# CURRENT SCENARIO OF DIGITAL EVIDENCE IN INDIAN LEGAL SYSTEM: IMPLICATIONS AND ISSUES

*By Anurag Gourav*[*]

## I. INTRODUCTION

People now manage their personal, social, and professional relationships primarily through smartphones and personal computers, creating an "always-on society" in which people are constantly connected to and linked to their devices. People who live in a constantly connected state leave behind large digital traces that can be saved, recovered, and examined by different third parties both in and out of context and after the event.[1]

It has made room for illegal activity to proliferate. Digital data transmissions, including text messages, emails, photos, and videos, have replaced physical mail as the primary means of interaction and communication in today's mostly virtual world. As the younger generation rapidly moves toward a digital environment, criminals continue to take advantage of these developments to damage others. This is the era of cyberwar, in which people attack one another using computers rather than firearms[2]. For personal gain, people or even an entire nation may be involved, and crimes have been committed using machines.



From a conceptual standpoint, digital evidence is no different from any other evidence; it is data that is used to try and position individuals and events in time and space in order to prove that a criminal act was caused by them. Compared to physical evidence, digital evidence is more broad movable, perhaps more personally sensitive, and requires new tools and training.[3] "Information and data of value to an investigation that is stored on, received by, or transmitted by an electronic device" is what is referred to as digital evidence[4]. Digital Evidence Types The

[*] Ph.D. Research Scholar, Narayan School of law, GNSU, Jamuhar (Rohtas). Email: anurag.law.nlc@gmail.com.

[1] Fanny Ramirez, *Interpretive and Interpersonal Challenges of Digital Evidence for Public Defenders,* JOURNALS.KU.EDU (Oct 27, 2023, 10:15 AM), https://journals.ku.edu/hct/article/view/18826/19142

[2] Syed Atir Raza, Aqsa Anwar, Abdul Hannan Khan, *Current Issues and Challenges with Scientific Validation of Digital Evidence,* INTERNATIONAL INFORMATION AND ENGINEERING TECHNOLOGY ASSOCIATION (Oct 27, 2023, 10:15 AM), https://www.iieta.org/journals/rces/paper/10.18280/rces.090304

[3] Sean E. Goodison, Robert C. Davis, Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System,* RAND CORPORATION (Oct 27, 2023, 10:15 AM), https://www.rand.org/pubs/research_reports/RR890.html

[4] Ibid

variety of digital devices and extraction techniques results in a similar possibility of recoverable evidence.

## II. Sources of Digital Evidence

- Internet: Message boards and chat rooms on communication websites provided some of the earliest digital evidence used in law enforcement investigations. Although other Internet-enabled technologies have proliferated, these kinds of sites still provide information for ongoing investigations; still, they are now just one of many possible sources of evidence.
- Computer – There is a lot of potential digital evidence on personal computers. When browsing the Internet, programs often keep temporary Internet files, cookies, and browsing history. Each of these factors can be used in an investigation to determine a user's web activity. [5]
- Portable Electronics – Today, the processing of digital evidence from portable electronic devices such as cell phones, Pendrive, DVD is a major focus of examiners and researchers.[6]

## III. Types of evidence in digital forms

- Documents and Files: These include text documents, spreadsheets, presentations, PDF files and other electronic files related to the case.
- Images and videos: Media files that may document events, actions or situations related to an investigation or legal matter.
- Social media posts: Other Posts, comments, likes and shares on social media platforms can provide insight into an individual's thoughts, activities and connections.[7]
- Internet browsing history: Information about websites visited, searches performed, and online activities that can provide context or timeline of events.
- Digital signature: Digital signatures can be used to verify the authenticity and integrity of electronic documents.

[5] Ibid
[6] Ibid
[7] Vanshika Shukla, *The Admissibility Of Digital Evidence: Challenges And Future Implications,* THE LAWBRIGADE (Oct 27, 2023, 10:15AM), https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf

- Authentication records: [8]Records of user credentials, access attempts, and account activity that can help determine who accessed a system or service.
- Network traffic data: Information about network connections, data transfers, and communication patterns can provide insight into network problems.
- Geolocation data: Location-based information from devices, applications or services can help determine a person's location at any given time.
- Call recording: Recording of telephone calls, including call logs and text messages, which may be relevant to investigations related to communication patterns. [9]
- Email: Email and attachments can provide valuable information about communications and interactions between individuals.
- Instant messaging and chat: Conversations that take place on platforms such as messaging apps, social networks, and chat apps can be important to understanding relationships and context.[10]
- Financial records: Digital records of financial transactions, bank statements, and payment history can provide insight into a person's financial activities.
- Deleted or modified files: Recovering deleted or modified files can sometimes reveal evidence of intentional concealment.

## IV. Laws governing Digital Evidence in India



The Information Technology (IT) Act 2000 was passed by Parliament in 2000, amending pre-existing Indian statutes to permit the introduction of digital evidence. Additionally offered changes to the Banker's Book Evidence Act of 1891, the Indian Evidence Act of 1872, and the Indian Penal Code of 1860 (which acknowledges transactions completed by electronic data exchange and other forms of electronic communication)[11]. Electronic records are now included in the definition of "evidence" (Section 3(a) of the Evidence Act). There are two types of evidence: oral or documentary. The term "documentary evidence" has been redefined to refer to any document, including electronic records that are produced for the court's scrutiny. The IT Act's definition of "electronic records," which includes "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-

[8] Ibid
[9] Ibid
[10] Ibid
[11] Tejas Karia, *Digital Evidence: An Indian Perspective,* LEXOLOGY (Oct 27, 2023, 10:15 AM), https://www.lexology.com/commentary/litigation/india/amarchand-mangaldas-suresh-a-shroff-co/digital-evidence-an-indian-perspective

generated microfiche," has been applied to the phrase "electronic records."[12] According to Section 17 of the Evidence Act, a remark made orally, in writing, or electronically that implies a conclusion about any relevant or in dispute fact now falls under the definition of "admission." The Evidence Act now includes a new Section 22A that addresses the admissibility of oral evidence pertaining to information found in electronic records. [13]It states that spoken disclosures about the contents of electronic records are irrelevant unless the authenticity of the documents is established.

Section 2(t) of the IT Act defines the term "electronic record" as "data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer-generated micro fiche[14] The Information Technology Act, 2000 (Act 21 of 2000)

Electronic evidence comprises computer evidence, digital audio, digital video, cell phones, and digital fax machines.[15] It is defined as any information of probative value that is either stored or transferred in electronic form under Section 79A of the IT (Amendment) Act, 2008.

## V. Issues and challenges

- Authenticity and tampering: Proving that digital evidence is authentic and has not been tampered with is a significant challenge. Modifying digital files, metadata, and other attributes is relatively easy, requiring establishing a clear chain of custody and demonstrating that the evidence presented is unchanged from its current state.[16]
- Privacy concerns: Admission of certain types of digital evidence may raise privacy concerns, especially when it involves personal or sensitive information[17]. Balancing the need for evidence and an individual's right to privacy can be a delicate issue.

[12] Ibid
[13] Ibid
[14] Aquib Husain, Dr. Eakramuddin, *Issues And Challenges Of Admissibility Of Digital Evidence: A Study*, INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT, (Oct 27, 2023, 10:15 AM), https://www.ijnrd.org/papers/IJNRD2306235.pdf
[15] Panjala Shreeya, Kaveti Vinisha, *Digital Forensics In India- An Overview*, LAW TIMES JOURNAL, (Oct 27, 2023, 10:15 AM), https://lawtimesjournal.in/digital-forensics-in-india-an-overview/
[16] Vanshika Shukla, *The Admissibility Of Digital Evidence: Challenges And Future Implications,* THE LAWBRIGADE (Oct 27, 2023, 10:15 AM), https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf?_gl=1*qkt937*_ga*MTk4MjgxNjcyLjE2OTg0ODA4MDY.*_ga_77Y54C8SBH*MTY5ODQ4MDgwNi4xLjAuMTY5ODQ4MDgwNi4wLjAuMA..
[17] Ibid

- Cross-border considerations[18]: Digital evidence can be stored in different jurisdictions, which can complicate matters jurisdictional issues, data protection law and international legal cooperation.
- Technological change: Due to the rapid development of technologies such as operating systems, application software and hardware, reading digital evidence becomes more difficult as new software versions are not supported by old versions and people take time to learn new applications,[19] leading to procedural delays.
- Admissibility in Court: Digital evidence collected from crime scenes is only admissible in court if it is obtained according to the procedure established by law[20]. In the Indian legal system, there is no detailed law explaining such debt collection procedure. Certain cases are provided for like; in section 65B of the Evidence Act 1872, but this is not enough.
- Preserving electronic evidence: Where electronic evidence is admissible, a Questions raised about preservation principles point to the fact that Preserving electronic evidence, which may involve a digital document to be preserved for up to 20 years during the trial and even beyond that for record of courts.[21]
- Lack of technological expertise: Practitioners and judges are generally less expert in the use of computer forensics or latest technology. Due to lack of expertise in digital evidence, they do not able to fully utilise the use and the effectiveness of digital evidence.
- Abuse of scientific language: As all the application are based on the coding There are many instances where evidence is distorted and using advanced technology, records such as photos, videos, and signatures are changed or falsified. This leads to unreliability of digital evidence.[22]
- Expensive and highly maintainable: Advanced technology is either too cheap or it easy to maintain. To install a complete system, it cost generally bit high. And to maintain the machines and data is tough task in developing country like India where pen paper system is prevailing, and people are redundant to change and accept new technology.

[18] Ibid
[19] Krati Jain, *Challenges faced by Digital Forensics*, LEGAL DESIRE, (Oct 27, 2023, 10:15 AM), https://legaldesire.com/challenges-faced-by-digital-forensics/
[20] Ibid
[21] Ibid
[22] Dr Ian Kennedy, *Presenting digital evidence in court*, BCS, (Oct 27, 2023, 10:15 AM), https://www.bcs.org/articles-opinion-and-research/presenting-digital-evidence-in-court

## VI. Some important judgement by Apex court on use of Digital evidence

One of the first cases to address the issue of admissibility of electronic evidence was State (NCT of Delhi) v. Navjot Sandhu[23], in which the Supreme Court held that even if a certificate under section 65B of the IEA (Indian Evidence Act) is not filed, it does not mean that secondary evidence cannot be mentioned. It held that the law allows such evidence to be presented in the cases mentioned in Section 63 and 65 of the IEA[24]. The court relied on the law under Section 63, stating that secondary evidence includes copies produced by mechanical processes to ensure accuracy of content.

In *Tomaso Bruno and Anr. vs. State of Uttar Pradesh* [25], the issue of admissibility of electronic evidence was once again dealt with by the Supreme Court of India. The Court held that computer-generated electronic records are admissible at trial if proved in the manner prescribed in Section 65B of IEA.

In another case In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Ors*[26], the Supreme Court held in this case that if the electronic record is first stored in a device that is part of a "computer network" or "computer system" and It is not possible to physically bring the network/system to the Court then secondary copies may be made along with the certificate specified in section 65B. [27]



## VII. Conclusion and future prospective of digital evidence

The field of digital evidence is new and growing. Potentially, digital evidence is an important new source of information that will help prosecutors obtain more conviction. Use GPS data to locate suspects at or near crime scenes, analyse text messages and emails to corroborate allegations, take incriminating photos on social media sites, and gather information about criminal associates from cell phone address books or social network metadata is just one way. Some of the ways in which electronic data provide police and prosecutors with information

[23] (2005) 11 SCC 600
[24] Aquib Husain, Dr. Eakramuddin, *Issues And Challenges Of Admissibility Of Digital Evidence: A Study*, INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT, (Oct 27, 2023, 10:15 AM), https://www.ijnrd.org/papers/IJNRD2306235.pdf
[25] (2015) 7 SCC 178
[26] (2020) 7 SCC 1
[27] Aquib Husain, Dr. Eakramuddin, *Issues And Challenges Of Admissibility Of Digital Evidence: A Study*, INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT, (Oct 27, 2023, 10:15 AM), https://www.ijnrd.org/papers/IJNRD2306235.pdf

sources that were not previously available.[28] As the type and sophistication of electronic media from which digital evidence can be collected increases, this type of evidence will become an essential part of the investigation and prosecution process for most people. all criminals. However, while the potential is great, leveraging digital evidence also poses significant challenges. i.e. lack of awareness, technological backwardness, privacy violations, data manipulation, etc. To overcome these problems, in September 2020, the Ministry of Home Affairs (MHA) of the Government of India passed two laws as National Forensic Science Universities (NFSU) Act, 2020 and Rashtriya Raksha University (RRU) Act, 2020. It provides for the establishment of regional educational and research institutions. In Gujarat, NSFU was formed and several RRUs were established in various cities like Gandhi Nagar.

Apart from being an amateur phase in the use of digital evidence in India, new innovative concepts are being introduced every day in different parts of the world and India is not lagging behind in implementing in state. The use of AI technology has been used to facilitate document review in legal cases. Law firms are investing in the use of AI and the legal services market is expected to grow. This means that in the future, practitioners may not only work with lawyers but also with new roles being created within the profession, such as legal data scientists and others works in the legal technology department.

Some authors, such as Richard Susskind, see a transformative future for the justice system with the rise of online courts. [29] Efforts are also being made to test the use of virtual reality in courts. Despite all these developments, there is still some scepticism about the growing use of technology in the courtroom due to its technical reliability and potential impact on vulnerable people, injured when participating in this process.[30]

[28] Sean E. Goodison, Robert C. Davis, Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System,* RAND CORPORATION (Oct 27, 2023, 10:15 AM), https://www.rand.org/pubs/research_reports/RR890.html

[29] Dr Ian Kennedy, *Presenting digital evidence in court*, BCS, (Oct 27, 2023, 10:15 AM), https://www.bcs.org/articles-opinion-and-research/presenting-digital-evidence-in-court

[30] Dr Ian Kennedy, *Presenting digital evidence in court*, BCS, (Oct 27, 2023, 10:15 AM), https://www.bcs.org/articles-opinion-and-research/presenting-digital-evidence-in-court

## REFERENCES

**Internet Sources:**


- Aquib Husain, Dr. Eakramuddin, *Issues And Challenges Of Admissibility Of Digital Evidence: A Study*, INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT, (Oct 27, 2023, 10:15 AM), https://www.ijnrd.org/papers/IJNRD2306235.pdf
- Dr Ian Kennedy**,** *Presenting digital evidence in court*, BCS, (Oct 27, 2023, 10:15 AM), https://www.bcs.org/articles-opinion-and-research/presenting-digital-evidence-in-court
- Fanny Ramirez, *Interpretive and Interpersonal Challenges of Digital Evidence for Public Defenders,* JOURNALS.KU.EDU (Oct 27, 2023, 10:15 AM), https://journals.ku.edu/hct/article/view/18826/19142
- Krati Jain*, Challenges faced by Digital Forensics*, LEGAL DESIRE, (Oct 27, 2023, 10:15 AM), https://legaldesire.com/challenges-faced-by-digital-forensics/
- Panjala Shreeya, Kaveti Vinisha, *Digital Forensics In India- An Overview*, LAW TIMES JOURNAL, (Oct 27, 2023, 10:15 AM), https://lawtimesjournal.in/digital-forensics-in-india-an-overview/
- Sean E. Goodison, Robert C. Davis, Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System,* RAND CORPORATION (Oct 27, 2023, 10:15 AM), https://www.rand.org/pubs/research_reports/RR890.html
- Syed Atir Raza, Aqsa Anwar, Abdul Hannan Khan, *Current Issues and Challenges with Scientific Validation of Digital Evidence,* INTERNATIONAL INFORMATION AND ENGINEERING TECHNOLOGY ASSOCIATION (Oct 27, 2023, 10:15 AM), https://www.iieta.org/journals/rces/paper/10.18280/rces.090304
- Tejas Karia, *Digital Evidence: An Indian Perspective,* LEXOLOGY (Oct 27, 2023, 10:15 AM), https://www.lexology.com/commentary/litigation/india/amarchand-mangaldas-suresh-a-shroff-co/digital-evidence-an-indian-perspective
- Vanshika Shukla, *The Admissibility Of Digital Evidence: Challenges And Future Implications,* THE LAWBRIGADE (Oct 27, 2023, 10:15AM),https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-ShuklaCLRJ.pdf?_gl=1*qkt937*_ga*MTk4MjgxNjcyLjE2OTg0ODA4MDY.*_ga_77Y54C8SBH*MTY5ODQ4MDgwNi4xLjAuMTY5ODQ4MDgwNi4wLjAuMA

**List of Statutes:**


- Constitution of India, 1950.
- Indian Evidence Act, 1872.
- Indian Penal Code, 1860
- Information Technology Act, 2000.


*******