



DIGITAL EVIDENCE AND CYBERCRIME: ADMISSIBILITY AND CHALLENGES UNDER INDIAN LAW

Poonam Kumari*

We live in a time when almost every human action leaves behind a digital footprint. A phone call, a money transfer, a message on WhatsApp, a Google search, a CCTV capture, or even a late-night tweet—everything is stored somewhere in the digital universe. Naturally, crimes too have entered this space. Today, we don't just talk about robbery or murder; we also worry about phishing scams, identity theft, cyberstalking, online defamation, cryptocurrency fraud, and even cyber terrorism.

When such crimes are committed, the most crucial aspect for investigation and trial is not just catching the criminal but proving the offence in court. This is where digital evidence plays a central role. Unlike a knife in a murder case, digital evidence is not tangible. It exists in the form of binary codes, stored in servers, cloud storage, or personal devices. Because of its fragile and easily manipulable nature, courts across the world—including India—face serious challenges in admitting and relying upon digital evidence. This article explores the legal framework, landmark judgments, and major challenges surrounding digital evidence and cybercrime in India, along with suggestions for the way forward.

We have to understand the meaning of Digital Evidence to make the topic easier.

Digital evidence refers to any information stored or transmitted in digital form that can be used in a court of law. It is not limited to computers but extends to mobile phones, smartwatches, cloud storage, and even IoT (Internet of Things) devices.

There are certain examples of Digital Evidence-

- **Textual Records:** Emails, SMS, WhatsApp messages, social media chats.
- **Visual/Audio Records:** CCTV footage, digital photographs, audio recordings.

*BBA LLB, THIRD YEAR, BANASTHALI VIDYAPITH, RAJASTHAN.

- **Metadata:** Location data, timestamps, IP addresses, browsing history.
- **Transaction Records:** Online banking logs, UPI transfers, credit card details.
- **Device-based Evidence:** Hard disks, pen drives, mobile phones.

What makes digital evidence unique is that it can either be a direct piece of evidence (like a video recording of a crime) or corroborative evidence (like call records proving presence at a place).

There are certain Legal frameworks for Digital Evidence in India which we have to understand for further details. It gives us the brief details about our topic, digital evidence and cybercrime. This gives more significant information for dealing with such matters.

The Indian legal system was originally designed for physical evidence. But with the rise of technology, Parliament amended laws to accommodate electronic records. Now, let's see the provisions or laws associated with our topic.

Indian Evidence Act, 1872 (Amendments of 2000):

Section 65A: Special provisions for electronic records.

Section 65B: Provides that electronic records are admissible only if accompanied by a certificate stating how the data was produced and confirming its authenticity.

The certificate must be signed by a responsible person in charge of the device or data.

Information Technology Act, 2000 (IT Act):

Section 4: Grants legal recognition to electronic records.

Sections 65–75: Deal with cyber offences.

Examples: Section 66 (Hacking), Section 66C (Identity theft), Section 66E (Violation of privacy), Section 67 (Obscenity in electronic form), Section 66F (Cyber terrorism).

Indian Penal Code (IPC), 1860: Traditional crimes like cheating, forgery, defamation, and harassment have **been** extended to the digital domain. For instance, sending defamatory content through email falls under IPC Section 499.

Code of Criminal Procedure (CrPC), 1973: Provides powers to police to search and seize electronic devices. Section 91 allows courts to summon electronic records during investigations or trials.

This legal framework talks about our topic. This is very beneficial for any country. There are various Landmark Case Laws on the Admissibility of Digital Evidence, which we have to understand that contain a lot more meaning about this.

Indian courts have played a crucial role in shaping the rules on digital evidence. The journey has been full of confusion, clarifications, and constitutional debates.

State (NCT of Delhi) v. Navjot Sandhu (2005) – Parliament Attack Case: Court **allowed** call records and digital documents without a Section 65B certificate. Treated electronic records as ordinary documents. Result: Law became flexible, but authenticity issues emerged.

Anvar P.V. v. P.K. Basheer (2014): A turning point in Indian evidence law. The Supreme Court ruled that, Section 65B certificate is mandatory. Oral evidence or other secondary evidence cannot replace it. Principle: “No certificate, no admissibility.”

Shafhi Mohammad v. State of Himachal Pradesh (2018): Relaxed the strictness of *Anvar*. The said certificate is not necessary if the party does not control the device (e.g., CCTV footage in a public place). Created another wave of confusion.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020): Constitution Bench judgment. Reaffirmed *Anvar* and overruled *Shafhi Mohammad*.

Clear Rule: Certificate under Section 65B is mandatory unless the original device is produced in court.

Sonu @ Amar v. State of Haryana (2017): If no objection to admissibility is raised during trial, it cannot be challenged later in appeal.

Jagdeo Singh v. State (2015, Delhi HC): Reiterated that the **Section 65B certificate is a condition precedent** for electronic evidence.

Kishan Tripathi v. State (2021, Allahabad HC): WhatsApp chats without a certificate were held inadmissible.

Justice K.S. Puttaswamy v. Union of India (2017): Not directly about admissibility, but important. Recognised right to privacy as a fundamental right. Any collection of digital evidence must respect privacy principles.

After discussing all These Case Laws, we can easily able to know that these case Laws give us a wider meaning or scope of Law. In *Bharatiya Nagararik Suraksha Sanhita, 2023*. This gives the wider meaning in digital evidence like footprint, audio-video, thumb impression and so on. This act digitally supports the availability of evidence. It was highly recommended to deal with a situation like cybercrime.

But there are Challenges in the Admissibility of Digital Evidence which we have to think of.

Despite clear judicial pronouncements, practical challenges remain-

Fragility of Evidence: Digital data can be tampered with, deleted, or manipulated easily. For example, a photo can be morphed, a video can be deep-faked, and chats can be fabricated.

Technical Limitations of Investigators: Many police officers and trial court judges lack advanced cyber forensic training. Mishandling during seizure or transfer can make evidence unreliable.

65B Certificate Hurdle: Victims or investigators often don't have control over servers (e.g., Facebook, Gmail, WhatsApp). Obtaining a certificate from foreign companies is a long process. Delay often results in evidence becoming useless.

Chain of Custody Issues: Courts require proof of an unbroken chain of custody. But in practice, devices are often passed through many hands without proper documentation.

Jurisdictional Problems: Cybercrimes are borderless. A fraudster in India may use a server in the US and transfer money to Europe. Cooperation depends on international treaties (MLATs), which are slow.

Privacy Concerns: Post-*Puttaswamy* case, the police must balance investigation with privacy rights. For example, accessing a person's private chats without proper procedure could violate Article 21.

Volume of Data: A single smartphone can store thousands of photos, videos, and chats. Investigating authorities often drown in data overload.

Evolving Nature of Technology: With encrypted messaging apps, blockchain, and the dark web, collecting reliable evidence has become more complex.

COMPARATIVE PERSPECTIVE – HOW OTHER JURISDICTIONS HANDLE IT

United States: Follows the Federal Rules of Evidence. Digital evidence must be authenticated, but no equivalent of Section 65B. Courts focus on reliability and expert testimony.

United Kingdom: The Police and Criminal Evidence Act (PACE) governs admissibility. Courts apply a “best evidence” rule and rely heavily on forensic experts.

European Union: General Data Protection Regulation (GDPR) ensures a balance between privacy and the use of digital evidence.

Compared to these jurisdictions, **India’s law is stricter** because of the rigid requirement of the Section 65B certificate.

WAY FORWARD – STRENGTHENING INDIA’S DIGITAL EVIDENCE REGIME

Capacity Building: Train police, prosecutors, and judges in cyber forensics. Establish digital evidence laboratories in every state.

Simplification of Section 65B: Introduce flexibility for cases where a certificate is impossible to obtain but authenticity is beyond doubt.

Specialised Cyber Courts: Set up dedicated courts with judges trained in digital law to handle cybercrime cases efficiently.

Blockchain Technology: Can be used to create tamper-proof records of evidence.

International Cooperation: Strengthen Mutual Legal Assistance Treaties (MLATs) for faster access to foreign servers.

Balancing Privacy with Justice: Develop clear guidelines for accessing private data to avoid arbitrary misuse while still ensuring effective investigation.

Public Awareness: Citizens should be educated about preserving digital evidence (e.g., not deleting scam messages, preserving transaction logs).

CONCLUSION

In the digital age, data is the new DNA of criminal investigations. Courts increasingly depend on digital evidence to convict or acquit. While India has moved forward with amendments in the Evidence Act and landmark judgments like *Anvar* and *Arjun Panditrao*, significant practical hurdles remain—especially regarding the 65B certificate, chain of custody, and privacy concerns. The future lies in a balanced approach: laws that are strict enough to prevent misuse but flexible enough to accept genuine evidence, supported by trained investigators and advanced forensic tools. Only then can digital evidence truly fulfil its role as the backbone of justice in the cyber era. This was the best way to understand this topic in a detailed manner.