

Judicial Reception of Digital Forensic Evidence in Indian Courts: A Study of Trends and Challenges

Ms. Tamanna Khatri¹, Dr. Grishma Bhavsar²

¹ Research Scholar, Faculty of Law, GLS University, Ahmedabad, Gujarat, India.
Email: tamannakhatri125@gmail.com

² Assistant Professor, Faculty of Law, GLS University, Ahmedabad, Gujarat, India.
Email: grishma.bhavsar@glsuniversity.ac.in

Corresponding Author:

Ms. Tamanna Khatri

Email: tamannakhatri125@gmail.com

Cite This Paper as: Ms. Tamanna Khatri, Dr. Grishma Bhavsar (2026) Judicial Reception of Digital Forensic Evidence in Indian Courts: A Study of Trends and Challenges..The Journal of African Development 1, Vol.7, No.1, 1506-1512

KEYWORDS

Admissibility, Cyber-Enabled Crimes, Digital Evidence, Digital Forensics, Forensic Science in Courts, Judiciary.

ABSTRACT

The rapid increase in cyber-enabled crimes has altered the dynamics of criminal investigation and adjudication in India, forcing courts to increasingly depend on digital forensic evidence. Ranging from mobile phone data and call detail records to Closed-Circuit Television footage (CCTV), emails and social media posts, digital evidence has become the pivot around which the guilt or innocence of the accused revolves. But the judicial acceptance of digital evidence remains irregular, influenced by concerns of authenticity, admissibility, procedural compliance and technological soundness. This research paper will investigate the response of Indian Courts, especially the Supreme Court of India and the High Courts, to digital forensic evidence over the past decade and examine how the courts have dealt with admissibility, evidentiary value, expert opinion and procedural requirements in digital evidence, while also highlighting issues relating to chain of custody, forensic certification and compliance under the Indian Evidence Act, 1872 and the recently introduced Bharatiya Sakshya Adhiniyam, 2023. The study also shows divide between the technological development of the investigative agencies and the courts' interpretation to evaluate complex digital forensic evidence. There are some decisions that reflect progressive approach towards accepting forensic science, others demonstrate caution and scepticism, often leading to exclusion or reduced reliance on such evidence. This paper concludes by emphasizing the need for the development of judicial guidelines and forensic protocols and improved forensic literacy among legal professionals..

1. INTRODUCTION

The advent of the digital age has also given rise to a new kind of crime which is either committed, facilitated, or proved through digital means. Cyber-enabled crimes like financial frauds or staling, as well as more modern ransomware crimes, have significantly impacted the landscape of criminal investigations and prosecutions in India. The new-age crimes demand new-age proof, which is why digital forensic evidence is an integral part of criminal investigations and prosecutions. This is the reason why the judicial system has borne the full brunt of these new-age crimes; courts are frequently asked to deal with such cases, wherein the most important evidence lies in digital form. It is either in the form of call detail records, GPS information, WhatsApp messages, email communications, or even Closed-Circuit Television footage (CCTV). Though such evidence is the key in proving one's innocence or guilt in such crimes, the utilization of such evidence in Indian courts is still in a state of flux. There is a number of challenges that the judiciary is faced with in the handling of such evidence that is of this kind. It is inherently technical in nature and is more prone to being tampered with.

The promulgation of the Bharatiya Sakshya Adhiniyam, 2023 represents a notable milestone in the legislative process to bring the standards of evidence in conformity with the requirements of modern technology. Nevertheless, the implementation and utilization of digital evidence in the judicial system raise several concerns, such as the lack of consistency in how the digital evidence is handled in courts, inconsistencies within the standardization process in relation to the authenticity of digital evidence, the chain of custody of digital evidence and the need for expertise in handling digital

evidence, among others. This paper aims to address these questions in detail by examining judicial trends, legislative developments and technological capabilities. In this study, we shall try to understand the judicial trend followed by the Supreme Court of India and various High Courts, wherein, while there have been some progressive trends witnessed, at the same time, some inconsistent and procedural difficulties have occurred leading to the neglect of digital evidence during trials. In the end, the goal of the research is to bridge the gap between the progress in investigations and the readiness of the judicial system with the help of insights and suggestions that might help in stronger integration of forensic evidence in the Indian judicial system.

NATURE AND SCOPE OF DIGITAL FORENSIC EVIDENCE:

2.1 Nature and Extent of Digital Forensic Evidence:

The term digital forensic evidence is used to define data that exists in electronic form and can be gathered for investigation or judicial proceedings. Digital evidence includes all kinds of data, which include mobile phones, computers, emails, social networking sites, Closed-Circuit Television (CCTV) camera, Global Positioning Systems (GPS) and even Internet of Things (IoT) technology.¹ It is important to note that digital evidence has a nature whereby it is intangible, volatile and often encrypted, making it difficult to handle. The most important feature of digital evidence is its vulnerability to manipulation if it is not handled with care. For example, if someone makes any alteration to the file, it can delete all its time stamps, raising questions of authenticity. Hence, special tools are used to handle digital evidence, which is essential for court proceedings as well.²

The digital footprint left behind by an individual, such as his browsing history, login records, phone records, messages and locations can be very useful in supporting other evidence. Digital evidence is often at heart of cases involving cybercrime, terrorism, organized crime and white-collar crime. In most modern crimes, digital evidence is at the heart of cases.³ The digital trial left behind by an individual, such as through browsing, login records, telephone records, messages and location information, can be very useful in corroborating other evidence or creating a timeline of events. In contemporary cases, especially in cybercrime, terrorism, organized crime and white-collar crime, digital evidence is at the heart of prosecution.⁴ The scope of digital forensic evidence in India has considerably broadened over the last decade. The relevancy of this evidence is no longer restricted only to cybercrime-related cases but it is an essential element in most other legal cases. For example: In the realm of criminal law, it is useful to track cases of financial frauds, cyberstalking and harassment. In cases related to family laws, it might involve extracting erased messages and pictures for proving the cause of divorce or resolving child custody conflicts. In corporate and intellectual property law, it is useful to determine cases of data theft and breached of contract. In relation to the matter of terrorism and national security, emails and chat logs have emerged as crucial evidence. Importantly, the scope also covers the legal procedure and mechanism relating to gathering, storing and retrieving such evidence. Legislations like the Information Technology Act, 2000, Indian Evidence Act, 1872 and recently the Bharatiya Sakshya Adhiniyam, 2023 decides the significance of such evidence.⁵

The extent of digital forensic evidence in the courtroom is influenced by the following significant factors: admissibility criteria (Sections 65A and 65B of the Indian Evidence Act, 1872), reliability of opinion offered by experts, forensic certification and hash values and adherence to the chain of custody. Despite its increasing importance in digital crimes, there is a general unawareness among judges and attorneys regarding the technical aspects of digital evidence. Furthermore, the lack of standardized procedures in different investigative authorities and judicial bodies, particularly lower courts, hinders the effectiveness of digital evidence and renders it irrelevant based on technical issues despite its relevance.⁶

2.2 Emerging Trends:

As the technology evolves, the ambit of forensics is expanding. The judiciary will have to increasingly take into account the following considerations: deep fakes, artificial media, AI content, end-to-end encrypted messages such as Signal or Telegram, blockchain transactions, cryptocurrencies, etc. The ever-evolving environment demands that both judicial bodies and authorities be trained not only in accepting newer forms of evidence but also in understanding the limitations of the technology involved.

LEGAL FRAMEWORK IN INDIA:

The legal framework concerning digital forensics in India constitutes a notable move from an age-old conventional system

¹ Eoghan Casey, *Digital Evidence and Computer Crime* (3d ed. 2011).

² Brian Carrier, *File System Forensic Analysis* (2005).

³ John R. Vacca, *Computer Forensics: Computer Crime Scene Investigation* (2d ed. 2005).

⁴ Peter Sommer, *Digital Evidence, Digital Investigations and E-Discovery*, 6 Digital Investigation 1 (2009).

⁵ Information Technology Act, No. 21 of 2000, India Penal Code, No. 45 of 1860, India.

⁶ Robin Verma, *Digital Forensics 2.0 Framework* (IIIT-Delhi)

to one that focuses on the use of technology. Specifically, while the Indian Evidence Act, 1872, a law that was enacted to suit the conditions at the time, has been updated by the amendment in accordance with the provisions of the Information Technology Act, 2000 to incorporate electronic records, the developments in cybercrimes and advances in technology have made it necessary to have a new law altogether. The need for such a change is seen in the creation of the Bharatiya Sakshya Adhiniyam, 2023. This new law will help deal with evidences in line with current technology trends. In this regard, both the Indian Evidence Act, 1872 and the Bharatiya Sakshya Adhiniyam, 2023 are discussed hereinafter.

3.1 Indian Evidence Act, 1872:

While it was drafted before the advent of digitization, Indian Evidence Act, 1872 was amended by way of Information Technology Act, 2000 by introducing Sections 65A and 65B, which established that electronic documents can be accepted as evidence. Nevertheless, the introduction of these sections made a very complicated legal framework of compliance. Section 65A provides special provisions for electronic records, wherein the records would follow the procedural requirements set out in Section 65B. Section 65B(1) provides the electronic records on optical and magnetic media made admissible subject to fulfilling certain criteria. Section 65B(4) discusses the controversial rule requiring certificate of authenticity to be issued by an individual responsible for the device, generating an electronic record.⁷ Even though the necessity for these changes could not be questioned, their implementation became difficult, especially after the landmark decision in *Anvar P. V. vs. P. K. Basheer*⁸, wherein the Supreme Court ruled strictly interpreting the provision and establishing that the absence of the certificate renders the document inadmissible despite its relevance. Later on, a more liberal approach in exceptional cases emerged in *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal*⁹, wherein it was ruled that there can be some exceptions to this rule. But the problem that was faced by the judiciary was that at times, due to procedural difficulties, it found itself unable to procure the certificate. Thus, there were instances when the judiciary's reaction to the use of digital evidence was inconsistent.

3.2 Bharatiya Sakshya Adhiniyam, 2023:

Acknowledging the limitations of the colonial era system, the Government of India enacted the Bharatiya Sakshya Adhiniyam, 2023, which simultaneously came into existence along with other amendments made to the criminal code. The object of this Act is to effectuate changes to bring about modernization of the law of evidence in tune with the present technology era.¹⁰

Some provisions in this Act include the following:

Equivalent of documentary evidence: There are numerous mentions of electronic records throughout the definition of evidence and documents, thereby making it evident that this form of evidence would be accepted in judicial proceedings.

Certification requirements: The newly enacted Act reiterates the importance of certification but permits digital signatures, hash value verification and metadata confirmation, a move towards harmonizing evidence and technology.

Chain of Evidence: This section lays stress on forensic reliability and chain of evidence to reduce risks of tampering with the evidence. Secure storage, handling and documentation of the evidence by authorized personnel are expected from courts.

Expert Opinion and Forensic Reports: This Act envisages increased acceptance of forensic evidence through provisions for employing digital forensic laboratories accredited by the government. However, there remain some issues regarding the qualifications and training of the same.

Definition: Various terms including “records in electronic form”, “communication device” and “information in electronic form” have been defined to broaden their interpretation.¹¹

JUDICIAL TRENDS AND CASE ANALYSIS:

The attitude of the judiciary of India towards the acceptance of digital forensic evidence has changes immensely during the past two decades with respect to the inclusion of technology with crime and investigations. This trend, however, shows

⁷ Indian Evidence Act, No. 1 of 1872, §§ 65A–65B.

⁸ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

⁹ *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

¹⁰ Law Commission of India, *Report No. 271, Human DNA Profiling – A Draft Bill for the Use and Regulation of DNA-Based Technology* (2017).

¹¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023.

a lack of uniformity because although there have been judgments wherein digital evidence was accepted, there have been other cases where the judiciary has shown conservatism due to lack of adherence to procedural formalities.

4.1 Supreme Court's Stance:

Growing with Prudence India's Supreme Court has always played an important role in shaping the jurisprudence of digital evidence. One of the important trends adopted by the Supreme Court has been the importance of adherence to procedure, especially with respect to the procedure for the certification of electronic documents under Section 65B of the Indian Evidence Act, 1872, which was subsequently preserved in the Bharatiya Sakshya Adhiniyam, 2023.

The early case law on this issue includes **State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru**¹²: In this case, the admissibility of electronic evidence was challenged by the defence side since there was no certificate under Section 65(B)(2) of the Indian Evidence Act, 1872 which is needed to make the record admissible. The validity of the mobile phones' call records was questioned by the defence side. The Court admitted electronic evidence (telephone records) without any Section 65B certificate on the grounds that there could be secondary evidence to prove this electronic record in terms of other provisions of the Evidence Act. It was considered a pragmatic approach to the matter.

However, such a liberal view was rejected in **Anvar P. V. v. P. K. Basheer**¹³: This case is an example of an election petition wherein there was a complaint of corrupt practices committed by Respondent 1 under Section 100(1)(b) and Section 123(4) of the Representation of the People Act, 1951, where in the speeches, songs and announcements were made by him in such a way as to prejudice the prospects of the appellant and it had a material effect on the result of his election. Compact Discs (CDs) (electronic evidence) are considered inadmissible in Indian Courts where there is failure to prove certificates as per the requirements laid down in Section 65(B) of the Indian Evidence Act, 1872. The Court in this case held that Section 65B(4) certificate is mandatory for admitting electronic records as evidence and it cannot be substituted by oral evidence or other forms of secondary evidence. Thus, there was a complete shift from the Navjot Sandhu approach.

Sonu v. State of Haryana¹⁴: In this case, the Apex Court of India upheld the conviction of the accused, even though one of the most essential pieces of evidence, which are Compact Disc-Recordable (CDRs), were produced before the Court without the requirement of a certificate under Section 65(B) of the Indian Evidence Act, 1872. The Hon'ble Court did not consider the ratio laid down in the Anvar Case, where a three-judge bench ruled on the matter. In addition, the division bench did not rely upon the decision made by the three-judge bench and ignored the arguments of the accused that evidence against him should be inadmissible since it does not satisfy the requirements of law.¹⁵

Tomas Bruno v. State of U.P.¹⁶: According to the Apex Court of India, normally it is not required for an appeal court to intervene in the judgment of the lower court unless it found any gap in the evidence presented before the Hon'ble Court. However, when the decision depends upon the circumstantial evidence, then it becomes imperative for the prosecution to prove the fact beyond reasonable doubt. The Hon'ble Court has observed that if an issue depends on any critical situation, then we cannot neglect such significant evidence. According to the facts and circumstances of the case presented before the Hon'ble Court, the Closed-Circuit Television (CCTV) footage becomes the deciding factors. It was found that there was no gap in the circumstantial evidence as well. Hon'ble Court has also observed that CCTV footage is very significant and it was unfortunate for the Court to neglect this type of important evidence. As CCTV footage is the electronic evidence, so it falls under the provision of Section 65(A) and 65(B) of the Indian Evidence Act, 1872. It must be remembered that it may not always be a mandatory condition under Section 65(B) in every case to have an issuance of a certificate when it comes to the question of reliability of the documentary evidence being produced before them by the Hon'ble Court. The Hon'ble court must satisfy itself of the reliability of the electronic documentary evidence being presented to it.

This strict position was further explained in the following decision, **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**¹⁷: The Apex Court in this case has already affirmed the ruling of the Anvar P. V. Case. The recording of statements by the Hon'ble Court about the admissibility of electronic evidence would not be regarded as legitimate in light of the necessity for the certificate. The main evidence need not abide by the stipulations provided for under Section 65B of the Indian Evidence Act, 1872. This is because whenever the document itself is tendered for inspection in court, no certificate will be needed according to the procedural requirements of Section 65B of the Indian Evidence Act, 1872. If the original documents like laptop, computer, tablet, mobile phone, etc (primary evidence) are produced then the provision of

¹² State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.

¹³ Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

¹⁴ Sonu v. State of Haryana [(2017) 8 SCC 570]

¹⁵ M.D. Chhatrapati & D. A. B. Prasad, Electronic Evidence–Admissibility and Authentication: A Judicial Perception of Apex Court of India, 3(1) *GLS Law Journal* (2021).

¹⁶ Tomas Bruno v. State of U.P., (2015) 7 SCC 178

¹⁷ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.



Section 65(B)(4) is not essential. If it becomes impossible to produce the original documents (electronic device/system/server) then it would become necessary to prepare copies from the original documents and the same would be presented along with the requisite certificate in accordance with Section 65(B)(4) of the Indian Evidence Act, 1872. It stated that although 65B certificate was necessary, there was no prohibition in the statute in exercising discretion when such a certificate cannot be provided by the side producing the electronic records due to their possession by third parties. Thus, the approach of the Supreme Court seems to follow a delicate balance between rigidity and pragmatism.

4.2 Observations of the High Courts:

From the High Courts' observations regarding the trend in judiciary with respect to digital forensic evidence, it is evident that there is much variance, which can be explained in terms of procedural issues and the presence of forensic experts.

Liberal approach: The High Courts in Bombay and Delhi have taken a liberal approach wherein the presentation of digital evidence is possible without the use of Section 65B certificates as long as its reliability is not put into question.

Approach of Literal interpretation: Literal interpretation was adopted by the Madras High Court and even Kerala High Court where anything that doesn't satisfy the requirements set out under Section 65B(4) has been considered as inadmissible.

Illustration: For instance, in case of **Shafhi Mohammad v. State of Himachal Pradesh**¹⁸ case, it was held by the two-judge bench of the Supreme Court that the decision rendered in Anwar was disregarded and the admissibility of electronic evidence was allowed when Section 65B certificates were unattainable. However, this standpoint was invalidated in the case of Arjun Panditrao.

The inconsistent application of these laws across different legal systems has led to a fragmented set of standards, causing confusion in many cases. In some of the more important criminal cases where digital evidence has played an important part, for example, death in police custody captured by Closed-Circuit Television footage (CCTV) and financial fraud committed by email, the verdict has depended upon the issue of certification.¹⁹

SYSTEMIC CHALLENGES IN ADJUDICATING DIGITAL FORENSIC EVIDENCE:

There are a number of systemic problems involved in the judicial assessment of digital forensic evidence that act as barriers in the effective use of this technology in the criminal justice system. In spite of all the developments in legislation, the translation of the scientific findings of the technological process of forensics to an admissible and persuasive evidence continues to pose challenges.

5.1 Issues related to Chain of Custody:

A chain of custody is essentially the chronological and systematic recording of the seizure, custody, control, transfer, analysis and ultimate disposal of physical evidence from the point of its discovery until it is ultimately used in the court, an idea that is discussed in the Black Law's Dictionary.²⁰ While chain of custody as such does not find mention in any statute in India, the concept is nevertheless evident in the form of the legal principles of evidentiary authenticity and reliability as enshrined in Indian Evidence Act, 1872 and Bharatiya Sakshya Adhiniyam, 2023, as well as the procedures adopted by the investigation and forensic agencies. However, for digital evidence, the need to establish a proper chain of custody assumes great importance because digital evidence, is extremely vulnerable to manipulation and forgery.²¹ This vulnerability has made it necessary for courts in various cases in India to either ignore or simply disbelieve the digital evidence. Moreover, since there are no clear guidelines regarding the process of seizure, labelling, transfer and storage of electronic devices, it makes it difficult for courts to accept digital evidence.²²

5.2 Expert Opinion and Judicial Understanding:

Finally, there is the serious problem of relying heavily on the opinion of an expert to make sense out of complex forensic information. The analysis of metadata, encryption keys, timestamps, or hash codes necessitates technical skills in the domain of digital forensics.²³ Judges, lacking formal education in digital forensics techniques, frequently turn to governmental or privately-owned forensic labs or experts to help them understand these processes. The problem with this approach, however, is as follows:

The risk of accepting evidence that one does not understand.

¹⁸ Shafhi Mohammad v. State of Himachal Pradesh, (2018) 5 SCC 311.

¹⁹ Pratyusha Das, *Role of Forensic Evidence in Decision-Making*, KIIT University (2016).

²⁰ Black's Law Dictionary (11th ed. 2019).

²¹ Paul C. Giannelli, *Scientific Evidence* (5th ed. 2012).

²² National Institute of Justice, *Digital Evidence in the Courtroom* (U.S. Department of Justice).

²³ Indian Evidence Act, 1872, § 45.

The opposite risk undermining the value of report due to scepticism in one's ability to assess its veracity.

Concerns regarding the credibility of experts who do not have a nationally accepted certification.

In conclusion, such issues contribute to judicial uncertainty in relation to digital forensics.²⁴

5.3 Diversity in approach to Digital evidence by different Benches:

One of the major problems that have been observed while analyzing cases relates to the difference in approaches taken by different benches of the same high court or even different high courts when dealing with digital evidence. Some benches take a more liberal approach to the handling of evidence by considering its relevance and context, while other benches take a very rigid approach where Section 65B certification becomes mandatory irrespective of its practicability. Such diversity creates uncertainty in the outcome of cases and weakens people's faith in the judicial process.²⁵

COMPARATIVE OBSERVATIONS: INSIGHTS FROM THE USA AND UK LEGAL FRAMEWORKS:

India is currently facing a crossroads in amending its legal framework for evidence in response to the modern-day realities of digital information forensics. Meanwhile, there exist several examples from other jurisdictions like United States of America (USA) and United Kingdom (UK) that can serve as templates for creating an evidence rule system that would allow a more accurate assessment of digital forensic findings. As the complexities of cyber laws increase, the need for lawmaking processes has also emerged.²⁶

6.1 United States of America: Daubert Test and Judicial Education:

There is also a standard that exists in the United States known as the Daubert test, which was set forth in the judgment of *Daubert v. Merrell Dow Pharmaceuticals*²⁷. In accordance with this test, the evidence will be considered admissible when:

The witness' opinion is based on scientifically sound reasoning.

The procedure followed is verifiable, reviewed by peers and recognized across the board.

The evidence is useful to the trier of facts.

The Federal Rules of Evidence (FRE) include Rule 702 that determines what is required of an expert witness whose testimony is sought. It ensures that only scientifically legitimate and relevant evidence will be considered by the court. Additionally, judges are trained to recognize flaws in forensic methods through programs run by the Federal Judicial Center.²⁸

6.2 United Kingdom: Codes of Practice and Accreditation:

For digital evidence collection, disclosure and utilization in the UK, the Criminal Procedure and Investigations Act, 1996²⁹ (CPIA, 1996) and Police and Criminal Evidence Act, 1984³⁰ (PACE, 1984) are implemented. Under the Forensic Science Regulator (FSR), there are some codes of practice that are obligatory. These codes include:

Accreditation of digital forensics service providers (ISO/IEC 17025)

The procedures involved in handling, imaging, analysis and preservation of digital evidence.

Chain of custody documentation with timestamps and qualifications of the analyst.

Additionally, UK courts should consider the significance of digital forensics by utilizing judicial case management, where pre-trial hearings involve the format and scope of expert testimony in the trials.³¹

CONCLUSION:

The rising trend of employing digital forensics as an approach to collecting evidence in Indian criminal cases is a landmark in administering justice in the digital age. In light of call detail records, mobile data, emails and cloud storage media, digital evidence has become the norm in terms of investigations and trials. This new paradigm, however, is fraught with

²⁴ State of H.P. v. Jai Lal, (1999) 7 SCC 280.

²⁵ Shubhi Mack, *Impact of Forensic Evidence in Criminal Justice: A Socio-legal study in Indian Perspective*, Adamas University (2022).

²⁶ M. S. Patel & S. Raval, Global Approaches to Intellectual Property (IP) Protection in Digital Realm and Cyberspace Governance, 7(2), *GLS Law Journal*, 65 - 87. (2025)

²⁷ *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993).

²⁸ Fed. R. Evid. 702.

²⁹ Criminal Procedure and Investigations Act 1996 (UK).

³⁰ Forensic Science Regulator, *Codes of Practice* (UK).

³¹ European Union Agency for Cybersecurity (ENISA), *Threat Landscape Report 2023*.



complications.

As some of the court cases indicate an understanding of the situation, other decisions are marred by lack of consistency in the handling and interpretation of digital evidence. The gap between the abilities of the investigative organs and those of the judiciary is evident and calls for immediate reforms. In order for India to be able to address the complexities in the prosecution of cybercrimes, there needs to be the creation of a clear link between law and technology.

This issue can only be addressed through a multilayered approach. There needs to be a pressing need for creating guidelines for collecting, preserving and presenting digital evidence. Also, judicial education programs are equally important to address the lack of technology-related issues amongst judges and other legal professionals. Moreover, a greater dependence on forensic experts and better infrastructure within courts would be helpful in this regard. To conclude, if India wants to successfully address the issues related to the prosecution of cybercrimes and digital evidence, it is essential to develop synergy between law and technology. Developing such synergy will not only make the legal process credible and reliable, but also make it more vigorous against future challenges.

The comparative analysis of legal systems such as the United States and the United Kingdom reveals certain reform initiatives which can be considered by India to improve its digital forensic practice. There is an urgent need to adopt a judicial gatekeeping process, similar to the Daubert standard, which will help guarantee the reliability of scientific validity of forensic evidence before courts. Similarly, the creation of an accreditation system for forensic experts will ensure objectivity and professionalism in forensic reporting. The creation of a comprehensive and standardized Standard operating procedures (SOPs) is also necessary to ensure consistency in collecting, analyzing and preserving digital evidence, thereby reducing the chances of procedural mistakes. Furthermore, the training of judges and prosecutors regularly to equip them with updated knowledge about digital forensic practices would go a long way in helping them make sound judgements..