# DIGITAL FORENSICS IN CRIMINAL JUSTICE: TECHNOLOGICAL EVOLUTION AND LEGAL FRAMEWORK IN THE INDIAN CONTEXT

Mr. Siddhant Naresh Pathak, BBA LLB (Hons.), School of Law, Christ University, Lavasa Campus, Pune

## ABSTRACT

Cybercrime cases in India have been Increasing day by day and year after year in India, making digital forensic as an essential part of modern criminal justice system. Over 60% of the households are now connected to the internet. As the use of computers, smartphones, and the internet, crimes are also taking place more often in the digital space, which is why we need digital forensics for solving such cases. There is a rapid increase in the cases from 10.29 lakhs in 2022 to 22.68 lakhs in 2024.The paper explores the evolution of digital forensics in India, from basic data recovery and computer analysis to advanced methods involving mobile devices, cloud storage, and artificial intelligence. The paper deals with the legal framework that regulates the process of digital forensic in India. Focuses on the Information Technology Act 2000 and the Bharatiya Sakshya Adhiniyam, 2023 (particularly section 63[1]), regulating the provisions and admissibility of electronic evidence in court. Judicial interpretation of these provisions has played a crucial role in shaping the admissibility of electronic records as seen in the landmark judgment of Anvar P.V. v. Basheer. Also, the right to privacy established in K.S. Puttaswamy v. Union of India and the Enactment of Digital Personal Protection Act, 2023. Furthermore the paper deals with challenges related to the cross-border mechanism like technical, legal and procedural challenges such as conflicts of jurisdiction, data being stored on overseas servers, and prolonged delays in obtaining evidence through Mutual Legal Assistance Treaties (MLATs) remains the persistent barrier. Since India is not a part of the Budapest Convention on Cybercrime underscoring the need for stronger global partnership. The paper further explores the significance of open-source software kali Linux which is widely used by forensic experts and cybersecurity for the purpose such as penetration testing, data recovery, and network analysis; however, it serves as a double-edged sword as it is also frequently misused by cybercriminals for unauthorized access, data theft, or covering digital traces.

[1] Bharatiya Sakshya Adhiniyam, 2023, § 63 (India)

## Introduction

Digital forensics in India has emerged as a necessary factor in the contemporary criminal justice system and as a crime continue it leaves digital footprint on computers, phones and networks. Cybercrime in India has increasing day by day as a result of rapid digitalization in India. About 86% of households are now connected to the Internet reflecting the remarkable progress under the Digital India initiative. According to the National Crime Bureau Investigation the incidence of cyber fraud and digital offices have surged dramatically approximately from 10.29 lakhs cases in 2022 to 22.68 lakhs cases in 2024[2]. As everyone now uses mobile phones, social media, online shopping and digital payments. Also, a large proportion of communication, financial transactions, entertainment, and government services now take place online and cybercrime cases are increasing which is why we need the police have to keep updating their methods. There is need of digital forensics officers to collect and verify data from many different devices and online platforms. Digital forensic thereby functions as a bridge between technology and law involving the scientific collection of evidence, preservation, examination and presentation of electronic evidence in criminal proceedings.This study examines how new developments from data recovery to new digital tools like devices and software interact with India's evidence law. It outlines the statutory and judicial framework of digital evidence and the growth of forensic tools and institutions. Also, the different types and techniques of digital forensics Reviewing case studies and highlighting the ongoing challenges. It discusses the important court rulings like Anwar P.V V. P.K Bashir and Arjun Panditrao Kotkar v. state of Maharashtra on Admissibility of electronic evidence. Related laws governing the Admissibility of evidence such as the Information Technology Act, Indian Evidence Act which is replaced by the Bharatiya Sakshya Adhiniyam, 2023.Furthermore, it highlights the cross-border challenges in evidence collection which arise from data being stored on global cloud servers, foreign based platforms and jurisdiction with different privacy and cooperation norms. Furthermore, the increase of use of advanced forensic and cyber security tools like Kali Linux which is widely used by forensic officers for digital evidence acquisition, analysis and penetration testing but it also can be used by the ethical hackers to tampered with the evidence so it can be served as a double edged-sword.[3] Therefore, strengthing India digital forensic framework requires investment, advanced technology,

[2] Press Information Bureau, *Curbing Cyber Frauds in Digital India* (Oct. 8, 2025),
[3] Storyboard18, *India Records Over 22 Lakh Cybersecurity Complaints in 2022; DoT Cracks Down With AI-Powered Measures*, Storyboard18 (Aug. 7, 2025),

Capacity building legal reform and stronger international collaboration.

## Evolution of Digital forensics: Global and Indian Perspective

### Early and modern Evolution:

Globally Digital forensic has become an independent field Emerged in the late 20th century response to the use of computers and use of technology enabling increase in crimes. Earlier the attempts were made at retrieving electronic evidence in 1970. But, only In the 1980s the police and intelligence unit began to allocating dedicate resources to the computer related crimes.The main development were done in 1984 where the US FBI Federal Bureau of investigation established a computer analysis and response team (CART) to tackle cyber inclusions.[4] After that during 1980s and 1990s there was a gradual formalization of methods investigators officers started creating a bit-by-bit disk images for analysis and basic file recovery techniques were done.This period also witnessed the development of specialized forensic Software such as Encase and Access Data Forensic Toolkit which significantly enhanced the investigative capabilities for the forensic officers. After this Computer forensics has gained Recognition as an academic and professional field and various types of training programs and frameworks. In late 1990s the adoption of mobile phones led to the creation of mobile forensics as networks and the Internet expanded forensics focus on analyzing data traffic and online communications. Later in early 2000s cloud computing and social media came which gave rise to the cloud forensics. In recent years there is a rapid increase in the digital data such as the CCTV videos, network logs, social media which made it impossible for investigators to analyze everything manually so to handle this they are now relying on the artificial intelligence and the machine learning tools. These tools help to find patterns which are unusual and hidden evidence in large amount of data. Specially AI is useful for analyzing videos, tracking digital footprints, and detecting tempered files. Big data techniques also help different types of information like matching location data with transaction records to identify crimes and suspects quickly. However, this year Driven Tools raises a serious question about algorithm bias and transparency of analytical process, privacy protection, and overall evidence of AI.

### Evolution in India:

India's digital forensic system developed slowly and slowly comparing to other countries

[4] *Piecing Together Digital Evidence*, Fed. Bureau of Investigation (Jan. 8, 2013),

mainly because the awareness of cybercrime was low in early years.According to studies know that Indias first cybercrime conviction came only in 2013 Stating that traditional investigations initially overlooked digital evidence. The Information Technology Act 2000 provided the first framework defining the computer related offenses but they need time to adjust these methods. During 2000 many computers forensic labs and state forensic laboratories begin setting up the cyber forensic divisions across the country. Major Center Forensics Science Laboratories are in Hyderabad, Kolkata and Chandigarh. They have their own cyber units and most states have their own cyber labs. For example, Odisha SFSL (State Forensic Science Laboratory) expressly list cyber forensic analyzing of hard disks, cellphones and memory devices and similarly in Rajasthan Jaipur Forensic Science Laboratory has a cyber forensic division handling the cases of digital fraud and social media crime. In 2004 the Government of India established the Indian Computer Emergency Response Team (Cert-In) became National Agency for handling cyber incidents. In 2018 the government launched Indian Cyber Crime Coordination centre (I4C) Initiative includes National Cyber Crime Forensic Laboratory and training Center for police officers. Also, special cybercrime police stations also become common in cities such as Bengaluru, Hyderabad, Mumbai and Delhi. Nowadays investigators use many types of forensic tools used globally. They widely used commercial software like Encase and FTK and mobile forensic tools which can unlock phones and retrieve data from apps such as WhatsApp and Telegram. police departments including Delhi and Hyderabad have confirmed possession of Cellebrite UFED system which can bypass locks.This type of tools has been used at the same times they also confirm that an open - source platform Kali Linux which includes hundreds of tools. India gradually depends upon the foreign tools but also developing its own technologies. India also building international partnerships through MLATs and Interpol to manage cross border cybercrimes.

**Types and Techniques of Digital forensics in India**

Digital forensics includes various branches each focusing on a different type of digital evidence There are some major areas.

1. **Computer Forensics**

   Computer forensic is the oldest and most common branch it deals with the analyzing computers, laptops, servers, storage devices, hard drives, recovering deleted files, system logs and many more. Forensic officers create the exact copies of the data which is called as

forensic images so they can examine files without changing the original evidence. For example, in India in case of Indian cyber bullying case an officer team created a copy of computer and recovered the deleted fake profiles. Similarly in hacking investigators used disk imaging tools to retrieve the important emails from the hacker's system. Email forensic analysis is very common forensic technique will search mail archives and backing up files to reconstruct communication even if user has tried to erase evidence. In The Indian Evidence Act which is now replaced by the Bharatiya Sakshya Adhiniyam, an officer must maintain a strict chain of the custody to ensure the digital evidence is not tempered. Common tools used in computer forensic include Encase, FTK, volatility for memory analysis and autopsy. Many CFSL reports in India now include the recovered chats, transactions and screenshots of computers as a part of criminal prosecution.

**2. Mobile Forensics**

With a rapid increase in the use of smartphones mobile forensics has become more important phone stores a large amount of personal information like messages, photos, contacts details, location, etc. Which can be used as evidence in case of fraud, extortion or terrorism or other crimes. Indian Investigators used advanced tools like Cellebrite UFED, Magnet Axiom and other tools to unlock phones and extract data These tools can recover deleted text, records, data from apps such as Whatsapp, facebook, Telegram etc. In 2021, Telangana Police noted that Ufed Ultimate can extract WhatsApp data even from a new device on which WhatsApp is logged in. They also Use inbuilt information such as call records an SMS history from the SIM card. Indian courts have accepted the phone-based GPS evidence in case of murder or trafficking as long as it is certified. Standard forensic practices to make the exact copy of the phone and examine that copy instead of the original. But nowadays app data is protected. Like WhatsApp, strengthen its security encryption. Also, smartphone security is improving day by day such as IOS protections they have their own security system stronger than android. So, they often require physical phone and its unique encryption key.

**3. Network Forensics**

Network Forensics involves collecting data and analyzing data across all the computer Networks. This includes capturing network packets, checking router and firewall logs and reconstructing the online activity. In India this is mainly used for the cases of cybercrime,

hacking and online fraud. Investigator officers Octane logs from an Internet service provider for use tools like Wireshark to capture live network traffic. By analyzing this they can trace the IP address identify which protocols were used and sometimes recover an unencrypted username or passwords. Logs from web searches, firewalls and proxy servers can also show signs of attempt to break-in or data theft. CERT-In And several police forensic labs run 24/7 monitoring centers for collecting traffic network data for analysis. However, challenges in encryption like HTPPS and VPN which means deep packet inspection is often impossible without cooperation from providers. But still network patterns can give some clues.

2021, Telangana Police noted that Ufed Ultimate can extract WhatsApp data even from a new device on which WhatsApp is logged in.Many People store their data on cloud platforms like Google Drive so investigators also have to collect evidence from the cloud. Cloud forensic means getting logs and data from cloud service providers, checking backups, Information that is stored across many servers. The biggest problem is jurisdiction and the chain of custody because the cloud data can be stored in different countries making it hard to gain the original data. In forensic investigators depends on the cloud company's corporation and by the MLATs process which is government to government approach. This often causes delays. In India there are no special cloud forensic laws but they use Section 69B of Information Technology Act [5]and international legal assistance to access such data. Indian courts accept the cloud records if they are properly collected. But proving the authenticity of the cloud snapshot is still a challenge. Experts observed that the traditional forensic models do not easily apply to the cloud forensics requires new and advanced technology.

## 4. Malware & Ransomware Forensics

Modern cyber-crime needs malware software or ransomware. In this type of forensics experts study the malicious software to understand how does it work. This is often done on 'sandbox' Which is an infected system. They check memory dumps, How the code looks and how it spreads or encrypts files. Sometimes by checking these Code They can find weakness that can help to recover the data without paying ransom. They also search for indicators of compromise across an organization system Like suspicious file hashes,

[5] Information Technology Act, 2000, § 69B (India).

registry changes, or communication with command and control (C2) Servers. In India the Computer Emergency Response Team (CERT-In) issues warnings about major Malware and provides decryption tools. Reverse engineering needs advanced skills and experts use tools like IDA Pro To study how program works. They also capture network traffic to see how the malware communicates. They use memory forensic tools like Volatility to recover hidden data such as decryption keys. The report that links the malware to the crime. Because this work is very technical in nature many big organizations in India take help from the cybersecurity companies to analyze malware evidence.

### 5. AI based Forensics

AI is now becoming a part of digital forensics. Police and analysts use machine learning to spot crime patterns, identify hotspots or suspect profiles based on past data. In forensic lab AI tools can automatically recognize faces or objects in CCTV videos much faster than the human. Machine learning is also used the filtering quantities of digital evidence like spam detection in seized emails or detect unusual activity on a network. In India some police investigative agencies are testing AI system to analyze large set of call details records to identify fraud groups. However, these techniques raise ethical concerns regarding the bias. Also raises privacy concerns too as AI tool can accidentally reveal personal information if not handled securely. Court make question AI based findings if the process is not transparent or scientifically valid.

## The Role of Kali Linux in Digital Forensics

Kali Linux is free and open-source operating system developed by offensive security. It is a Debian based and comes with pre-loaded 600 hundreds of tools for penetration testing, vulnerability analysis and digital forensics.[6] Some of the common tools are autopsy which is used for disk image, Wireshark used for network packet analysis, Nmap used for network scanning, John the Reaper used for passwords cracking and aircrack-ng used for Wi Fi security testing and many others. One of the major features of Kali is its “forensics mode” When you boot Kali from USB in forensic mode, it does not automatically open any internal hard drives.[7] This keeps the evidence because nothing is changed from the suspects device. This makes Kali

[6] “What Is Kali Linux, ” *Kali Linux Documentation* (updated June 18, 2025),
[7] “Why Hackers Use Kali Linux,” *GeeksforGeeks* (last updated July 23, 2025),

a useful portable forensic tool for investigators.

**Why Kali Linux is useful:**

For forensic investigators Kali Linux serves as a good option Because it is free, avoids cost fees on other forensic tools. Investigators can install Kali on laptop through USB drives ed crime scenes. It contains Various tools in one place so officers can recover deleted files, analyze disk image, or capture network traffic without switching the devices. It also receives regular updates helping the experts to stay current with new file system and security threats. These capabilities help Indian labs to recover evidence like financial records, pornography, or defamation content from the suspect device.

**Concerns and Challenges:**

The availability of Kali Linux is free so anyone can install it because of that these powerful tools can be misused by Hackers or the criminals engaging in illegal activities[8]. Current Indian frameworks do not separately regulate open-source forensic platforms, focusing instead on offenses under the Information technology Act and associated penal provisions (unauthorized access, damage, malware). Certain guidelines from Meity and CERT-IN refers generally to forensic tools and requiring integrity preservation and proper chain of custody but, do not address the competence standards, certification or minimum training for investigators using powerful tools like Kali. Because India lacks training cyber forensics experts and many users rely on self-taught skills, the country needs a proper certification system, a verified forensic tools and dedicated training academics to make sure that open-source tools improve investigation instead of weakening their quality. In India some companies have established formal certification or SOPs for using kali Linux to protect their security.

**Legal Framework Governing Admissibility of Electronic Evidence in Courts**

Cybercrime in India is increasing day by day as using of electronic devices increasing because of this electronic evidence became important in modern investigation. Whether it is cyber fraud, extortion, ramsomware software or encrypted communications etc. As these crimes increasing day by day then the forensic experts became an important role to ensure that the

[8] Vijay Kumar Gupta, *Understanding the Legal Implications of Using Kali Linux Tools*, Medium (Oct. 21, 2024),

digital evidence is admissible in court.[9] India's frameworks governing the electronic evidence is based on Information technology Act, 2000 which defines the computer related offences and Indian evidence act which is replaced by the Bharstiya Sakshya Adhiniyam, 2023 which lays down certain provisions for the evidence to be admissible in court. These acts states hoe law enforcement collect evidence and preserve them and present them before the court.

Under Information Technology Act, 2000 which governs laws related to the computer offences. some sections are related to the admissibility of evidence. Section 43 [10]provides the civil liability for unauthorized access or misuses someone else computer, network, data, or other things without permission. Section 66[11] says if any dishonestly or fraudulently does any act that is mentioned under section 43 of the act then that person can be punished upto 3 yrs of imprisonment and fine upto 5 lakhs or both. The other main section is 69[12] and 69B during prosecution. Section 69 gives power to central or state government or an authorized officer to intercept, monitor, decrypt any information on a computer when they think it is essential for the interest of public or national security. Section 69B gives government power to watch and collect the data from computers and networks to protect cybersecurity and prevent cyber-attacks or threats and stop things like hacking or spreading harmful software. The is Fine upto 3yrs and fine or both. While the existence of such powers raises debates on privacy, it is vital to substantial investigations involving anonymized networks, encrypted messaging, and cross-border data flows. The 2008 amendment inserted section 79A[13] which allows government to appoint the expert officer or agencies who is expert in electronic evidence and help courts to interpret and handle the evidence properly.

However, the IT Act 2000 doesn't not provide the rules for the admissibility of evidence. So some sections are mention in the Indian evidence Act which is replaced by the Bharatiya Sakshya Adhiniyam, 2023 brings clarity about the rules regarding the admissibility of evidence.Under Bharatiya Sakshya Adhiniyam, 2023 Section 2(1)(d)[14] defines the the Document means anything that records information in any form like paper documents, maps, logs, electronic evidence emails, chats, photos, files, Vedios, cloud files, and more on computer

[9] Pratyusha Das & Pradeepta Sarkar, *The Importance of Digital Forensics in the Admissibility of Digital Evidence*, 7 NUJS J. Reg. Stud. II
[10] Information Technology Act, 2000, § 43 (India)
[11] Information Technology Act, 2000, § 66 (India)
[12] Information Technology Act, 2000, § 69 (India)
[13] Information Technology Act, 2000, § 79A(India)
[14] Bharatiya Sakshya Adhiniyam, 2023, § 2(1)(d) (India)

or phones which can be used as an evidence in court.Before document is only included the printed documents or physical papers. So, they added this section and court started to take digital evidence.Further Section 2(1)(e) defines evidence means any statement made by the witness or any document including electronic records that is presented in the court as evidence.

Section 61[15] of BSA states that electronic or digital records cannot be excluded as evidence just because they are in digital form.They have same value as written document or other documents. Section 62 says that the electronic evidence can be used in court if rules mentioned under section 63[16] has been fulfilled.Section 63 states that electronic records can be treated as same as documents.It should fulfill certain conditions,

1. The information must have been produced when the computer or device was being regularly used for normal work by the person who legally controls that computer.

2. During that time, similar types of information were regularly entered into the computer as part of routine activities not something unusual or specially done just once.

3. The computer or device must have been working properly during that period.If it was not working properly at some point, that malfunction should not have affected the accuracy of the electronic record.

4. The electronic record must be a true copy of the information that was actually entered into the computer in the normal course of work. It must not be changed, altered, or created later.

Also, if several or multiple devices were used to create or store information then the all devices will be treated as one. Also to use electronic evidence in court you must attach a certificate describing how it was recorded, from where it was taken and fulfilling the above 4 conditions of section 63. This certificate must be sign by the person in charge of it or by an Expert. In case of digital evidence, it must not only be admissible but also supported by the chain of custody. Unlike other documents the digital evidence can be easily tampered, change it, corrupt it, alter it, etc. So while collecting the evidence hash value must be taken means the digital footprint should be taken by the investigators, maintaining clear access logs, sealing the evidence and

[15] Bharatiya Sakshya Adhiniyam, 2023, § 61) (India)
[16] Bharatiya Sakshya Adhiniyam, 2023, § 63 (India)

allow only the trained officers to handle the data and record every transfer of evidence.This proves that the evidence shown in court is as same as it was collected and not tampered.Also court thinks that the chain of custody has not been serious the evidence will be seen as tampered and they will reject it.Along with the chain of custody the another thing is transparency and Fairness.

Despite these India face some challenges like 63 of BSA 2023, mandates strict rules and must require certificate so in some cases investigatos struggle to get the certificate from the service providers or private companies specially when the data is stored on foreign platform which is beyond the India's jurisdiction.Additionally, the lack of trained officers specially in cyber forensic, also the inconsistent chain of custody.Courts have repeatedly stated that even the minor procedural lapses can render the digital evidence unreliable[17].Also in case of cross border as India is not part of Budapest convention on cybercrime. India is depended on the Mutual Legal Assistance Treaty (MLAT) process which is a government-to-government process.[18] This takes a lot of time and this delay Is particularly damaging in cases involving time sensitive evidence such as social media messages, volatile server logs Which can be deleted before getting the evidence from the foreign authorities. Although India participates in the G7 24/7 High Tech Crime network, The absence of treaty-backed obligations limits the speed and reliability of global evidence exchange.[19]

The two landmarks supreme Court judgments have shaped the admissibility of evidence in court. In Anvar. P.V V. P.K Basheer [20](2014) It was a nine-judge bench. Court held that the electronic evidence which involves a recording or a print out of some other electronic data is admissible in court only if it fulfills the condition under the Section 65 of Indian Evidence Act which is now replaced by the Bharatiya Sakshya Adhiniyam, 2023 and the current section is 63 of BSA. The court noted that the tendency of electronic records can be easily tempered so this certification is essential. In, CDS containing election campaign songs and speeches were presented without a certificate so, the court struck them out. However, the court also clarified that the primary electronic evidence such as the device seized by the police or evidence directly by the witness can be admitted without the certification. This case was later restated and refined

[17] Changing Scope of Certificate as per BSA 2023 for Admissibility of Electronic Evidence, Corpotech Legal (Nov. 2024)
[18] Mutual Legal Assistance in Criminal Matters, Ministry of External Affairs (India), *Government of India* (last updated Mar. 3, 2023)
[19] *The G7 24/7 Cybercrime Network Protocol* (G7 24/7 Network), May 2021
[20] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473

in the Arjun Pandit Rao Kotkar V. state of Maharashtra [21](2020) It was a three-judge bench. Court held that that Anwar P.V. V. P.k Basheer in this case the law is correct and they overruled the case of Shafhi Mohammad (2018)[22] case which had wrongly allowed digital evidence without the section 65B which mandates certificate in the secondary form according to the Indian Evidence Act. However, no certificate is needed if the party brings the original device like a laptop or phone or a primary device.

**Challenges related to the Cross-border Issues**

One of the most acute challenges in the Indian digital forensic setup is the cross-border issues, particularly in cases where the evidence is in the form of electronic evidence and the evidence if stored, processed or transmitted in the servers which are located outside India. As an increasing share of cybercrime is carried out across national frontiers, there are difficulties for Indian law enforcement to obtain timely access to data stored by global service providers such as Google, Meta or Apple, who are bound by the data protection laws of their respective jurisdictions.[23] Even when the cybercrimes target Indian citizens, for example, by financial frauds on online platforms, ransomware attacks and transmission of illegal content, key evidence such as user logs, mails and cloud blockchain storage database files may be stored in foreign servers covered under strong international privacy laws such as the European Union's General Data Protection Regulations Act. But currently, India relies on a system of mutual legal assistance treaty (MLAT), which is used to formally ask for access to such data, but this has been slow down and is a bureaucratic and inconsistent process taking a lot of time about months to see results because of that time data can be deleted or altered. Such delay can badly affect investigations particularly those involving an urgent need to preserve data. The situation is complicated by the use of strong encryption and techniques like anonymization by cybercriminals, as well as the use of anti-forensics. Applications that use end-to-end encryption, such as WhatsApp or Facebook, make it nearly impossible for forensic analysts to recover the content even with the benefit of lawful access. Additionally, criminals often utilize VPN (Virtual private network), browsers in the dark web and remote data wiping tools to cover their tracks, rendering digital evidence collection across jurisdictions very unreliable[24]. India's

[21] Arjun Pandit Rao Kotkar V. state of Maharashtra AIR 2020 SC 4908
[22] Shafhi Mohammad v. State of Himachal Pradesh AIR AIR 2018 SC 4321
[23] "Cyber Crime: Data Deprivation and Data Localisation, " *Drishti IAS* (Aug. 23, 2019),
[24] Gargi Sarkar & Sandeep K. Shukla, *Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies*, J. Economic Criminology (2023)

legal system and specifically the law related to the authentication and certification of the electronic evidence under Sections 63 of the Bharatiya Sakshya Adhiniyam, 2023 which require careful adherence to the process of authentication and certification of electronic evidence in order for it to be admissible in court. But, When the source of evidence is a foreign server or a non-cooperative provider then it is difficult to ensure the compliance of these provisions, with the risk of inadmissibility for trial. Although Section 75 of Information Technology Act, 2000 provides for extraterritorial jurisdiction, to implement it in practice it is difficult as the holder of data is operating under a different national framework. The issue becomes even more complex because India refuses to join the the Budapest Convention on Cyber Crime which is the primary international treaty designed to facilitate faster cross-boundary cooperation with respect to digital evidence. But India is concerned about the national security, national sovereignty, and possible violations of constitutional protections such as the right to privacy as protected in a landmark case (K.S. Puttaswamy v. Union of India)[25] judgment. Specifically, provisions such as Article 32(b) of the Convention that enable some forms of data access without prior consent from the host country have raised the red flags. So instead, India has chosen to go for bilateral arrangements and participation in regional associations such as the Shanghai Cooperation Organization (SCO) which, while providing scope for international agreements, often lack the efficiency, legal standardization and global reach provided by multilateral treaties. Furthermore, non-uniform procedures for digital evidence sharing, absence of quick preservation mechanisms and interoperability of legal systems prevent timely investigation and prosecution. In the backdrop of the ever-changing legal environment in India, including the passage of Digital Personal Data Protection Act, 2023[26] and the Bharatiya Sakshya Adhiniyam, 2023, cross-border sharing of data must also consider the balance between the right to privacy and the need for investigation. In essence, India's digital forensic efforts are severely limited by inadequate availability of international data environments given their fragmented and inaccessible nature, the issues in existing legal cooperation frameworks, and increasing sophistication of cybercriminal tactics. These types of the cross-border difficulties are a crucial challenge to delivering justice that is effective and timely in the digital age.

[25] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
[26] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, India (2023)

## Conclusion:

India's rapid growth in the digital domain has altered the way people communicating, working, banking, learning and even committing crimes. With the increase in the activities which are performed online, criminals have also adopted technology in new ways. Because of this, digital forensics emerged as an important for modern policing and justice in India. Digital forensics assists investigators with recovery, preservation, and analysis for electronic evidence from computers and phones, networks and cloud, electronic, and other digital platforms. Without these techniques, it would be almost impossible to solve a large number of cybercrimes today. The paper shows that India's approach towards solving the digital forensics has grown step by step. In the early years, there was not much awareness of cybercrime and very fewer cases were scientifically investigated. Over the years India developed institutions such as CERT-In and Indian Cyber Crime Coordination Centre (I4C), cyber forensic labs and specialized cyber police stations etc.[27] Today, investigators are increasingly relying on sophisticated tools both commercial and open source tools like kali linux to recover deleted data, trace online activity, examine mobile phones, analyze malware and even artificial intelligence to study large amounts of digital information.The legal framework has also grown to support this growth.The Information Technology Act defines computer related offences and gives the authorities some powers to investigate digital misconduct. The Bharatiya Sakshya Adhiniyam, 2023 through section 63 provides the rule regarding the certification of electronic evidence and its presentation in court.Important judgments of Supreme Court particularly Anvar P.V. V. P.K.Basheer and Arjun Panditrao[28] have explained that how electronic evidence must be admissible, reliable, and it has to be certified properly. At the same time, Puttaswamy case set the field of privacy as a fundamental right, meaning investigators need to respect the constitutional boundaries when gathering digital information. Together these laws and judgments ensure that digital evidence is handled in a scientific and ethical manner, however there are still a lot of challenges faced in India. There is a lack of trained forensic experts in India. Many police officers do not have the technical skills to perform the safe collection and preservation of digital evidence. Forensic laboratories are frequently challenged with outdated equipment, small budgets, and long work lists. Chain-of-custody errors and lack of standard operating procedures result in evidence being challenged in court. Things are even more difficult when cross-border issues come into play, given that much of the data related to

[27] "Exploring the Growth of Digital Forensics in India, " *Pelorus Technologies* (last visited Dec. 12, 2025)
[28] Anvar P.V. V. P.K.Basheer and Arjun Panditrao AIR 2020 SC 3847

cybercrime is stored on foreign servers. As with anything, the access of this data requires international cooperation, but this is often a slow and complicated process. So even with these challenges, the future of digital forensics in India is a very important one. Crime will further become more digital and courts will increasingly rely on electronic records. To keep up, India needs to improve forensic laboratories, need more expert hand, standardized procedures, updated laws and cooperation between police and forensic scientist. It must also develop faster international channels to accessing data stored overseas[29]. At the same time, privacy and individual rights should be respected so that technology is used responsibly and responsibly. to conclude, digital Forensics is now an essential part of India's criminal justice system.[30] It is an enhancement in achieving accuracy and strength of the investigation and helps the courts come to the truth in a digital world. But for Digital forensics to reach its full potential, India has to continue to invest in skills, tools, laws and collaboration. So, with the right combination of technology, training, and legal protection, digital forensics can significantly contribute to justice and security in the process of India's digital future.

[29] Deepali & Prof. (Dr.) Radhika Dev Verma, *Role of Digital Forensics and Criminal Investigation in India*, 5 IJRPR 87 (Nov. 2024)

[30] Chandan Kumar Singh & Arunanshu Dubey, *The Role of Digital Forensics and Cyber Crime Provisions in India's New Criminal Laws*, 20 Nanotechnology Perceptions S5, 1078–1092 (2024).