this risk. For example, the Supreme Court observed in *Anvar* that if a trial is based on electronic records without "adequate safeguards," it may be a "travesty of justice". Ensuring that data has not

[10] *ibid*

[11] International Journal of Law, Legal challenges and lacunas in the digital forensics jurisprudence in India

[12] Hindustan Times, Electronic evidence on trial: It's time for some clarity from the courts

[13] *Ibid*

been tampered with is therefore essential to its reliability.

Several legal and technical tools address authenticity:

- **Section 65B certificate:** As discussed above, the certificate itself is supposed to verify the origin and integrity of the electronic record. By requiring an official custodian to attest to the condition of the device and the genuineness of the output, it aims to assure the court that the evidence is trustworthy.

- **Digital signatures and presumption:** If an electronic record carries a valid digital signature, the law gives it weight. Section 85B (IEA) presumes that an electronic signature relates to the person purported to have signed, once its certificate has been established. Section 90A (BSA) goes further: if an electronic record is over five years old and has been in proper custody, the court may presume its signature (or e-signature) is genuine.[14] These presumptions reduce the burden of proving authenticity in routine cases.

- **Expert examination:** Courts can appoint an Examiner of Electronic Evidence to report on authenticity. The BSA explicitly allows courts to seek such expert opinion on electronic records (similar to Section 79(6) of the IT Act, formerly 67C) when needed. This ensures a technical evaluation of whether data has been changed or corrupted.

- **Metadata and forensic hashing:** Though not yet codified in law, best practice in digital forensics is to hash files (compute a cryptographic fingerprint) and maintain logs at each transfer. In *Arjun Panditrao*, the Supreme Court suggested that formal rules should be made (under Sections 67C etc.) to mandate retention of metadata, stamping, and chain-of-custody for digital evidence.[15] Such measures would provide a verifiable trail proving that a record in court matches the one seized.

Despite these tools, courts still grapple with proving authenticity. Unlike ink on paper, electronic records lack visible security features. When parties dispute a record's genuineness, judges look to process: if the police followed proper procedures, the court may infer the record

[14] *Supra Note 10*

[15] D Judiciary, Impact of Information Technology Act on Indian Evidence Act

is genuine. If not, they may reject it. In the absence of uniform national standards (as scholars lament, there are "no established standards" for digital evidence), these authenticity determinations can be inconsistent.

Chain of Custody of Digital Evidence

A related practical challenge is preserving and documenting the **chain of custody** for electronic items. The chain of custody records every person who handled an item of evidence, from seizure to trial. As one commentator notes, the chain "is the mechanism by which evidence is accounted for from the time it is collected to its production in court." In digital forensics, an unbroken chain is critical because data can be altered at any step. The Supreme Court has warned that without such safeguards, electronic evidence is prone to tampering.[16] In theory, each transfer of a device or file must be logged with who transferred it, when, why, and to whom.

Ensuring the integrity of digital evidence begins with a documented chain of custody. In practice, however, Indian courts have noted that "no clearly defined standard" exists for digital evidence, leading to inconsistent application. If the prosecution fails to prove that each link in the chain was secure, the defence may argue that the evidence was altered. As one analysis explains, the absence of standards "leads to inconsistencies in judicial assessment" when the chain is disputed.[17] Despite this, prosecutors and investigators often lack rigorous protocols, so courts must sometimes weigh the risk of manipulation.

To reduce this problem, recent directives have emerged. For example, the Karnataka High Court (in the *Virender Khanna* case) issued guidelines for searches involving computers: a **qualified forensic expert** must accompany the search team, the investigating officer must not browse the seized device, and storage media (USB drives, etc.) should be sealed in Faraday bags to prevent remote wiping. These precautions help establish a trustworthy chain. The Supreme Court has also recommended that the government frame rules (under the IT Act) on data retention, metadata, and custody procedures. The parliamentary Standing Committee likewise urged that "all electronic and digital records collected as evidence… be securely handled and processed through proper chain of custody".

[16] *Supra Note 10*
[17] SCC Times, Securing the Links: A Framework for Chain of Custody in Indian Courts

In sum, a secure chain of custody requires meticulous documentation at each step: who first collected the evidence, the dates it changed hands, descriptions of the device or file, and how it was stored. Scholars note that absent clear national protocols, such record-keeping can be inconsistent, potentially jeopardizing admissibility.[18] The courts now treat any break in this chain with suspicion. In practice, trial judges will often exclude evidence or conduct a careful inquiry if they find gaps in custody.

Procedural Safeguards and Compliance

Beyond the substantive rules of admissibility, procedural law governs how digital evidence is collected. Investigators must adhere to search-and-seizure laws when dealing with computers and networks. Under the CrPC, police generally need a warrant to search premises (Section 96–98) or the court's permission to demand evidence (Section 91–92). The Supreme Court has held that these protections apply to digital media as well. When police seize computers, they must follow chain-of-custody steps (log items in an inventory etc.) and preserve the data.

The IT Act supplements this. For example, Section 69 requires magistrate's approval for any interception of private computer data. Section 70 empowers police to search and seize computers and order their safe custody. Importantly, Section 67C of the IT Act (as incorporated by Evidence Act) allows a police officer to give a certificate saying that the computer was accessed and the data extracted was sent for forensic analysis; this certificate then becomes evidence of the chain-of-custody and authenticity of the extracted data. In *Arjun Panditrao*, the Court explicitly recognized this power to obtain expert assistance and ordered the framing of rules to govern data retention during trials.[19]

In practice, adherence to procedure has been uneven. One notable decision is *Virendra Khanna v. State of Karnataka* (2021), where the Supreme Court addressed the rights of an accused during device search. The Court ruled that an accused person cannot refuse to unlock his device by invoking the right against self-incrimination.[20] This means that if police act within the law to seize a phone or computer, they can compel the suspect to provide passwords or fingerprints

[18] *ibid*

[19] International Journal of Law, Impact of Information Technology Act on Indian Evidence Act

[20] Virender Khanna vs State of Karnataka (Device Seizure) • Page 1 • CYRILLA: Global Digital Rights Law

to access the content. However, the Court emphasized that these powers are constrained by proper process: a valid warrant or court order must exist before any compulsion.

There are still procedural grey areas. For example, there is no separate "cyber search warrant" in Indian law, so courts apply old provisions to new technology. If police skip steps (e.g. seize a computer without a warrant or fail to log the seizure), courts may exclude the evidence. Defendants often raise technicalities – such as improperly stamped documents or unsigned certificates – to challenge digital proof. Recent legislative proposals (like the Bharatiya Nagarik Suraksha Sanhita, 2023) would codify certain procedures, but as of 2025 the law still relies heavily on case-by-case judicial standards.

Judicial Capacity and Expertise

A persistent challenge is the competence of the judiciary to handle technical evidence. Many judges and lawyers have limited training in digital forensics. Senior judges have explicitly noted this gap. In August 2025, the Supreme Court lamented the lack of "modern forensic infrastructure" and specialized expertise in India.[21] The bench remarked that law enforcement and prosecution units often lack forensic scientists and digital experts, even as crimes increasingly involve cyber elements. The Court urged the establishment of special courts and training programs: "Provide judges proper training and ensure time-bound judgments… The time has come for specialised courts," it declared.

India has taken steps toward capacity-building. Several states have designated cyber crime cells and trained judges to hear technology cases. The National Judicial Academy conducts courses on e-evidence. Private firms and government agencies offer digital forensics training to police and forensic lab technicians. Nevertheless, the pace of technological change makes it hard for courts to stay current. Judicial officers may struggle to evaluate forensic reports or understand data formats, leading to underutilization or mistrust of cyber evidence. This underscores the need for continuous education and perhaps court-appointed experts in complex cases.

Conclusion

Digital forensics has become indispensable to criminal justice, but Indian law is still catching up. The statutory framework – IT Act, Evidence Act (and now BSA), CrPC – provides a

[21] Mathrubhumi. Com, Is this 18th or 19th century investigation?: SC slams archaic criminal justice system

skeleton for admitting electronic evidence, but many details remain unsettled. Courts have clarified major issues: they now require stringent proof of authenticity (through certificates or originals) and emphasize proper handling of electronic records. Yet significant challenges persist. As one analysis observes, despite recognising electronic records as evidence, the law offers only broad principles with inconsistent implementation. Without uniform standards for collecting, preserving and presenting digital evidence, each court is left to its own devices.

In sum, the major hurdles in India are (1) **admissibility** – ensuring certificates and rules are followed; (2) **chain of custody** – proving evidence was unaltered; (3) **authenticity** – using technical and legal means to verify data; (4) **procedural compliance** – obtaining and handling data lawfully; and (5) **judicial expertise** – having trained decision-makers and experts. The Supreme Court and legislature have signaled remedies: mandating certificates, issuing handling guidelines, and even rewriting the Evidence Act. But effective change will require not just new laws, but rigorous implementation and education. As one recent critique warned, until courts uniformly apply these rules, digital evidence remains "subject to doubt". The way forward lies in codifying clear procedures (including custody protocols), investing in forensic infrastructure, and equipping judges with the technical knowledge to give proper weight to cyber evidence. Only then can Indian courts fully meet the promise of digital forensics.