WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Role of Digital Forensics and Criminal Investigation in India

Deepali[1], Prof. (Dr.) Radhika Dev Verma[2]

[1]LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India
[2]Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

ABSTRACT

Digital forensics has been adopted now as a useful tool in the criminal justice system of India for handling difficulties concerning cyber crimes and digital evidence. Based on the doctrinal research methodology, this study analyzes the role, issues, and development of digital forensics in India concerning pertinent legal provisions of the Indian Information Technology Act, 2000, Bharatiya Sakshya Adhiniyam 2023, and Bharatiya Nyaya Sanhita 2023. Using the international comparison, the research reveals some key challenges, including the absence of well-defined protocols, compromised accreditation in forensic laboratories, and inadequate training of judicial and enforcement agencies. Issues such as the impossibility of encrypting, the use of anti-forensic tools, and non-reformist provisions previously cited, including tribulations associated with stringent electronic evidence certification rules under Section 63 of the Indian Evidence Act, effectively affect the input of such evidence in Indian courts. The problematic issues are, for instance, the rights of privacy during the collection and analysis of digital evidence. The outcomes of the study highlight issues of implementation of international practice, including using protocols for the handling of evidence, improving training, and increasing international cooperation. Based on the research, it can be said that significant enhancement of the aggregate of digital forensic standards can enhance significantly India's stance in supporting a contemporary technologically progressive justice system that is fair for today's complex crimes.

Keywords: Digital forensics, cybercrime, Information Technology Act, Bharatiya Sakshya Adhiniyam, electronic evidence

1. Introduction

The advancement of technology and the availability of new gadgets in use have significantly altered criminal investigations across the globe and in India as well. Digital forensics have become an essential component in fighting and investigating cyber and other incidents that involve digital evidence. Computer forensics in India and computer forensics investigations as a recent tool of investigation are used in the context of modern complex crimes; following this, electronic evidence is even more prevalent. With increasingly frequent hacking, phishing, cyberstalking, and online financial fraud, legal security agencies have the problem of combating crime using modern technologies while conforming to the legal provisions of capturing, preserving, and presenting digital evidence.[1]

India has not been behind the world in this regard. The Indian legal provision to address digital evidence has gone through amendments, especially in the year 2000 with the enactment of the Information Technology Act, 2000 ("IT Act, 2000"). However, several shortcomings are observed, as follows: legal issues, legal gray areas, limitations in the existing laws, and legitimate shortcomings in the ability of the police force to deal with digital forensics. It has now become clear that the problem of developing a full-bodied picture of digital forensics as an issue belonging to the sphere of criminal investigation is more urgent than ever before. This understanding must also hold these and other factors along with legal procedures and judicial considerations to be knowledgeable about, as the credibility and admissible use of digital evidence often attract controversies in courtrooms.

Digital forensics involves the use of forensic science methods to collect, examine, and process digital information to fit legal processes. This field is especially suitable in criminal investigations as it makes available to law enforcement agencies tools to reveal concealed information, find out the source of cyber conduct, and verify the originality of electronic material. Still, the implementation of digital forensics in the Indian criminal justice system faces several challenges: procedural, legal, and having no set best practice in place about electronic evidence. This use of digital evidence also brings additional important concerns about the privacy of individuals and the propensity of misuse of technology by police.

This peculiar discipline appeared in practice: mistakes investigate technologies for giving solutions to crimes in devices and the internet. Digital forensics has been in force in India since the increase in the usage of internet services and mobile technologies. Computer and mobile crimes have become rampant, and therefore digital evidence plays a central role in investigation processes. The "IT Act, of 2000" and its amendments have been the most instrumental legislation to contain the legal recognition for cyber-crimes as well as the digital evidence system in India. Among aspects that can be highlighted in the Act are definitions and legal treatment for different cybercrimes, data protection, and security questions.

[1] Vaibhav M. Agrawal, "Critical Analysis of Forensic Science in Effective Administration of Criminal Justice System in India", 12 *Indian Journal of Law and Legal Research* 78 (2023).

Digital forensics is a significant investigation procedure in searching for evidence of cybercrimes like hacking and data break-ins, apart from conventional crimes where computer records may be important. Investigations can comprise different aspects; this includes how to recover deleted files, how to track the IP addresses of individuals, how to understand the communication system used in computers and even the geographical position of a suspect given through GPS. Whether it is in cases of cybercrimes, financial fraud, cases of online defamation, or an offense under the 'Protection of Children from Sexual Offenses Act, 2012', therefore, digital forensics is relevant. However, law enforcement agencies in India struggle with challenges and barriers like poorly developed infrastructures, a lack of expertise in digital investigation, and a lack of standardized, formulated policies and procedures in connection with digital evidence in different regions.

This study main purpose is to analyze and evaluate digital forensics to offer a critical reflection on its deployment in criminal investigations under the Indian legal system. The purpose of this research is to assess the examination of digital forensic material in criminal proceedings, concentrating on practical aspects, regulation, and case law. It also aims to determine the gaps in existing laws as well as provide recommendations aimed at enhancing the effectiveness and trustworthiness of digital forensics in criminal justice processes. As a result of reviewing the case laws and statutes that guided in this, the study will provide a clear picture of the role of digital forensics in the criminal justice system of India.

This research addresses several key questions: Finally, the following research question: How is digital forensic evidence collected and presented in the Indian criminal justice system? Independent of the nature of the crime committed, how has the contemporary legal system of operation provided for the admissibility of digital evidence in criminal trials? What does the Indian judiciary understand by digital forensic evidence, and how do they use it when making their decisions?[2]

2. Understanding Digital Forensics

Digital forensics has become one of the most important components of modern investigation, demonstrating the role of technology in today's society. Digital forensics is therefore the extraction, identification, analysis, and reporting of electronic digital media that is computer-based, including phones and networks, for use in legal processes. When people first began to speak about digital forensics, it was mainly about simply recovering deleted files or analysing hard disk drives of computers; today, however, the term has grown to cover far more grand concepts such as decrypting encrypted data, tracking an attack backward to its source, and authenticating digital signatures. This division of forensics has proven invaluable not only in solving computer crimes but also in backing traditional police work where reference to a piece of digital evidence may be useful. Digital forensics serves a dual purpose: it helps in suspect identification and also helps in proving the series of events, so it helps in fulfilling the principles of justice, particularly in proving data that is electronic so that it was collected and handled legally.[3]

2.1 Definition and Evolution of Digital Forensics

Thus, digital forensics, as the subdiscipline of forensic science, is aimed, on the one hand, at the legal and, on the other hand, at the efficient extraction, identification, analysis, and documentation of digital data stored in computer systems and computer networks. When the concept of digital forensics was introduced, it mainly dealt with computation systems, but as technology grew, the cases of it expanded to reflect more on devices such as smart devices, tablets, cloud storage, and even the Internet of Things (IoT) devices. The main focus of performing digital forensics is to collect and examine data that could help identify a criminal or their accomplices. Because computers and mobile gadgets have invaded almost every sphere of our lives, even those offenses not directly connected with computer crime can be helped by digital forensics: for instance, when the electronic notes can describe where the offenders are, give out details of the communication, or multiple financial transactions.

The history of digital forensics/discipline as a recognized academic field is relatively recent, beginning at the end of the Twentieth Century with the emergence of the PC and the Internet, which created a new need for coming up with new ways of handling new crimes like hacking, unauthorized access, or break-ins on computer systems. The progression moved to mobile technology, where smartphones became almost a must-have item, and many of them stored large amounts of personal information and matters of national importance, thus making the field of digital evidence even broader. In the Indian context, the legal recognition of cybercrimes and their evidence started with the passing of the Information Technology Act 2000. The Act, along with later amendments and the relevant provisions of "Bharatiya Nyaya Sanhita, 2023" and "Bharatiya Sakshya Adhiniyam, 2023," have been instrumental in dealing with cybercrime and defining standards for the electronic records that were admissible in the court of law. As it is, however, there are still areas of legal and procedural ambiguity in which digital forensics and its application and limitations in criminal investigation are not adequately covered, including complexities relating to jurisdictional boundaries, the ephemeral nature of digital evidence, and the correspondingly short lifespan of the technology.

2.2 Types of Digital Forensic Analysis

Digital forensics includes several categories of analysis, all different; each of them has different methods of use and difficulty for the different kinds of evidence and crimes. A common form is computer forensics used in handling civil and criminal matters by analysing data on desktop and laptop

[2] Sadhna Gupta, Meghali Das, "Criminal Investigation of Electronic Evidence: Challenges Faced with Digital Forensics", 2 *Journal of Forensic Justice* 97 (2023).

[3] Hemlata B. Patil, Anjula Chowbe, "An Examination of Digital Evidence and Its Relevance for Indian Forensic", 30 *Educational Administration Theory and Practice* 112 (2024).

computers, including retrieval of deleted data, analysis of system logs, and detection of malware or unauthorized access. Computer forensics can often become valuable in cases of fraud, piracy, or hacking since evidence in electronic form may be present in a case. Computer forensics processes and procedures encompass data carving that involves extracting deleted files without the use of the file system metadata, while memory forensics examines the computer's volatile memory with the view of pulling out evidence of malicious software or activity.

Another significant branch is mobile forensics, which is connected to the investigation and identification of data on operational mobile devices such as cell phones, tablets, and others. Since mobile phones contain call logs, text messages, emails, GPS locations, and social media activity, as well as photographic and video content, which they found when people had no other means of recalling it, these devices serve as powerful evidence in cases including kidnapping, terrorism, cyberstalking, and drug trafficking. In other cases, mobile operating system security mechanisms like password protection or encryption have to be violated by using tools like Cellebrite or Oxygen Forensic Detective and get access to the data. In addition, another branch of the discipline, cloud forensics, can take on the problems of data that is stored on distant hosts, such as Dropbox, Google Drive, or iCloud, for example.

The last of the key sub-disciplines is network forensics, which entails the analysis of actual network traffic in a bid to investigate or look for specific security threats such as unauthorized access, DoS attacks, or data leakage. It is possible to learn the point of entry of the unauthorized user, and the type of intrusion, follow the transfer of data on the network, and help identify the assailants. It ordinarily includes packet sniffing tools, intrusion detection systems, and network protocol analysers to capture and scrutinize the data that packets travel in a network.[4]

Besides these, there are other digital forensics subcategories, including database forensics, which focuses on structured data in the databases, and forensic audio & video, which focuses on validating the digital recording or recovering damaged multimedia files. Every kind of forensic analysis has its tools and skills; it demands and needs the case to determine which type to apply. In the context of the legal laws of India, it is pertinent to note that the admissibility of such evidence and its authenticity are governed by statutes like Bharatiya Sakshya Adhiniyam, 2023, that specify the admissibility in court of digital evidence.

3 Legal Framework Governing Digital Forensics in India

Over the decades, legal provisions related to digital forensics in India have largely been based on statutes that deal with the issues surrounding the admissibility, credibility, and handling procedures of e-oriented evidence. With new types of computers and cybercrime, as well as any other criminal offense involving digital evidence, the legislative framework has had to evolve to support the fusion of digital forensics with criminal justice. The Information Technology Act of 2000 and its amendment regulate the field of cyber law in India; however, the recently passed Bharatiya Nyaya Sanhita, 2023, has incorporated some recent provisions relating to the offenses and the procedural laws that were required for the digital era. However, difficulties in the process of legal interpretation, legal regulation, and the development of new types of information and communication technologies remain, and, thus, there is a further need for judicial control. This study has outlined the most important legal provisions governing cybercrime regulation in India and the role of digital forensics in the country.[5]

3.1 Overview of Relevant Legislation

Most of the laws governing Cyber Crimes and disposition of Cyber Crimes space evidence in India rely on the “IT Act, 2000." cyber-criminal acts, i.e., hacking (“Section 66”), cheating by impersonation (“Section 66C”), and identity theft by constant stalking (“Section 66A"), but struck down in “*Shreya Singhal v. Union of India*[6]”, and provides for these offenses. As is the case with the USA and as is seen in Table 6, the Act also gives legal recognition to electronic records and digital signatures and hence permits the use of electronic evidence in judicial proceedings to the same extent as traditional evidence. Also, “Section 79” of the “IT Act, 2000” has contained a safe harbour provision regarding the intermediaries’ defending activities of third parties and provided that the intermediaries agree to abide by guidelines for blocking access to unlawful contents as well as preservation of data. The provision will be of paramount importance for the gathering of digital evidence because the police or other enforcement agencies may require the assistance of other third parties, such as the intermediary, usually a telecommunications company or social media firm, to assist in investigating a crime.

In the procedural law context, where such provisions are already in place, “Bharatiya Nyaya Sanhita, 2023” (BNS) has reformed certain sections of the old Indian Penal Code to bring more proficiency in cybercriminal cases. For example, the BNS encompasses offenses like cyber terrorism and electronic fraud, which show the high potential of crimes as a tool that uses technologies. It also deals with several matters regarding the taking into possession, preservation, and tendering of digital evidence in criminal processions, which have become the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). The BNSS empowers the police to search for and seize electronic devices and data storage media, while certain procedures have been imposed to provide safeguards to the admissibility of digital evidence. In addition, the BNS and BNSS stress the idea that digital evidence must be properly chained out of custody, as its alteration or any attempts to interfere with it are likely to render digital evidence inadmissible in a court of law.

The newly enacted “Bharatiya Sakshya Adhiniyam, 2023,” has repealed the Indian Evidence Act and channelled a new approach to issues of admissibility, standards for presenting digital evidence, etc. The Act does, however, affirm electronic records as admissible under specific conditions given in ‘Sections

[4] Harjinder Singh Lallie, "An Overview of the Digital Forensic Investigation Infrastructure of India", 9 *Digital Investigation* 3 (2012)

[5] Kunal Kanwat, "The Role of Forensic Evidence in Criminal Investigations in India", 12 *International Journal of Creative Research Thoughts* 117 (2024).

[6] [2015] 5 SCC 1.

62 and 63'. These sections state the conditions under which electronic records will be admitted as evidence; this places the requirement of having a certification on the records by an authorized person who can testify to the same. The judgment in "*Anvar P.V. v. P.K. Basheer*" [7] had a drastic change in legal methodology regarding digital evidence by adding that electronic records can be admitted only and only where they satisfy the provisions of Section 63 of the Indian Evidence Act, which has now been undergone by Bharatiya Sakshya Adhiniyam. The ruling on digital evidence stated that any electronic documents, such as emails or digital photographs, must also have a certificate of their authenticity, which creates the benchmark to ascertain the electronic documents in the law courts.

3.2 Admissibility of Digital Evidence in Indian Courts

The admissibility of digital evidence is controlled by principles related to the originality of digital evidence, reliability of the digital evidence, and relevancy of the offer in the court of framers of Indian justice system. Bhartiya Sakshya Adhiniyam, 2023 of Bharat contains "Section 63" to describe the process of proof of electronic records. The provision also demands that a certificate stating how the electronic record was created, the identity of the device that used it, and a declaration by the person making it to the legal sufficiency of the evidence be attached to it. This procedural precaution is meant to cope with doubts as to the change or fabrication of digital information, hence serving as protection from the admission of biased, false evidence. However, what many have criticized for demanding technical adherence by way of Section 63 has also received criticism for offering an extremely narrow provision for parties seeking to introduce electronic evidence, especially where it becomes virtually impossible to obtain the said certificate.[8]

Therefore, the understanding of the Supreme Court to the Section referred to as 63 has been extraordinary in determining the legal position of digital evidence. In the case of "*Anvar P.V. v. P.K. Basheer*" [9],the Court pointed out the compulsory character of the certificate in question and dismissed electronic records that otherwise were inadmissible without a proper Section 65B certificate. This decision has reversed an earlier judgment, i.e., *State (NCT of Delhi) v. Navjot Sandhu*[10], it was held that electronic records could be brought as secondary evidence even absent such certification. Since the ruling in 'Anvar', other cases have also sustained it to confirm the demanding need to follow the statutory provisions on digital evidence. However, the judiciary has also acknowledged some difficulties that are connected to such requirements, especially in cases when the original electronic copy is lost or certification cannot be received. That is why it is suggested to change the legislation relating to such matters.

In the landmark case, "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[11]", certain uncertainties surrounding "Section 65B" were explained again. The Supreme Court further held that though the certificate under Section 65B makes the digital evidence inadmissible without the same, it may be allowed to be produced later if it is at all impossible to obtain the same at the time of filing. This interpretation aims to perform a role that tries to entrench proper procedural provisions against the backdrop of the practical details without allowing justice to be stalled or denied on account of formalities. The judgment communicates a sensible attitude toward incorporating into its methodology the dynamic nature of digital evidence without violating the principles of legal certainty or procedural fairness.[12]

3.3 Role of the Indian Judiciary in Interpreting Digital Forensic Laws

The Indian judiciary has effectively been involved in a kind of law-making process by interpreting digital forensic laws while setting up the legal parameters relating to electronic evidence. From authority decisions, the courts have dealt with issues of uncertainty of statutory provisions and laid down a procedural regime for dealing with digital evidence. For instance, in *K.L. Nagadev v. State of Karnataka*[13], the Karnataka High Court touched upon a topic of admissibility of electronic evidence that was obtained from a digital storage device wherein the state had not strictly followed the provisions of the code of criminal procedure relating to seizure of the device, and therefore an important discussion on chain of custody arose. In the same way, they helped to interpret procedural safeguards under section 79A' of the 'Information Technology Act, 2000', which inspires the appointment of government-authorized digital forensics experts that would reasonably reduce chances or risks of seizing of digital evidence being tampered with or innocent people being framed for crimes committed. This change of heart from the judiciary means that legal analysis of these crimes still has to be updated to keep pace with technological advancements and the ever-developing facet of computer criminality.

4. Challenges in Digital Forensics and Criminal Investigation in India

The use of digital forensics as an investigatory tool is extensively used in current criminal prosecutions and cases. In India, however, applying digital forensics in the legal system has multiple issues. These challenges cut across technical, legal, and procedural, as well as ethical, arenas, which creates practical and impartial challenges towards the effectiveness and impartiality of the criminal justice system in processing and analysing digital evidence.

---

[7] [2014] 10 SCC 473.

[8] J K Verma, *Bharatiya Sakshya Adhiniyam, 2023 (Evidence): A Commentary* 180 (Eastern Book Company, 1st edn., 2024).

[9] [2014] 10 SCC 473.

[10] [2005] 11 SCC 600.

[11] [2020] 7 SCC 1.

[12] Supreme Court on the Admissibility of Electronic Evidence under Section 65B of the Evidence Act, *available at:* https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/ (last visited on October 15, 2024).

[13] [2019] SCC OnLine Kar 669.

Because technology is dynamic, any solutions provided for digital forensics must also have the ability to address matters of concern like encryption, new data instability, use of anti-forensic tools, and question marks in the legal systems that surround digital evidence. Also, the question of who has the right to privacy when facing an opponent who, using digital forensics tools, conducts legal and LLC activities also raises the issue of ethical standards and ad hoc procedures. Due to the increasing significance of digital evidence in the Indian criminal justice system, it becomes important to study these challenges to know their effects on investigations and to look for possible solutions.[14]

4.1 Technical Challenges

Amidst the technical challenges are the ones attributed to growth in technology and inherent properties of the digital evidence. Encryption is one of the biggest challenges for any digital investigation, mainly because when data is encrypted using a strong encryption standard, there is close to no way investigators can access the data without the decryption key. For instance, in communication applications such as WhatsApp, when digital devices employ end-to-end connection encryption, the service providers themselves cannot access the communication data, hence complicating the investigation of cybercrimes and other offenses where encrypted data may be vital in investigations. Widespread use of encryption is compounded by the presence of anti-forensic tools that are specifically designed to prevent the process outlined above. These tools can conceal or delete information; falsify dates and times; or generate erroneous information that can complicate efforts by investigators to retrace the original data and its origin. Other methods, such as steganography, where there is an embedment of data into other files, also make it difficult to detect and retrieve the evidence.

The other important technical factor that needs to be addressed is a technical factor that refers to the consistency of data that changes frequently and is also susceptible to change quickly. Although it may be possible to shred written documents and it is very easy to alter or delete electronic data, the integrity of the evidence is an essential issue in digital forensics. For instance, data that is stored in a computer's RAM (random access memory) may be erased when the machine is shut off, and so solving the crime may involve very swift and specialized capture of volatile ESI. Moreover, further problems arise with cloud computing and remote storage in connection with jurisdiction and accessibility of the evidence because the data may be hosted in different countries receiving different data protection laws. Such technical challenges require sophisticated forensic technologies, properly skilled professionals, and an understanding of best practices regarding the preservation and handling of digital evidence to make certain that this evidence will be collected and investigated by these requirements.[15]

4.2 Legal and Procedural challenges

The issues of legal and procedural framework are closely connected with the admissibility and credibility of digital evidence in India. The regulatory laws, which include the IT Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023, though partially helpful, adaptation to the fast-growing technology has not yet been addressed efficiently. One of the major problems is the compliance with requirements set under "Section 63" of "Bharatiya Sakshya Adhiniyam, 2023," which provides for the furnishing of certificates for the admissibility of electronic records. In practice, great difficulties can arise in gaining this certificate, which is often impossible if the source of information is unavailable or if the data is shared in various jurisdictions. In cases including '*Anvar P.V. v. P.K. Basheer*[16],' the strict definition of 'Section 63' has added to the procedure and controversies regarding the possibility of its implementation in all such cases that involve digital evidence.

Chain of custody is another procedural puzzle in digital forensics that states that a proper trail of evidence from the time it is collected right up to the time it is presented in court is necessary and admissible. Since digital data is a product of technological advancement, small changes in the method of data storage or transmission are likely to bring the admissibility of the evidence into question in a court of law. The famous case *Ram Singh v. Col. Ram Singh* [17]adopted certain written policies regarding the 'chain of evidence' as far as the handling of evidence is concerned. Nevertheless, these principles are not systematically applied in the field of digital forensics because there are many different levels of professionals and equipment in police departments. The procedural irregularities can also be stretched to the episodes involving the seizure of electronic gadgets: failure to properly handle or improperly obtain the images can result in evidence tampering.

Moreover, the existing legal systems of India internally do not fit the bill when it comes to cross-border offenses in the virtual world. The commission of cybercrimes mainly incorporates perpetrators, victims, and evidence originating from more than one nation, raising issues of collection and presentation of evidence within the acknowledged procedural laws of different countries. The MLATs are the legal instruments assuring international cooperation in criminal matters; nevertheless, such treaties in practice cause significant procedural and jurisdictional delays that hamper effective investigations. As a result, there is a need to review or introduce modern statutes to reflect technological changes and also strive to contain procedures governing the acceptance and consideration of digital evidence.

4.3 Ethical Concerns in Digital Forensics

The major ethical issues discussed in connection with digital forensics are policing and privacy issues, whereby privacy rights may be trampled on in the name of effective crime fighting. If an investigator is searching digital evidence, the investigator may stumble onto personal or perhaps pertinent

---

[14] Dattatray Bhagwan Dhainje, "Cyber-crime Investigations Issues and Challenges", *5 International Journal of Law* 129 (2019).
[15] *Supra* note 14.
[16] [2014] 10 SCC 473.
[17] [1985] 1 SCC 61.

information that has nothing to do with the investigated crime; in so doing, the investigator violates the privacy provisions as provided by "Article 21" of the Indian Constitution. The Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*[18] holds the right to privacy as a fundamental right of Indian citizens. It should be noted that any intrusion into any person's digital life should be done for lawful reasons, necessity, and proportionate to the context. Further, the amorphous accumulation of digital evidence or overdependence on mass surveillance technologies, including spyware or generally intrusive data mining methods, compromises the legitimacy of personal information and docket trust in the security forces.

Furthermore, the ideas of police analysis of digital evidence raise ethical concerns since police authorities may misuse these tools during an investigation, especially where the whole process is not very transparent. One can recall cases where technology, particularly digital forensics, was used to distort the facts and frame a person, or to control protests and opposition. The lack of set ethics for forensic practitioners in India also increases the problem of misconduct because the practitioners are unlikely to follow standard rules on how to collect, analyze, and report findings. Hence, letting ethical issues come out in digital forensics needs a strong legal system underpinning without eradicating privacy, obtaining strong standard procedures in handling evidence, and finding ways of preventing misuse.

5. Role of Digital Forensics in High-Profile Criminal Cases

The importance of digital forensics in organizing high-profile crimes in India cannot be underemphasized; it is the dominant tool in determining negligence or otherwise in many criminal scenarios. As technology has seeped into every segment of citizens' daily existence, tangible proof retrieved from people's handheld gadgets has assumed considerable importance in the investigation of multi-layered crimes, including financial fraud, terrorism, cyber threats of harassment or murder, etc. Information that is stored in electronic devices can be pulled out, and facts from them can be retrieved and processed as primary evidence that conventional evidence may not offer law enforcement and the judiciary. In high-stakes cases, digital forensics of the crime scene can contribute to the investigations, supporting alibis, affirming the witness' accounts, or disproving a suspect's fabricated stories based on the scene. In the last two decades of crime and criminal investigation in India, one can witness several sensational cases, which were originally judged with the help of digital evidence, indicating the significance of digital forensics in crime investigation in the country.[19]

5.1 Analysis of Landmark Cases Involving Digital Forensics in India

To the best of my knowledge, one of the most profound examples of applying/using digital forensics in India is in the case of *Arushi Talwar and Hemraj Double Murder Case*[20], where the call details record and Internet browsing history were crucial for the investigation. In this case, the death of a teenage girl named Arushi Talwar and the family's domestic help, Hemraj, was carried out. Mobile phone records and internet activity were used to determine timelines and the reliability of such statements. However, the case also revealed the weakness of digital forensics because differences in the analysis and understanding of the electronic evidence caused such differences in conclusions, which, in the end, contributed to the acquittal in the Allahabad High Court in 2017. This case shows that while digital evidence can be gathered, it also has to follow not only best practices in forensics but also rules of these standards that will allow for the evidence to be presented in court properly.

Another ground-breaking case is the "Mumbai Terror Attacks Case" where the investigative reports and digital investigation were a major factor in the conviction of Ajmal Kasab, the only terrorist who survived the 2008 Mumbai attack. Even call detail records, e-mail, and movement details that led the attackers and connected them to handlers in Pakistan were recovered by the digital forensic team. The investigation of the communication equipment, such as the handphones and satellite phones, enabled some of the understanding of the planning of the attack that enabled a conviction of Kasab under terror charges, murder, and conspiracy. This case demonstrates that the analysis of digital evidence is used not only to indicate the direct involvement of a suspect in criminal activity but also to reveal organizational networks and other assistants, which makes digital forensics essential in the fight against terrorism.

As in the case of *Nirbhaya Gang Rape Case*[21]: "Confirming the evidence adduced at the trial through digital forensics was crucial in this matter. The case refers to the brutal gang rape and subsequent murder of a young woman in New Delhi; the situation attracted considerable national and international attention. Mobile phone records, CCTV, and those calls made by the accused proved his presence at the scene of the crime by forensic experts. A combination of digital and physical evidence accompanied by reports—medical together with statements made by the eyewitnesses—led to the conviction of the accused, and the penalty of death was imposed on four of the individuals. This case also illustrated the applicability of digital forensics in heinous crimes but also showed how the sophistication of forensic technology extends to help in the fluidity of the hard-to-solve criminal investigation.

5.2 Impact of Digital Forensic Evidence on Case Outcomes

The impact of digital forensic evidence in Indian cases by the increased use in both the lower courts and higher judicial appeals. In both the 'Mumbai Terror Attacks Case' and the 'Nirbhaya Gang Rape Case' the use of admission of digital evidence was central to the conviction and accordingly the justice meted out. The courts have begun to slowly appreciate cyber evidence admitting it as true, though this is on the condition that it is trustworthy and

[18] [2017] 10 SCC 1.

[19] Aybeyan Selim & Ilker Ali, "The Role of Digital Forensic Analysis in Modern Investigations", 4 *Journal of Emerging Computer Technologies* 1 (2024).

[20] [2013] 14 SCC 456.

[21] *Mukesh and Anr v. State for NCT of Delhi*, (2017) 6 SCC 1.

genuine in compliance with provision Section 63 of the Bharatiya Sakshya Adhiniyam'. More importantly, in these and other landmark cases, it not only assisted in reconstructing the chronology of events but also supported the general prosecution case by offering an impartial, scientifically evidenced chronology of events that was independently verified and, where possible, given expert opinions.

But the role of digital forensics does not end here; that is, to secure conviction. It also acts as a method for opposing evidence and cross-examination of the accused and is also used in the *"Arushi Talwar Case."*[22] If the digital evidence analysed and managed is inaccurate or wrong, then it would promote wrongful implications for suspicion or an acquitted accused. As such, even though the use of digital forensic evidence is today seen as an imperative part of criminal investigation across India, this has provided the much-needed shift towards digital investigations, but the effectiveness in terms of providing successful cases depends heavily on the quality of the forensic processes, the judicial perception and proceedings, and sticking to the legal guidelines provided as well. As the law about digital forensics remains in its state of development, it is evident that its future direction remains with criminal justice systems across continents where improvements in technology and the law are needed on an ongoing basis.

6. Suggestion

To tackle the different challenges pointed out regarding the field of digital forensics and criminal investigation in India, specific actions can be proposed from the legal standpoint, from the infrastructural standpoint, or from the standpoint of good practices and ethical dilemmas. The intent is to develop an integrated 'blueprint' for enhancing the use of digital forensics within the criminal justice process and meet the requirements of the protection of individuals' rights and policing requirements.

- India should adopt uniform procedures for the collection, preservation, and analysis of digital evidence known as the ACPO Good Practice Guide for Digital Evidence used in the United Kingdom. The common guidelines will effectively address the major challenges of the variations in the forensic processes and increase the dependability of virtual proof among various states.
- Proposed and adoption of a national accreditation and certification program for the labs and the professionals in digital forensics would enhance the quality of forensic practice. Accredited labs would work according to protocols; certified forensic experts would be more capable of solving complicated digital evidence, thus making forensic testimony more trustworthy in court.
- The existing law needs reform to try and achieve more leeway in terms of other formalities, such as the "Section 63" certificate. The ability of the court to admit digital evidence does not require compliance with these formalities; in exceptional circumstances, it is necessary to allow the exclusion of necessary evidence for technical reasons.
- The creation of cybercrime courts or the formation of benches of a forensic nature within the framework of the common court system can be effective in satisfying the needs of cases connected with cybercrime. These courts would deal with cases that may be complicated to try by ordinary trial courts since they need more technicality in terms of acceptance of electronic evidence such as digital forensic evidence.
- There is a need to improve the teaching and implementation of digital forensics in the police and judicial systems. With this in mind, and as part of their training, personnel ought to attend workshops and courses to sharpen their knowledge of what is expected of them when dealing with tools and standards in forensics, current trends in technologies, etc.
- Cybercrime is a provincial offense requiring enhanced international legal systems as a solution. India should sign better Mutual Legal Assistance Treaties (MLATs) and put in place fast-track regimes of international collaboration where the evidence, including communication records, might be hosted on servers in other countries.
- Proposing specific legislation that deals with anti-forensic tools and techniques that point towards hindering investigations can go a long way in helping enforcing agencies. Legal measures should be taken to discourage the use of countermeasures that hinder investigations and act with the aim of adversely fascinating them.
- True independence of digital forensic practitioners would encourage employees to be truthful about their incidents and situations that require forensic analysis. It can guarantee ethical standards adherence and forensic purity and would effectively deter some unpleasant people from exploiting forensic services for nefarious purposes.
- Resolution of the above-discussed ethical dilemmas can be best achieved by strong data protection laws that hinder access to personal data while also guaranteeing that the actions taken in DRF are inequality to the crime committed. Privacy measures should be incorporated into forensic practice to reduce pre-emptive invasions into people's technological existence.
- More investment in forensic input equipment as well as databases that offer secure storage of data is recommended. Such funding would enable the enhancement of digital capabilities of the police for the efficient and expeditious investigation of cyber and other more traditional crimes where the perpetrator used electronic devices as their crime instrument or technique.
- A tripartite partnership between enforcing agencies and academic bodies with the aim of research and development in digital forensics helps in providing Indigenous solutions that fit well within the Indian legal and technical structure.

[22] *Dr. Nupur Talwar & Anr v. Central Bureau of Investigation*, (2018) 4 SCC 530.

By implementing these suggestions, India can address existing challenges in digital forensics, improve the quality and admissibility of digital evidence, and enhance the overall effectiveness of criminal investigations involving electronic data.

7. Conclusion

Digital forensics has now become a crucial element in criminal investigation throughout India, mainly because there is an increase in technology crimes and the exercise of electronic tools. Its proponents point to digital forensics as a force multiplier that assists law enforcement agencies to investigate crimes and prosecute offenders. This shows that its legal and procedural use presents several challenges. Soon with the passing of the IT Act, of 2000, provisions under the Bharatiya Sakshya Adhiniyam, 2023 and Bharatiya Nyaya Sanhita, 2023 have framed the way to combat cyber-crimes and digital evidence. However, it is unfortunate that the current legal approaches are still characterized by challenges that influence the ability of digital forensics to deliver justice. This focuses on the admissibility and reliability of digital evidence in courts, which are challenged by issues like strict compliance with procedural requirements under Section 63, inconsistent manner of handling the evidence, and absence of forensic standardization.

Encryption hinders investigation, data are dynamic and may be altered at any given time, and criminals also use tools that conceal evidence known as 'anti-forensic' measures. There are also other technical challenges in digital investigations. While legal factors include jurisdiction hitches and principles dealing with custody of digital evidence, such rights raise ethical questions for privacy rights while putting into consideration the need for the police and other responsible authorities to fight crimes effectively. It is true that such cases as the 'Nirbhaya Gang Rape Case' and the '*Mumbai Terror Attacks Case'* [23]reveal how advanced technology, inclusive of digital forensics, can revolutionize important criminal matters; however, it is equally apparent that the increasing use of advanced technologies calls for more effective, rigorous procedures to safeguard the soundness of the proof.

Compared with international practices, it was found that India can gain from having standard protocols similar to those of the ACPO Good Practice Guide for Digital Evidence of the U.K., accreditation of the forensic labs, and certification of the professionals. Also, the training of judges in digital evidence and cross-border cooperation in connection with extraterritorial cybercrime are other fields where India can learn a lot from the advancements of the United States of America and the United Kingdom.

In conclusion, it could be asserted that while digital forensics proved to be a critical tool for modern Indian investigators, the ongoing legal and procedural evolution must substantially enhance the field. Standardizing the forensic processes, raising judicial consciousness, and implementing best practices anywhere in the world will be the principal steps while invigorating the digital forensics' role in the Indian Criminal Justice System and making that justice technologically sophisticated and operationally just will be the pathway.

[23] Md.Ajmal Md.Amir Kasab @Abu Majahid v. State Of Maharashtra, AIR 2012 SC 3565.