INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 3 | 2025 Art. 10

The Intersection of Digital Forensics and Criminal Investigation in India: Legal and Procedural Dimensions of Evidentiary Standard

Harshit Gupta
LLM Student,
Lingayas Vidyapeeth, Faridabad, Haryana

Prof. (Dr.) Monika Rastogi
HOD Law Department,
Lingayas Vidyapeeth, Faridabad, Haryana

Ruchi Kaushik
Professor Law,
Lingayas Vidyapeeth, Faridabad, Haryana

Recommended Citation
Harshit Gupta, Prof. (Dr.) Monika Rastogi and Ruchi Kaushik, *The Intersection of Digital Forensics and Criminal Investigation in India: Legal and Procedural Dimensions of Evidentiary Standard*, 4 IJHRLR 127-144 (2025).
Available at www.humanrightlawreview.in/archives/.

The Intersection of Digital Forensics and Criminal Investigation in India: Legal and Procedural Dimensions of Evidentiary Standard

Harshit Gupta
LLM Student,
Lingayas Vidyapeeth, Faridabad, Haryana

Prof. (Dr.) Monika Rastogi
HOD Law Department,
Lingayas Vidyapeeth, Faridabad, Haryana

Ruchi Kaushik
Professor Law,
Lingayas Vidyapeeth, Faridabad, Haryana

Manuscript Received	Manuscript Accepted	Manuscript Published
05 May 2025	07 May 2025	09 May. 2025

ABSTRACT

In the digital age, terrorism has transcended physical boundaries and adopted sophisticated technological tools to plan, coordinate, and execute attacks. The tragic killing of 28 tourists in Kashmir in April 2025 underscores the urgent need for advanced investigative techniques to combat such threats. This paper explores the critical role of digital forensics in counter-terrorism efforts in India. It examines how agencies such as the NIA, IB, and CERT-In utilize digital evidence—from encrypted messaging apps and social media footprints to GPS metadata and cloud storage—to track and prosecute terrorist operatives. Through an analysis of real-life case studies, including the 2019 Pulwama attack and the Hyderabad ISIS module, the paper illustrates the effectiveness and challenges of digital forensics in high-stakes investigations. Furthermore, it delves into the legal framework governing digital evidence, highlighting procedural and admissibility issues under Section 65B of the Indian Evidence Act. The study concludes with recommendations to strengthen India's digital forensic capabilities while ensuring due process, data integrity, and constitutional safeguards.

KEYWORDS

Digital, Forensics, Terrorism, Intelligence, Evidence

INTRODUCTION

Recent incidents, such as the tragic killing of 28 tourists in Kashmir in April 2025, highlight the evolving and persistent threat of terrorism in India[1]. These attacks not only demand a swift security response but also underline the growing role of digital footprints — from encrypted chats to mobile communications — in both the planning and investigation of such crimes.

In the digital age, the nature of terrorism has evolved beyond physical borders, entering the intangible realm of cyberspace. Modern terrorist organizations increasingly exploit technology for planning, recruitment, financing, and executing acts of terror, creating new complexities for national security agencies[2]. From encrypted communications and social media propaganda to digital financial transfers and anonymous browsing, the digital ecosystem has become a double-edged sword — offering tools for both innovation and destruction. Against this backdrop, digital forensics the scientific acquisition, preservation, analysis, and presentation of electronic evidence — has emerged as a critical pillar in terrorism investigations[3]. In India, a country grappling with both internal insurgency and cross-border terrorism, the role of digital forensics has become particularly vital. Investigative agencies such as the National Investigation Agency (NIA), Central Bureau of Investigation (CBI), Indian Cyber Crime Coordination Centre (I4C), and CERT-In have increasingly relied on digital forensics to decode complex terror networks[4]. Notable instances such as the 2019 Pulwama attack, the Bodh Gaya blast case, and the ISIS-linked Hyderabad module underline the importance of digital evidence in identifying conspirators and proving criminal intent[5].

However, the rapid advancement of technology has also exposed significant legal and procedural gaps in India's criminal justice system. Questions surrounding the admissibility of electronic evidence, the interpretation of Section 65B of the Indian Evidence Act, and the lack of specialized forensic infrastructure continue to

[1] "28 Tourists Killed in Terror Attack in Kashmir," *The Hindu* (April 2025).
[2] Vinod Kumar, *Terrorism and Technology: Challenges to National Security*, Journal of National Security Studies (2022).
[3] Casey, Eoghan, *Digital Evidence and Computer Crime*, Elsevier Academic Press (2011)
[4] Ministry of Home Affairs, Annual Report 2023-24, Government of India.
[5] "NIA Files Chargesheet in Pulwama Attack Case," NIA Press Release (2020).

pose major challenges.[6]

WHAT IS DIGITAL FORENSICS?

Digital forensics is a specialized field within forensic science that involves the systematic identification, preservation, extraction, examination, and presentation of digital evidence[7]. It enables investigators to retrieve data from computers, smartphones, cloud storage, and other electronic devices that may be relevant in criminal or civil proceedings. In the context of criminal investigations—especially terrorism cases—digital forensics serves as a critical tool in reconstructing the sequence of events, identifying suspects, and establishing connections between individuals, networks, and planned operations. Unlike traditional forms of evidence, digital evidence is inherently fragile and volatile[8]. It can be altered or destroyed with a single keystroke, and its effective handling requires adherence to strict technical and legal standards. As digital communication becomes ubiquitous, digital forensics has emerged as indispensable to modern criminal justice systems around the world.

- ***The Rising Use of Technology in Terrorism***

  The landscape of terrorism has undergone a significant transformation in recent years. The contemporary terrorist no longer relies solely on physical weapons or face-to-face meetings; rather, they leverage digital tools for recruitment, radicalization, communication, coordination, fundraising, and execution[9]. This shift has given rise to cyberterrorism, where attacks are orchestrated via the internet to target critical infrastructure, financial systems, and public safety.

  Encrypted messaging platforms such as Telegram, Signal, and WhatsApp provide anonymity and real-time communication, making it increasingly difficult for intelligence agencies to intercept communications. Terrorist groups also utilize social media for propaganda dissemination, virtual private networks (VPNs) to hide identities, and cryptocurrencies to conduct untraceable financial transactions[10]. The infamous Islamic

[6] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473
[7] Casey, Eoghan, *Digital Evidence and Computer Crime*, Elsevier Academic Press (2011)
[8] National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response* (NIST Special Publication 800-86, 2006)
[9] Weimann, Gabriel, *Terrorism in Cyberspace: The Next Generation*, Columbia University Press (2015)
[10] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020*

State's extensive digital media strategy and use of encrypted chats in attacks like the 2015 Paris bombings and the 2019 Sri Lanka Easter attacks highlight the global nature of this threat.

- ***India's Vulnerabilities: Internal And Cross-Border Threats***

India, given its geographical and political context, is particularly vulnerable to terrorism fueled by both domestic insurgent groups and cross-border extremist organizations. States such as Jammu & Kashmir, Chhattisgarh, and parts of the Northeast face recurring threats from separatist or left-wing extremist groups. Meanwhile, cross-border terrorism emanating from Pakistan-based entities poses a constant challenge to India's national security architecture[11].

The increasing digitization of these threats has compounded the problem. The use of digital communication by groups like Lashkar-e-Taiba (LeT), Jaish-e-Mohammed (JeM), and the Indian Mujahideen has been documented in multiple investigations. In several high-profile cases including the 2008 Mumbai attacks, the Pulwama bombing, and the Burdwan blast, digital footprints played a pivotal role in mapping the conspiracy, identifying co-conspirators, and establishing linkages with foreign handlers.

IMPORTANCE OF COLLECTING, ANALYZING, AND PRESENTING DIGITAL EVIDENCE

In terrorism cases, the probative value of digital evidence is often paramount. It can serve as direct evidence of intent, preparation, or participation in a terrorist act[12]. From retrieving deleted WhatsApp messages, to analyzing GPS data on vehicle movement, to identifying social media connections between accused individuals, digital forensics enables law enforcement to build a robust evidentiary framework.

However, for digital evidence to be admissible in court, it must be collected lawfully, processed without alteration, and certified in compliance with evidentiary standards such as Section 65B of the Indian Evidence Act, 1872. The investigative chain must maintain integrity, authenticity, and accountability—factors that are often contested in courtrooms. A single procedural lapse may render

[11] Institute for Defence Studies and Analyses (IDSA), *Cross-Border Terrorism in India: Challenges and Responses* (2021).
[12] Sharma, Gaurav, "Digital Evidence and its Admissibility in Indian Courts: Challenges and Road Ahead," *Indian Journal of Criminology* (2020).

crucial evidence inadmissible, weakening the prosecution's case.

DIGITAL FORENSICS IN TERRORISM INVESTIGATIONS IN INDIA

The proliferation of digital communication and technological advancement has significantly altered the way terrorism is perpetrated and investigated in India. As terrorists increasingly adopt sophisticated digital methods, law enforcement and intelligence agencies have turned to digital forensics to counter the evolving threat[13]. In India, the investigative approach to terrorism now includes rigorous extraction and analysis of digital evidence, ranging from mobile forensics and encrypted communication to IP tracking and social media surveillance.

TOOLS AND TECHNIQUES IN DIGITAL FORENSICS

Modern terrorism investigations in India rely heavily on the following digital forensic tools and techniques:

1. *Mobile Forensics*: One of the most crucial components in counter-terror investigations, mobile forensics involves extracting data from cell phones, including call records, contact lists, GPS location history, SMS, media files, and app data such as WhatsApp and Telegram. Tools like Cellebrite, Oxygen Forensics, and XRY are commonly used[14].
2. *IP Tracking and Metadata Analysis*: IP tracking helps identify the origin of digital communications and website visits. It is often used to trace emails or social media posts to specific locations or devices. Packet sniffers and network analyzers such as Wireshark are employed to monitor data transmission in real-time.
3. *Social Media Monitoring*: Many extremist groups use social media for propaganda and recruitment. Agencies monitor platforms like Facebook, YouTube, Twitter, and Telegram using both manual surveillance and AI-driven analytics to track suspicious content, hashtags, geotags, and fake accounts[15].
4. *Encrypted Communication Analysis*: Tools like Volatility and FTK (Forensic Toolkit) are used to retrieve or decrypt hidden or deleted files, analyze memory dumps, and reconstruct user activity from encrypted applications and browsers.

[13] National Crime Records Bureau (NCRB), *Annual Report on Cyber Crime and Terrorism*, Ministry of Home Affairs (2023)
[14] Cellebrite, "Digital Intelligence in the Fight Against Terrorism," *Cellebrite Whitepaper* (2022).
[15] Indian Cyber Crime Coordination Centre (I4C), *Manual on Digital Forensics for Law Enforcement* (2022).

5. *Digital Image and Video Forensics*: These techniques help identify doctored content and verify the authenticity of videos and images circulated by terrorist groups. They are crucial in tracking beheading videos, recruitment media, and confessional clips.

REAL-LIFE CASE STUDIES

In the 2019 Pulwama attack, digital forensics enabled investigators to recover call detail records, WhatsApp communications, and GPS metadata from mobile phones at the blast site. These helped trace the network of conspirators and confirmed links to Jaish-e-Mohammed operatives in Pakistan. In the 2016 Hyderabad ISIS module case, the NIA collaborated with cyber forensic units to decrypt Telegram and WhatsApp chats, leading to the arrest of individuals planning terror attacks under ISIS influence. Advanced digital forensics tools were used to recover encrypted instructions from ISIS handlers based abroad[16]. *2025 Kashmir tourist killings;* in the ongoing investigation into the, authorities are reportedly analysing mobile call records, WhatsApp data, and GPS metadata to trace the movements and communications of suspected operatives. This incident further exemplifies how digital forensics is now central to any serious terrorism probe in India.

- ***Agencies Involved In Digital Terror Investigations***

National Investigation Agency (NIA): As the primary counter-terrorism body, NIA spearheads digital investigations in terrorism-related offenses. It has established state-of-the-art cyber forensic labs to analyze digital evidence seized during raids and arrests[17]. *Indian Computer Emergency Response Team (CERT-In):* CERT-In deals with cyber threats and incidents, especially those involving infrastructure or public networks. It supports digital tracing of cyberattacks linked to terrorism[18]. *National Technical Research Organisation (NTRO):* NTRO handles signals intelligence and cryptanalysis, often assisting with encrypted communication decryption, network penetration, and cyber surveillance of foreign terror networks[19]. *Intelligence Bureau (IB):* The IB plays a pre-emptive role in identifying digital threats and flagging suspicious online

[16] Press Information Bureau (PIB), *NIA Breaks ISIS Hyderabad Module Using Digital Forensics*, Press Release (2016).
[17] National Investigation Agency, *Annual Report on NIA's Cyber Forensics Wing*, Ministry of Home Affairs (2021)
[18] Indian Computer Emergency Response Team (CERT-In), *Incident Response Statistics and Cyber Threat Report* (2022).
[19] National Technical Research Organisation (NTRO), *Cyber Security and Signals Intelligence Overview*, Government of India (2020).

activities. It works closely with ISPs and social media platforms for deep surveillance and tracking[20]. *State Cyber Cells:* These specialized units operate at the state police level and handle the seizure, imaging, and basic analysis of digital devices. They coordinate with central agencies for advanced forensics.

CHAIN OF DIGITAL EVIDENCE: FROM SEIZURE TO ANALYSIS

In terrorism cases, the chain of custody and forensic integrity of digital evidence is paramount. The process typically follows these steps:

Seizure: Digital devices such as mobile phones, laptops, and external storage devices are seized from suspects or crime scenes. This must be done in compliance with procedural laws, including warrant requirements. *;Imaging:* Forensic experts create a bit-by-bit clone of the device's memory to ensure that original data remains untouched. This is done using write-blockers and imaging tools like FTK Imager or EnCase.; *Hashing:* A cryptographic hash value (MD5/SHA-1) is generated to prove that the image is identical to the original and has not been tampered with. This hash is used in court to establish authenticity. *;Analysis:*The copied image is analyzed using forensic suites to extract useful information, such as deleted files, browser history, app data, location data, and communication logs. *;Reporting:* A forensic report is generated, documenting the evidence and the methodology used. This report must be certified under Section 65B of the Indian Evidence Act for admissibility in court. *;Presentation in Court:* Forensic experts may be called upon as witnesses to testify on the evidence collected, the tools used, and the conclusions drawn from the analysis.

LEGAL CHALLENGES AND EVIDENCE ADMISSIBILITY IN DIGITAL TERRORISM INVESTIGATIONS

As digital evidence becomes central to the prosecution of terrorism cases in India, it raises a range of legal challenges regarding its collection, preservation, authentication, and admissibility. While technology empowers law enforcement with advanced surveillance and analytical tools, the legal framework must evolve simultaneously to safeguard constitutional rights and ensure fair trials. This section explores the key statutory provisions, judicial interpretations, and practical hurdles in the legal treatment of

[20] Intelligence Bureau, *Threat Assessment Report on Digital Radicalization*, Ministry of Home Affairs (2019).

digital evidence, particularly in cases involving terrorism.

RELEVANT LEGAL FRAMEWORK

a) *THE INFORMATION TECHNOLOGY ACT, 2000:* The IT Act is India's primary statute governing cyber activities, including cyber terrorism and electronic surveillance. Key provisions relevant to terrorism investigations include:

Section 43: Provides civil liability for unauthorized access to computer systems and data theft. Though not specific to terrorism, it is invoked when digital systems are illegally accessed to plan or facilitate attacks. *Section 66F – Cyber Terrorism*: Introduced via the 2008 amendment, this provision criminalizes activities that threaten India's sovereignty, integrity, or security through computer networks. It directly links cyber activities—such as hacking, virus dissemination, and disruption of critical infrastructure—with acts of terrorism[21]. *Section 69 – Interception, Monitoring, and Decryption:* Grants the Central and State governments the power to intercept or monitor digital communication if it is in the interest of national security or public order. This is the legal basis for surveillance of emails, social media, and encrypted chats in terrorism cases.

Challenges: The, interception must follow the 2009 IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, which many agencies allegedly bypass[22].

b) *INDIAN EVIDENCE ACT, 1872 – SECTIONS 65A AND 65B: Section 65A:* Introduced by the IT Act amendment, it states that electronic records must be proved in accordance with Section 65B. Section 65B: This section governs the admissibility of electronic records as evidence. It requires: A certificate under Section 65B(4), affirming that the electronic evidence was produced by a computer regularly used for such purposes, the integrity of the data and device must be maintained, the device must be in lawful control of the person producing the evidence.

JUDICIAL INTERPRETATION: In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court ruled that Section 65B is the exclusive method to admit electronic evidence and that oral

[21] Ministry of Electronics and Information Technology, *Information Technology (Amendment) Act, 2008*, Government of India.
[22] Prashant Iyengar, *Interception and Monitoring Framework in India*, Centre for Internet & Society (CIS), 2014

evidence or other documentary proof is insufficient without the certificate[23]. However, in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), the SC clarified that if the certificate cannot be produced despite reasonable efforts, the court may exercise discretion in its admission.

Application in Terror Cases: Often, terrorism-related digital evidence from encrypted chats, call records, device imaging is collected without the proper 65B certificate, especially when extracted from foreign servers or apps. This renders the evidence vulnerable to legal challenges.

c) *CODE OF CRIMINAL PROCEDURE (CRPC), 1973:* While the CrPC predates digital technology, it lays down the procedural safeguards for searches, seizures, and arrests: *Section 91:* Permits the issuance of summons or written orders to produce documents or digital devices before the court. *Sections 100 & 165:* Deal with search and seizure operations, including entry into premises, and the creation of search lists or panchanamas. *Sections 451 & 457*: Concern the custody and disposal of property or articles seized during investigation, which includes digital devices.

Challenges: No explicit mention of digital cloning or hashing in CrPC leads to ambiguity in handling forensic images. The absence of standard guidelines for digital chain of custody results in frequent tampering allegations. Delays in producing digital devices before magistrates, or extracting data without authorization, affect the admissibility of evidence[24]

d) *UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967 (UAPA)* - UAPA is India's primary anti-terror law. Over the years, its definition of terrorism has expanded to cover digital, financial, and ideological aspects of terror. Pertinent to digital investigations: *Section 15:* Defines a "terrorist act" which includes disruption of computer networks or services that threaten national security. *Sections 17–18B:* Penalize terror funding, conspiracy, and recruitment, often proved via online communication records. *Section 43D(5):* Introduces stringent bail conditions in UAPA cases, which makes digital evidence pivotal in pre-trial detention.

Challenge: The reliance on preliminary digital leads without

[23] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473
[24] Apar Gupta, *Chain of Custody for Digital Evidence in Indian Criminal Procedure*, National Law School of India Review, 2016.

corroborative physical evidence has led to extended detentions under UAPA, drawing criticism from human rights advocates.

LEGAL CHALLENGES IN PRACTICE

Authentication and 65B Certificate Compliance: As noted, digital evidence without a 65B certificate is inadmissible. This poses practical issues when: Devices are seized without immediate access to forensic tools. Service providers (like WhatsApp or Telegram) are based abroad and do not issue legally compliant certificates and Investigating officers lack training in digital evidence handling and fail to maintain logs or hashes. In cases like State v. Navjot Sandhu (2005) (Parliament attack case), courts previously allowed printouts and oral testimony, but these are no longer valid after Anvar[25].

Jurisdictional and Cross-Border Data Issues: Terror networks often use foreign-hosted platforms and servers, such as Signal or ProtonMail, which operate from privacy-protecting jurisdictions. Legal challenges include: Inability to access data stored outside India without Mutual Legal Assistance Treaties (MLATs), which are time-consuming and rarely successful within investigation timelines.

Chain of Custody and Forensic Integrity : Courts require assurance that the digital evidence has not been tampered with from the point of seizure to presentation in court. However, many terrorism cases falter due to: No hash value generated at the time of device seizure. Delay in forensic imaging. Inadequate storage facilities leading to data corruption. Lack of logs documenting who accessed or analyzed the data. The absence of a secure digital evidence management system weakens prosecutorial claims and invites defense objections[26]. In cases like the Kashmir killings (2025), any delays in obtaining call logs or decrypting communications could impact the timely arrest of conspirators. Additionally, the admissibility of intercepted messages or foreign-hosted server data under Indian law poses procedural hurdles in prosecuting such acts of terror."

Surveillance and Privacy Concerns: India lacks a dedicated privacy or surveillance law. The existing regime under Section 69 of the IT Act is considered opaque, and there's minimal judicial oversight over interception orders. In Puttaswamy v. Union of India (2017), the Supreme Court upheld the Right to Privacy as a fundamental right. This decision places constitutional checks on digital surveillance, which complicates proactive terror monitoring unless legally backed[27]. Additionally, critics

[25] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 – The Supreme Court held that electronic evidence must be accompanied by a certificate under Section 65B of the Indian Evidence Act, 1872, to be admissible in court.
[26] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 – Clarified that secondary electronic evidence, including printouts or copies, must have a certificate under Section 65B for admissibility, unless the original producer of the evidence is unavailable.
[27] Puttaswamy v. Union of India, (2017) 10 SCC 1 – The Supreme Court ruling that recognized the Right to Privacy as a fundamental right, which affects the use of digital surveillance tools.

argue that excessive use of social media monitoring tools and facial recognition may lead to profiling and abuse, particularly in communally sensitive cases.

ADMISSIBILITY OF ELECTRONIC EVIDENCE: LEGAL AND PRACTICAL CHALLENGES

SECTION 65B: THE CORNERSTONE OF ADMISSIBILITY: Section 65B of the Indian Evidence Act, 1872, is the statutory provision governing the admissibility of electronic records. It mandates a certificate under Section 65B(4) to authenticate any digital document or record, without which such evidence is inadmissible. The certificate must confirm: The electronic record was produced by a computer regularly used during the ordinary course of activity. The device was operating properly. The information is a faithful reproduction[28]. The Supreme Court in Anvar P.V. v. P.K. Basheer (2014) laid down a strict interpretation, holding that no electronic record can be admitted without a 65B certificate, regardless of whether the original device is available.[29]

CHALLENGES IN CROSS-BORDER DIGITAL EVIDENCE

In terrorism investigations, digital trails often lead to platforms hosted outside India—such as WhatsApp (Meta, U.S.), Telegram (Dubai), ProtonMail (Switzerland), etc. This presents a serious challenge: Indian investigators cannot directly compel foreign service providers to hand over data or furnish a 65B certificate. Even if data is received through Mutual Legal Assistance Treaties (MLATs), the foreign format of the evidence may not conform to Indian evidentiary standards. Time lags in cross-border cooperation often render the data obsolete or inadmissible by the time it reaches court.

This jurisdictional vacuum allows accused persons to challenge the integrity of data and, in several cases, walk free due to technicalities despite strong circumstantial evidence.

ARTICLE 21 AND THE PRIVACY-SURVEILLANCE BALANCE

Article 21 of the Constitution guarantees the right to life and personal liberty, including the right to privacy, as declared in Justice K.S. Puttaswamy v. Union of India (2017)[30]. While this

[28] This position was clarified and reaffirmed in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), where the Court held that secondary electronic evidence (e.g., printouts, copies) without the certificate is inadmissible

[29] State v. Navjot Sandhu, (2005) 11 SCC 600 – The case where the court allowed printouts and oral testimony, but the use of these forms of evidence was rendered inadequate following the Anvar ruling.

[30] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 – The Supreme

right is not absolute, any restriction must meet the test of: Legality (a law must exist), Necessity (based on a legitimate state aim), and Proportionality (least intrusive means). This constitutional safeguard clashes with digital surveillance practices under Section 69 of the IT Act, which permits interception without judicial sanction, raising concerns over mass surveillance, profiling, and breach of individual liberties. Terrorism cases often justify such surveillance on grounds of national security. However, when evidence obtained through such surveillance is brought to court, it can be challenged on grounds of constitutional illegality, particularly if not authorized, overbroad, or disproportionate[31].

Procedural And Infrastructure Gaps

Delays in forensic reports: Central and State Forensic Science Laboratories (FSLs) are often understaffed and under-resourced, leading to delays of months or even years in generating digital evidence reports. *Lack of certified digital forensic labs:* India lacks adequate NIST-certified digital labs capable of hashing, imaging, and verifying large volumes of data, especially in high-profile terrorism cases. *Inadequate training*: Police officials often do not follow proper chain-of-custody procedures or hash generation protocols, which opens the door to tampering allegations and evidentiary exclusion.

Role Of Technology In Enhancing National Security

The digital transformation of warfare and crime has necessitated a corresponding transformation in national security architecture. In India, as terrorism increasingly adapts to the digital age—through cyberattacks, online radicalization, and encrypted communications—technology has emerged not only as a challenge but also as an indispensable tool in counter-terrorism operations. This section explores the emerging technologies deployed to bolster national security, their operational potential, and the ethical dilemmas they present.

EMERGING TOOLS IN NATIONAL SECURITY AND COUNTERTERRORISM

Artificial Intelligence (AI) and Machine Learning

AI and ML are being increasingly deployed to detect patterns in

Court ruling that recognized the Right to Privacy as a fundamental right, significantly affecting surveillance laws and practices in India.

[31] Section 69 of the IT Act, 2000 – Provides the legal framework for government surveillance, allowing interception, monitoring, and decryption of information for national security reasons, without judicial oversight.

vast datasets, identify abnormal behavior, and predict potential threats. For instance: Facial recognition algorithms powered by AI are used in real-time surveillance to track suspects in crowded places like railway stations and airports[32] ML models trained on behavioral data help forecast radicalization trajectories, flagging individuals who exhibit early signs of extremist ideology on social media.

Data Mining and Big Data Analytics

Data mining allows security agencies to uncover hidden connections among suspects, locations, financial transactions, and communications. By correlating billions of data points across platforms and geographies, agencies can: Map out terrorist networks and funding channels. Identify sleeper cells and logistical support systems through cluster analysis.

Drone Forensics and Surveillance

Drones are not only being used for physical surveillance but also carry forensic potential, Drone forensics involves extracting flight logs, GPS data, and payload deployment information to reconstruct suspect activities. In operations like in Jammu & Kashmir, drones have been used to intercept arms drops and conduct terrain mapping of infiltration routes.

Blockchain Tracing

Terrorist organizations often utilize cryptocurrencies to move funds anonymously. However, blockchain's immutability also becomes a tool for investigators: Tools like Chainalysis[33] allow investigators to trace crypto wallets, understand token flows, and uncover fundraising campaigns for terrorism on the dark web. The Financial Intelligence Unit-India (FIU-IND)[34] has started training in blockchain tracing to counter crypto-enabled terror financing.

PREDICTIVE POLICING AND INTELLIGENCE ANALYSIS

The predictive policing uses algorithms to assess crime probability in specific areas or by specific individuals, based on historical

[32] Crime and Criminal Tracking Network & Systems (CCTNS) - An initiative aimed at creating a nationwide network for tracking and managing criminal activities through digital data
[33] Chainalysis - A blockchain analytics tool that helps investigators trace cryptocurrency transactions and uncover illicit activity related to terrorism financing.
[34] Financial Intelligence Unit-India (FIU-IND) - The governmental agency responsible for analyzing financial data to combat money laundering and terrorism financing in India.

data, time patterns, and behavioral cues.

For example, metadata from mobile towers, financial transactions, and travel history can feed into predictive models to assess the threat level of an individual. Fusion centers like the National Intelligence Grid (NATGRID)[35] aggregate data from multiple ministries (immigration, tax, telecom) to create actionable intelligence in real-time. This enables security agencies to intervene before an attack occurs, shifting the paradigm from reactive to preventive counterterrorism.

METADATA ANALYSIS AND TERRORIST PROFILING

In the absence of content, metadata becomes the next best asset for intelligence gathering: Call Detail Records (CDRs) reveal not only whom a suspect talks to, but also when, where, and how often. Geolocation metadata from photos and videos can provide location clues even if the content is encrypted or deleted. Social media metadata—likes, shares, and hashtags—helps map out ideological networks and influence patterns of online radicalizers[36]. Through such profiling, agencies can isolate "nodes" and "hubs" in a digital terror ecosystem, allowing targeted interventions.

ENCRYPTED EMAIL TRACING, GPS, AND FACIAL RECOGNITION

While terrorist organizations increasingly use end-to-end encrypted platforms, agencies are evolving countermeasures: Encrypted email tracing techniques involve obtaining metadata from service providers, applying correlation analysis, and using endpoint surveillance or Trojan implants to breach secure systems. GPS tracking both through active surveillance (like vehicle trackers) and passive data from smartphones helps reconstruct movement histories and verify alibis. Facial Recognition Technology (FRT) is now integrated with CCTV grids in cities like Delhi and Hyderabad, and is also used in border control and immigration checks[37]. India's Home Ministry is implementing the Automated Facial Recognition System (AFRS) to link facial data with crime records, passports, and Aadhaar databases.

[35] National Intelligence Grid (NATGRID) - A project aimed at providing law enforcement agencies with real-time access to vast datasets from various government ministries for national security purposes.
[36] United Nations Office on Drugs and Crime (UNODC), *Handbook on the Use of Social Media in Investigations of Terrorism* (UNODC, 2021).
[37] Home Ministry of India, *Automated Facial Recognition System (AFRS) Guidelines* (2020).

ETHICAL AND CONSTITUTIONAL IMPLICATIONS

Surveillance vs. Privacy

The expanded use of surveillance technologies raises critical questions about the right to privacy, affirmed as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017). With the increasing use of tools like Pegasus spyware, facial recognition, and mass metadata collection, the tension between individual liberty and collective security becomes pronounced. Critics argue the lack of a robust data protection law in India allows unchecked surveillance[38]. There is also no independent oversight mechanism to ensure accountability in intelligence operations.

Comparative Perspective

The global nature of terrorism and cybercrime necessitates comparative legal and enforcement responses. Countries like the USA, UK, and the EU have significantly advanced their digital forensics frameworks to tackle terrorism-related threats. India, while making commendable progress, still lags in terms of integration, infrastructure, training, and legal clarity. Studying how other jurisdictions approach digital forensics in terrorism cases offers India a roadmap for institutional reform and capacity building.

- ***United States:*** The USA's approach is deeply influenced by the post-9/11 security doctrine. The USA PATRIOT Act, enacted in 2001, expanded the surveillance and investigation powers of federal agencies. The FBI's Cyber Crime Division works alongside agencies like the NSA and Department of Homeland Security to detect and prevent cyberterrorism[39]. The USA also passed the CLOUD Act (2018), allowing the government to access data stored by US companies even if hosted abroad, resolving many jurisdictional challenges. In terms of practice, agencies rely heavily on tools like IP tracking, device imaging, decryption software, and AI to identify threat actors and prosecute them effectively[40].
- ***United Kingdom:*** The UK employs a robust intelligence and cybersecurity framework led by MI5 (domestic security), MI6 (foreign intelligence), and the Government Communications Headquarters (GCHQ). The Investigatory Powers Act 2016, also known as the "Snoopers' Charter,"

[38] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[39] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)
[40] CLOUD Act, Pub. L. No. 115-141, 132 Stat. 348 (2018)

governs interception, equipment interference, and bulk data collection, providing legal backing for surveillance in terrorism cases.[41]
GCHQ is known for its prowess in decryption and threat monitoring. UK agencies also work closely with local police cyber units to maintain chain-of-custody protocols in forensic investigations[42]. The UK uses social media monitoring tools, metadata analysis, and AI-driven profiling to anticipate and neutralize threats.

- ***European Union:*** The EU maintains a delicate balance between civil liberties and counterterrorism through legislation like the General Data Protection Regulation (GDPR). While GDPR imposes strict rules on data collection and storage, it also allows member states to carve exceptions for national security purposes. Agencies such as Europol and ENISA (European Union Agency for Cybersecurity) play pivotal roles in inter-country coordination.

CONCLUSION

Digital forensics has emerged as a cornerstone of modern counterterrorism strategy. As terrorism morphs into increasingly digital forms—ranging from encrypted communications to dark web propaganda and online fundraising—the Indian state must enhance its capacity to lawfully extract, preserve, and present digital evidence.

Legal admissibility alone is insufficient. What India needs is a robust framework that marries technical excellence with procedural fairness and constitutional compliance. Safeguards under Article 21 must coexist with national security imperatives. A dedicated legal regime, institutional capacity building, and stronger coordination mechanisms will ensure that digital forensics transitions from a reactive investigative tool to a proactive intelligence asset.

BIBLIOGRAPHY

Statutes and Bare Acts:

- *Information Technology Act, 2000*
- *Indian Evidence Act, 1872*
- *Code of Criminal Procedure, 1973*
- *Unlawful Activities (Prevention) Act, 1967*

[41] Investigatory Powers Act 2016, c. 25 (UK)
[42] GCHQ, "Cyber Security: Protecting the UK from Cybercrime" (GCHQ, 2020)

Landmark Judgments:

- *Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473*
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1*
- *Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1*

Government & Institutional Reports:

- *National Investigation Agency (NIA) case files*
- *CERT-In Annual Reports*
- *NTRO Cyber Security Strategies*

Secondary Sources:

- *Academic journals on digital evidence and national security*
- *News articles from The Hindu, Indian Express, Hindustan Times, and Scroll*
- *International reports by Europol, ENISA, and the Council of Europe*
- *Commentary on the Data Protection Bill and Surveillance Laws in India*