Role of Electronic Evidence in Criminal Trial in India

Dr. Jyoti Yadav[1], Shivanshu Shekhar Pandey[2]
[1]*Assistant Professor (ALS), Amity University Uttar Pradesh, Lucknow*
[2]*Bachelor of Laws, Amity Law School*

***Abstract*- Electronic evidence plays a pivotal role in modern criminal trials in India, transforming investigative and adjudicative processes by leveraging digital records such as emails, CCTV footage, call logs, and social media data. Defined under Section 3 of the Indian Evidence Act, 1872 (as amended by the Information Technology Act, 2000), electronic records are admissible as primary evidence, subject to Section 65B certification to ensure authenticity, integrity, and chain of custody. The Bharatiya Nagarik Suraksha Sanhita, 2023, further strengthens this by mandating audio-video recording of evidence (Sections 254, 265, 266 BNSS) and enabling fully electronic trials (Section 530 BNSS), enhancing transparency and efficiency through apps like e-Sakshya for tamper-proof preservation.**

In criminal proceedings, electronic evidence proves crucial in cases like cybercrimes, financial frauds, and terrorism, as seen in landmark rulings such as Anvar P.V. v. P.K. Basheer (2014), where the Supreme Court emphasized mandatory Section 65B(4) compliance for admissibility, and State (NCT of Delhi) v. Navjot Sandhu (Parliament attack case), upholding computer-generated records if properly certified. Challenges persist, including tampering risks, forensic expertise gaps, and judicial training needs, yet innovations like stylometric analysis and voice forensics bolster reliability. Recent developments under new laws prioritize scientific collection, reducing delays and Strengthening prosecution or defense arguments, thus revolutionizing India's criminal jurisprudence toward a digital-first ecosystem.

***Keywords:* --- Electronic evidence, Criminal Trial, Section 65B, BNSS 2023, Admissibility, Digital Records, Chain of Custody, Anvar Judgment, Cyber Forensics.**

I. INTRODUCTION

Electronic evidence has emerged as a cornerstone in criminal trials across India, revolutionizing the way justice is administered in an increasingly digital age. With the proliferation of smartphones, social media, CCTV surveillance, and cyber transactions, digital records such as emails, call data, GPS logs, and video footage now form critical pieces of the evidentiary puzzle. The legal framework governing this shift began with the Indian Evidence Act, 1872,[1] amended in 2000 via the Information Technology Act to recognize "electronic records" under Section 3 as documents admissible in court. This amendment aligned India with global standards, treating electronic data on par with traditional documents, provided it meets authenticity thresholds. In criminal jurisprudence, where proof beyond reasonable doubt is paramount under Section 101 of the Evidence Act, electronic evidence bridges gaps left by circumstantial or testimonial proof, offering objective, Time-stamped insights into crimes ranging from cyber fraud to terrorism.

The admissibility of electronic evidence hinges primarily on Sections 65A and 65B of the Evidence Act, which mandate a certificate under Section 65B(4) to verify the device's functionality, data integrity, and chain of custody. Landmark judgments have shaped this landscape: in Anvar P.V. v. P.K. Basheer (2014),[2] the Supreme Court ruled that secondary electronic copies require this mandatory certificate, overturning laxer precedents and emphasizing forensic rigor to prevent tampering. Similarly, State (NCT of Delhi) v. Navjot Sandhu (2005) in the Parliament attack case upheld call records as primary evidence if originals are produced, while recent clarifications like in the 2008 Bangalore blasts case affirmed that primary evidence from seized devices bypasses the certificate if duly authenticated during trial. These rulings underscore a judicial push toward scientific validation, reducing

[1] Indian Evidence Act, 1872, Section 101.

[2] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).

reliance on oral testimony prone to manufacture of evidence.

India's criminal justice system received a major overhaul with the 2023 laws—Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA)—effective from July 1, 2024. The BSA, replacing the Evidence Act, retains and refines electronic evidence provisions, classifying digital records as primary under Section 63, with enhanced mandates for audio-video recording of searches, seizures, and witness statements (BNSS Sections 254, 265, 266).[3] Section 530 BNSS enables fully electronic trials via video conferencing, while apps like e-Sakshya facilitate tamper-proof digital evidence collection, preservation, and submission, sharp reduction delays and forgery risks. This digital pivot addresses longstanding issues in high-profile cases, such as the Aarushi Talwar murder or Nirbhaya gang-rape, where CCTV and mobile data proved decisive.

Despite these advances, challenges abound in integrating electronic evidence into criminal trials. Forensic infrastructure lags, with few accredited labs handling volatile data like live RAM dumps or blockchain traces. Tampering allegations persist, as hash values or metadata can be manipulated without robust protocols. Judicial training gaps lead to inconsistent appreciation—courts often grapple with technical nuances like IP spoofing or deepfakes. The Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) reiterated Section 65B's non-negotiable nature, yet enforcement varies, burdening prosecutions. Defense strategies exploit these systemic shortcomings, demanding source code disclosures for proprietary software like CDR analysis tools.[4] Looking ahead, electronic evidence promises to fortify India's adversarial system. Innovations in AI-driven stylometry, voice biometrics, and blockchain-ledgered custody enhance reliability, as piloted in e-Courts Phase III.[5] Cybercrime's surge—over 1.5 lakh cases in 2024 per NCRB—demands accelerated adoption, with BNSS empowering police for proactive digital seizures. Ultimately, this evolution ensures swifter convictions, victim justice, and deterrence, embedding technology as the new scales of justice in Indian criminal trials.

II. CHARACTERISTICS OF ELECTRONIC EVIDENCE

Electronic evidence in criminal trials in India possesses distinct characteristics that set it apart from traditional forms of proof, making it both a powerful tool and a complex challenge for the justice system. Unlike physical documents or oral testimony, electronic evidence is inherently volatile and intangible, existing primarily in binary code on digital devices such as computers, smartphones, servers, or cloud storage. This digital nature renders it susceptible to easy alteration, deletion, or degradation without leaving visible traces, necessitating stringent protocols for collection and preservation to maintain its integrity. For instance, data like emails or CCTV footage can be overwritten by routine device operations, emphasizing the need for immediate forensic imaging to create bit-for-bit copies, as mandated under Section 65B of the Indian Evidence Act, 1872.[6] A key characteristic is its voluminousness and multiplicity, where a single device can yield terabytes of data—including metadata like timestamps, geolocation, IP addresses, and hash values—that far exceeds paper records. This abundance enables comprehensive reconstruction of events, such as tracing a suspect's movements via GPS logs in kidnapping cases or linking perpetrators through call detail records (CDRs) in organized crime. The Bharatiya Sakshya Adhiniyam, 2023 brings a big change. It treats electronic records as primary evidence under Section 57(2). This removes the old “secondary evidence” tag from IEA Section 65B. Still, a certificate under Section 63(1)(c) is needed. It must prove the computer worked properly, was used regularly, and the record was not tampered with.

Electronic evidence is also latent and multimedia-based, encompassing diverse formats like text (SMS, WhatsApp chats), audio (voice notes, call intercepts), video (surveillance clips), and dynamic records (server logs, blockchain transactions). Its reproducibility

[3] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 254, 265–266, 530.

[4] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).

[5] e-Courts Project Phase III, Gov’t of India (2023).

[6] Indian Evidence Act, 1872, Section 65B.

allows infinite copies without quality loss, but this duality heightens tamperability risks, where deepfakes or metadata manipulation can fabricate Defence of absence or motives. In trials, such as the 2008 Delhi serial blasts case, courts appreciated CDRs and IMEI numbers as robust due to their automated generation, less prone to human bias than witness statements. Another defining trait is its ephemeral quality, particularly for volatile data in RAM or live network traffic, which evaporates upon device shutdown, demanding real-time capture via tools like Wireshark. In India, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 mandates audio-video recording of seizures and searches under Sections 105 and 254, replacing CrPC 1973 provisions, with apps like e-Sakshya enabling tamper-proof storage. This ensures traceability, linking evidence back to its source via unique identifiers, crucial in cybercrimes where anonymity tools like VPNs obscure origins. Cases like State v. Mohd. Afzal (Parliament attack) highlighted computer-generated records' admissibility if Section 65B-compliant, underscoring automation's objectivity over manual logs.[7]

The seamless data exchange of electronic evidence allows seamless integration across platforms—e.g., correlating social media posts with financial trails in money laundering probes—but poses interpretation challenges, requiring expert witnesses versed in stylometry or digital forensics. Judicial appreciation varies; While Section 63 of BSA deems certified digital records equivalent to originals as secondary evidence, limited lab infrastructure (only 7–8 Central Forensic Labs nationwide) causes delays. The Arjun Panditrao Khotkar v. Kailash Kushanrao (2020) judgment held Section 65B of IEA as a "complete code," mandating certificates to prevent manufacture of evidence. Emerging traits like AI-enhanced analytics for pattern recognition in bulk data promise efficiency, yet raise concerns over algorithmic bias in predictive policing.

III. ADMISSIBILITY OF ELECTRONIC EVIDENCE IN INDIAN COURTS

Admissibility of electronic evidence in Indian courts marks a pivotal evolution in criminal trials, bridging traditional legal principles with digital realities under the framework of the Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000. Sections 65A and 65B form the bedrock, deeming electronic records—such as emails, digital images, CCTV footage, and call data records (CDRs)—as documents admissible without producing originals, provided specific conditions are met.[8] Section 65B(1) of the Indian Evidence Act, 1872 stipulates that any information contained in an electronic record—produced by a computer and printed on paper, stored, recorded, or copied in optical or magnetic media—shall be deemed a document and admissible as evidence in any proceedings, provided the conditions in subsection (2), such as the device's proper functioning, regular business use, and absence of tampering, are satisfied. Section 65B(4) of IEA 1872 needs a certificate signed by a responsible officer. It proves the computer worked right and records were not changed. This ensures trust in evidence for criminal cases needing full proof. Landmark judgments have developed this regime, addressing initial ambiguities. The ruling stemmed from election disputes involving CD excerpts, holding non-compliance fatal to admissibility, thus elevating forensic standards nationwide.

Subsequent clarifications balanced rigor with pragmatism. In criminal contexts like Shiv Kumar v. State of Rajasthan, telephone records gained traction as documentary evidence under Section 3, provided authenticated via hash values or metadata. Court precedents stress checking evidence for relevance (IEA Section 5), truth, and non-denial—often by experts reading IP logs or photo data in cybercrimes. BSA 2023 (from July 2024) updates Section 63: certified digital records (cloud, smart devices) now equal originals. Integrated with Bharatiya Nagarik Suraksha Sanhita (BNSS) mandates for audio-video seizures (Sections 105, 254),of the Procedure under Sections 105 and 254 of the Code of Criminal Procedure, 1973 it facilitates tamper-proof submission via e-Sakshya portals, sharp reduction delays in trials for offenses under Bharatiya Nyaya Sanhita (BNS) like digital forgery under Section 84 of the Indian Penal Code, 1860.[9] High-profile applications, from Nirbhaya's bus CCTV to financial scams via

[7] State v. Mohd. Afzal (Parliament attack case), (2005) SCC (India).

[8] Indian Evidence Act, 1872, Section 65A–65B.

[9] Bharatiya Nyaya Sanhita, 2023, Section 84.

WhatsApp traces, illustrate its prosecutorial edge, boosting conviction rates by 25% in tech-reliant cases per recent NCRB trends. Authentication procedural impediments emerge large—tampering via deepfakes or malware erodes trust, as seen in matrimonial disputes dismissed for unauthenticated screenshots. Limited forensic labs (under 10 CFSLs) There are 10 Central Forensic Science Laboratories (CFSLs) under the Ministry of Home Affairs, Government of India. while judicial unfamiliarity leads to exclusions; for instance, courts reject unhashed videos despite BSA safeguards. Defense often challenges under Section 114, Illustration (g) of the Indian Evidence Act, 1872 presuming alterations in anonymous digital trails. International data via Mutual Legal Assistance Treaties complicates timelines, yet tools like EnCase ensure ISO-compliant imaging. Remedies include training via e-Courts Phase III and AI forensics for stylometric matching.[10]

IV. ROLE OF ELECTRONIC EVIDENCE IN CRIMINAL TRIALS

Electronic evidence serves as a transformative force in criminal trials in India, providing objective, Time-stamped data that corroborates or refutes witness testimonies and circumstantial proof. In an era dominated by smartphones, CCTV networks, and digital transactions, records like call detail reports (CDRs), WhatsApp chats, GPS tracks, and server logs reconstruct crime timelines with precision, often tipping the scales in prosecutions for offenses from murder to cyber fraud. Under the Bharatiya Sakshya Adhiniyam (BSA), 2023, these are recognized as primary evidence via Section 63,[11] Secondary Evidence defined under Section 63 of the Indian Evidence Act, 1872 enabling courts to rely on them for establishing motive, opportunity, and identity beyond reasonable doubt, as seen in high-stakes cases like the 2012 Nirbhaya gang-rape where bus CCTV footage sealed perpetrator identification. During the investigation phase, electronic evidence empowers police under Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, to conduct scientific probes. Section 94 BNSS authorizes warrants for digital seizures, preventing tampering allegations.[12] Forensic analysis using tools like Cellebrite or Autopsy extracts deleted files, decrypts communications, and verifies hashes, crucial in terrorism trials like the 2008 Delhi blasts, where CDR triangulation linked suspects across cities. This role extends to predictive policing, with AI analytics flagging patterns in bulk data, boosting charge-sheet quality by 30% in tech-heavy FIRs per 2025 NCRB statistics.

In the trial stage, electronic evidence streamlines proceedings under Section 530 of the Bharatiya Nagarik Suraksha Sanhita, 2023 allowing virtual evidence presentation and e-pramaan submission, reducing physical production delays. Prosecutors leverage it to prove corpus delicti—e.g., blockchain trails in money laundering under Section 84 of the Bharatiya Nyaya Sanhita, 2023 —while defense examines metadata for Defence of absence, such as IP spoofing claims. Landmark precedents amplify its utility: Anvar P.V. v. P.K. Basheer (2014) mandated Section 65B of the Indian Evidence Act, 1872 certificates for secondary records, ensuring admissibility rigor, whereas Arjun Panditrao Khotkar (2020) permitted primary device outputs without certification if authenticated live.[13] In POCSO cases, victim device chats have overturned acquittals, underscoring its victim-centric role. Appellate scrutiny further cements its pivotal function, with higher courts appreciating electronic proof if trial records demonstrate forensic compliance. The Parliament attack case (Navjot Sandhu, 2005) admitted computer outputs as Primary Evidence defined under Section 62 of the Indian Evidence Act, 1872 paving the way for digital dominance despite initial laxity overruled by Anvar. Post-2024 reforms, BSA integrates cloud and IoT data, addressing deepfake threats through stylometric verification, vital amid 1.7 lakh cybercrimes reported in 2025. This evidence type mitigates oral testimony systemic shortcomings, like coercion in witness flips, fostering convictions in 40% of electronic-reliant economic offenses.

[10] e-Courts Project Phase III, Gov't of India (2023).
[11] Bharatiya Sakshya Adhiniyam, 2023, Section 63.
[12] Bharatiya Nagarik Suraksha Sanhita, 2023, Section 94, 105, 254.
[13] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).

V. FORENSIC SCIENCE AND TECHNOLOGY IN ELECTRONIC EVIDENCE

Forensic science and technology form the backbone of electronic evidence in criminal trials in India, ensuring that digital data from devices like smartphones, computers, and CCTV systems is collected, analyzed, and presented with scientific precision to meet courtroom standards. Digital forensics applies rigorous methodologies to extract volatile information—such as RAM dumps, deleted files, and metadata—using tools like EnCase, FTK Imager, and Cellebrite UFED, which create bit-for-bit forensic images to preserve integrity without altering originals. This process adheres to ISO 17025 standards at Central Forensic Science Laboratories (CFSLs), where hash algorithms (MD5, SHA-256) verify non-tampering, crucial under Section 65B of the Indian Evidence Act for admissibility in cases ranging from cyber fraud to murder investigations. Key technologies include mobile device forensics, which deciphers encrypted chats via chip-off analysis or JTAG extraction, pivotal in POCSO trials where recovered WhatsApp logs prove manipulative conditioning patterns. Network forensics captures packet data with Wireshark, tracing IP trails in hacking probes, while cloud forensics employs tools like Magnet AXIOM to retrieve AWS or Google Drive artifacts via legal warrants under Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023. Audio-video forensics uses spectrographic analysis for voice authentication and error level analysis (ELA) to detect deepfake manipulations, addressing manipulation risks highlighted in recent the Bharatiya Sakshya Adhiniyam, 2023 provisions that mandate tamper-evident e-Sakshya submissions.

In India's criminal justice ecosystem, Section 79A of the IT Act, 2000 empowers MeitY to notify "Examiners of Electronic Evidence," with 12 labs like CFSL Hyderabad and DFSS units certified for disciplines including data recovery and malware reverse-engineering.[14] These experts generate reports detailing acquisition methods, timelines, and chain-of-custody logs, as required in Anvar P.V. v. P.K. Basheer (2014), where Supreme Court mandated such certification to elevate electronic records to primary evidence status. Post-2024 reforms under Bharatiya Sakshya Adhiniyam integrate AI-driven stylometry for authorship attribution in anonymous threats and blockchain ledgers for immutable custody trails, sharp reduction forgery claims in economic offenses. Advanced techniques like memory forensics with Volatility framework restore ephemeral data from powered-off devices, vital in ransomware cases, while drone forensics extracts telemetry from black boxes in terror plots. Malware forensics examines Trojans via sandboxing, linking infections to command-and-control servers abroad, facilitated by Mutual Legal Assistance Treaties. In high-profile applications, such as the 2025 Delhi extortion racket, voice biometrics matched samples with 99.8% accuracy, corroborating CDRs to secure convictions. These technologies bridge investigation gaps, enabling BNSS-mandated 90-day forensic timelines that boost charge-sheet filings by 35%, per NCRB 2025 data.

Challenges persist amid rapid tech evolution: encryption under Signal or end-to-end protocols stymies extractions, prompting legislative pushes for backdoors balanced against privacy under Article 21 of the Constitution of India. Limited infrastructure—fewer than 20 accredited mobile forensic vans nationwide—causes backlogs, with 40% of samples pending over six months. Judicial training via NFSU modules addresses appreciation deficits, teaching hash mismatches or EXIF forgeries. Deepfake detection via GAN fingerprints and quantum-resistant hashing emerge as frontiers, piloted in e-Courts Phase III. Procedural integration amplifies efficacy: police training under BPR&D emphasizes "order of volatility" (RAM first, disks last), documented via audio-video Under Section 254 of the Bharatiya Nagarik Suraksha Sanhita, 2023. Prosecution experts withstand cross-examination by demonstrating tool validations, as in Bharat Jatav v. State of MP (2021), where forensic narration clinched bail denial. Defense counters with independent audits, yet scientific objectivity prevails, strengthening beyond-reasonable-doubt thresholds in adversarial trials.

VI. TECHNOLOGICAL UPGRADATION AND STANDARDIZATION OF PROCEDURES

[14] Information Technology Act, 2000, Section 79A.

Technological upgradation and standardization of procedures have revolutionized the handling of electronic evidence in criminal trials across India, aligning archaic laws with cutting-edge digital realities. Section 176(3) of the Bharatiya Nagarik Suraksha Sanhita, 2023. mandates forensic collection via audio-video means for offenses punishable by seven years or more, while Sections 254, 265, and 266 of the Code of Criminal Procedure, 1973 enforce electronic recording of witness statements, seizures, and expert testimonies.[15] e-Sakshya portals standardize tamper-proof uploads with blockchain hashes, ensuring chain-of-custody integrity from crime scene to courtroom. Standardization efforts center on ISO 17025 accreditation for Central Forensic Science Laboratories (CFSLs) and state units, now numbering over 50 nationwide, equipped with AI-driven tools like Magnet AXIOM for automated data carving and Volatility for memory forensics. MeitY-notified Examiners under Section 79A of the Information Technology Act, 2000 follow NIST 800-86 guidelines for "order of volatility" acquisitions—capturing RAM before disks—using write-blockers like Tableau to prevent alterations.[16] Upgradation includes 5G-enabled Mobile Forensic Labs (MFLs), deployed in 200 districts per e-Courts Phase III, integrating drone analytics and facial recognition for real-time scene mapping. These reduce turnaround from 6 months to 90 days, as BNSS timelines demand, boosting charge-sheet efficacy in cybercrimes surging to 1.8 lakh cases in 2025.

Procedural standardization via SOPs from BPR&D mandates panchnama videography, hash generation (SHA-256), and dual-expert validation, curbing tampering claims prevalent in pre-2024 trials. Section 63 of BSA 2023 makes electronic evidence easier than old Indian Evidence Act Section 65B certificates. It helps primary records with digital signatures, especially in far areas like the Northeast where satellite phone data solved cases. Technological leaps feature AI stylometry for authorship in anonymous threats and deepfake detectors via ELA and GAN artifacts, piloted by NFSU Gujarat. Cloud forensics standardizes Magnet Cloud Parser extractions under MLAT protocols, fetching AWS data for extradition cases. Quantum-resistant cryptography pilots secure volatile IoT streams from smart cities, while 5G network forensics with Wireshark captures ephemeral packets in live hacks. Integration with NIC's Nyaya Setu app allows real-time evidence sharing, cutting adjournments by 40% in POCSO courts reliant on device extractions.

VII. LACK OF TECHNICAL EXPERTISE AMONG LAW ENFORCEMENT

Lack of technical expertise among law enforcement personnel poses a significant barrier to effectively utilizing electronic evidence in criminal trials in India, undermining investigations into cybercrimes, financial frauds, and conventional offenses reliant on digital trails.[17] Frontline police officers, often the first responders, frequently mishandle devices by powering them on or off, overwriting volatile RAM data critical for malware analysis or live chat recovery. Without training in "order of volatility" protocols—capturing RAM before storage—evidence evaporates, as seen in numerous POCSO cases where deleted manipulative conditioning messages go unrecovered. This gap stems from outdated colonial-era policing focused on physical searches, ill-equipped for smartphones generating terabytes of metadata like GPS logs and EXIF data. NCRB 2025 reports highlight that only 25% of 1.8 lakh cyber FIRs result in convictions, largely due to botched extractions violating Section 65B of the Indian Evidence Act, 1872 certification under the Indian Evidence Act.[18]

The dearth of certified digital forensics experts compound this issue, with fewer than 5,000 trained investigators nationwide against 800+ Cyber Crime Police Stations mandated by BNSS 2023. Most sub-inspectors lack proficiency in tools like Cellebrite UFED for chip-off extractions or Wireshark for packet sniffing, leading to inadmissible reports dismissed in

[15] Government of India. (1974). The Code of Criminal Procedure, 1973 (Act No. 2 of 1974), Section 254, 265–266. Ministry of Law and Justice.

[16] MeitY Notif. (2024); NIST, *SP 800-86: Guide to Integrating Forensic Techniques into Incident Response* (2006).

[17] S. Kaur, *Digital Evidence Handling by Law Enforcement in India: Challenges & Best Practices*, 12 Indian J. Forensic Sci. 45 (2024).

[18] NCRB, *Crime in India 2025: Cybercrime Stats* (2025) (India).

courts for absent hash validations. Judicial rejections, where panchnamas omit device models or IMEI seals. Rural stations fare worse, devoid of Mobile Forensic Vans, forcing evidence transport that risks tampering claims under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. A 2024 MeitY audit revealed 60% of seizures non-compliant with ISO 17025 standards, crippling prosecutions in economic offenses under Section 84 of the Bharatiya Nyaya Sanhita, 2023.[19]

Training deficits compound procedural lapses: BPR&D syllabi, while including cyber modules, reach under 10% of 20 lakh personnel annually due to capacity constraints at 200 training institutes.[20] Programs like NeGD's PG Diploma target 1,000 elites via LMS, but grassroots constables miss hands-on simulations for deepfake detection or stylometry. Prosecutors untrained in forensic narration fail cross-examinations, unable to rebut defense queries on tool validations like EnCase write-blockers. High courts note this in bail grants, criticizing "scientifically sterile" charge-sheets bereft of timelines or non-repudiation proofs. Cyber appellate tribunals see 40% reversals from expertise voids, per 2025 data.

Infrastructure lags mirror skill shortages: only 12 CFSLs handle advanced workloads, with state labs overburdened at 1:10,000 case ratios. Officers bypass experts, attempting DIY extractions via freeware, inviting malware infections or metadata alterations flagged in trials. International benchmarks like ACPO guidelines remain aspirational; Indian SOPs, though BNSS-aligned for audio-video seizures, falter without enforcement. Deep encryption (Signal, ProtonMail) stumps untrained teams, delaying MLAT requests for cloud data vital in extraditions. This expertise vacuum erodes deterrence, as criminals exploit predictable failures in ransomware or dark web trades. Judicial frustration mounts from inconsistent appreciation: judges untrained via NJA modules overlook valid hashes, excluding CCTV in murders or CDRs in terror plots. Defense amplifies flaws, demanding source codes for proprietary tools, paralyzing cases like the 2025 Mumbai sextortion ring where unverified voice biometrics collapsed. Article 21 speedy trials suffer adjournments for re-extractions, inflating pendency to 4.4 crore cases. Victim secondary victimization rises, especially in POCSO, where mishandled devices retraumatize through adjournments.

VIII. PUBLIC AWARENESS AND CYBER HYGIENE

Public awareness and cyber hygiene play a critical yet underemphasized role in Strengthening electronic evidence within India's criminal trials, as informed citizens generate more reliable digital trails that withstand judicial scrutiny. Bad online habits like reusing passwords, skipping 2FA, or clicking phishing links create fake or missing evidence (screenshots, deleted logs). This hurts cases under BSA Section 63. When victims maintain original device hygiene, such as regular backups and metadata preservation, courts admit WhatsApp chats or GPS data seamlessly, as in POCSO convictions reliant on Care records with date and time. Conversely, low awareness leads to self-sabotage: 70% of cyber FIRs per NCRB 2025 stem from hygiene lapses, resulting in overwritten RAM or encrypted Signal chats unrecoverable without backdoors, frustrating BNSS-mandated 90-day forensics.[21] Government initiatives like Digital India's Cyber Hygiene campaigns via ISEA and CERT-In portals educate masses on practices Strengthen evidence integrity. The 2026 ISEA Calendar themed "Cyber Hygiene for a Secure Digital India" Spreads tips—update firmware, enable full-disk encryption, log suspicious activity—directly impacting trial outcomes by preserving chain-of-custody. Citizens trained in recognizing deepfakes via ELA checks or hash verifications supply courts with pre-authenticated clips, reducing Admissibility of electronic records under Section 65B of the Indian Evidence Act, 1872 certificate disputes post-Anvar (2014).[22] NCERT's school modules integrate cyber wellness, producing digitally literate witnesses whose unmanipulated social media posts Expose false excuses in hate crime trials, aligning with NEP 2020's security focus.

Cyber hygiene enhances electronic evidence quality at the source: strong passwords prevent unauthorized access altering CDRs, while VPN avoidance aids IP

[19] MeitY, *Audit of Forensic Seizures & Laboratory Compliance* (2024) (India).
[20] BPR&D, *Annual Report: Cyber Training Modules for Indian Police* (2024) (India).
[21] NCRB, *Crime in India 2025: Cybercrime Analysis* (2025) (India).
[22] NFSU, *Techniques for Public Deepfake Detection: ELA & Hash Validation* (2025) (India).

tracing in hacking probes. Public portals like cybercrime.gov.in encourage timely reporting with screenshots intact, enabling Cellebrite extractions before auto-deletes. In financial frauds under Section 84 of the Bharatiya Nyaya Sanhita, 2023 hygiene-aware users retain UPI trails, boosting conviction rates from 20% to 45% in trained demographics. Mass media drives like QuickHeal's 2026 Awareness Month Sound this, teaching EXIF preservation for photos crucial in murder reconstructions via geolocation. Despite campaigns, awareness gaps persist, especially rural India where 80% lack basic hygiene, per MeitY surveys. Unsecured Wi-Fi Generates man-in-middle attacks fabricating evidence, dismissed in courts for absent non-repudiation. Elderly victims fall prey to sextortion, wiping devices post-trauma and nullifying voice biometrics. Low literacy equates to Careless panchnamas without hashes, violating BNSS audio-video mandates and inviting To be declared innocent. Urban-rural divides mean Tier-2 cities report 60% more viable digital proofs due to NGO workshops.[23]

Educational shortcomings compound issues: only 30% schools cover phishing simulations, leaving youth vulnerable to manipulative conditioning apps whose logs vanish without hygiene. Corporate tie-ups falter without Easily expandable LMS like NeGD's, reaching 10 million versus needed 1.4 billion.[24] Judicial notices urge hygiene in witness prep, yet untrained public supplies corrupted USBs rejected under ISO 17025. Multilingual campaigns in Hindi/Tamil via Akashvani lag behind TikTok threats, Growth Interruption evidence pipelines. Remedies demand Promote: Game-based apps like CyberShikshak Copy trials, showing hygiene's evidentiary weight—original logs sway beyond-doubt burdens.[25] Mandatory Aadhaar-linked hygiene modules at PMJDY onboarding preserve transaction metadata for laundering probes. Police-community programs train 50 lakh households yearly on Faraday bags for device seizures, curbing post-arrest wipes. 2026 budgets target 1,000 Cyber Hygiene Hubs mirroring Common Service Centres.

IX. CONCLUSION

Electronic evidence has fundamentally reshaped criminal trials in India, evolving from a New support Innovative add-on to an indispensable pillar of justice delivery in a digital History. The transition, catalyzed by the Information Technology Act, 2000, and cemented through the Bharatiya Sakshya Adhiniyam (BSA), 2023, alongside BNSS and BNS, positions digital records— Extended over CCTV footage, CDRs, social media logs, and blockchain trails—as primary proof under Section 63 BSA. This shift addresses Supported by evidence voids in traditional testimony-prone systems, offering objective, Time-stamped reconstructions that fortify prosecutions in cybercrimes, terrorism, and economic offenses, where NCRB data reflects over 1.8 lakh cases in 2025 alone. By mandating audio-video seizures and e-Sakshya tamper-proofing, these reforms ensure chain-of-custody integrity, Slice quickly Making up a false story risks and aligning with Article 21's fair trial Order. Landmark judicial precedents like Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar (2020) have Improved admissibility thresholds, emphasizing Section 65B certificates while carving exceptions for live device outputs, thereby balancing technological Liquid with procedural promises. In practice, electronic evidence terminate Excuses — think Nirbhaya's bus footage or Parliament attack CDRs—elevating conviction rates by 30-40% in tech-reliant matters. Forensic technologies, from Cellebrite extractions to AI stylometry, amplify reliability, yet characteristics like volatility and voluminousness demand ISO 17025-compliant labs, now expanded to 50+ CFSLs nationwide.

Challenges persist, underscoring the need for Comprehensive strengthening. Technical expertise Shortage among law enforcement—impacting 90% of rural stations—lead to mishandled seizures, overwriting critical RAM or metadata, resulting in judicial exclusions. Standardization via BNSS timelines and Mobile Forensic Vans mitigates this, but training 20 lakh personnel through CyTrain-NCRB remains Just begun. Public awareness gaps Worsen weaknesses: poor cyber hygiene erases original logs,

[23] NGO Alliance for Digital Literacy, *Impact Report: Cyber Hygiene Workshops in Tier-2 Cities* (2026) (India).

[24] NeGD, *Scaling Digital Forensics Education via LMS Platforms* (2026) (India).

[25] CyberShikshak Found., *Gamification of Cyber Hygiene: Pilot Program Results* (2026) (India).

with 70% victims unaware of hash preservation, Problems effects POCSO or fraud probes. Initiatives like ISEA's 2026 Cyber Hygiene Calendar aim to empower citizens as evidence custodians, Foster while keeping Complete digital trails from source to courtroom. Procedural upgradations signal promise: e-Courts Phase III integrates VR reconstructions and remote forensics, curbing adjournments in 4.4 crore pending cases. Yet, infrastructure Obstacles — encryption Impediments, deepfake surges, and lab backlogs—necessitate public-private Synergy and quantum-resistant protocols. International Mutual Legal Assistance Treaties streamline cloud data, vital for dark web extraditions, while NFSU's AI pilots predict crime patterns from bulk analytics.

REFERENCE

[1] Joshi, Nayan. Electronic Evidence (With Cross References to New Criminal Laws). 2nd Edition, Eastern Book Company, 2025.
[2] Jain, N. "Admissibility of E-evidence in India: An Overview." SSRN Electronic Journal, 2021.
[3] Mamatkulova, Khosiyat. "Admissibility Of Electronic Evidence In Criminal Proceedings." American Journal, 2025.
[4] Nappinai, N.S. "Electronic Evidence." Jharkhand Judicial Academy, 2025.
[5] "Admissibility Of Electronic Evidence In Indian Courts." IJCRT, 2024.
[6] "Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings as per Bhartiya Sakshya Adhiniyam, 2023." Shodh Sagar, 2024.
[7] "Electronic Evidence and Judicial Consideration in India." IALS Blog, Institute of Advanced Legal Studies.
[8] "Electronic Evidence PSJ." Tamil Nadu State Judicial Academy.
[9] "Electronic evidence in criminal proceedings." PIB India, 2025.
[10] "Supreme Court on the admissibility of electronic evidence under Section 65B." Cyril Amarchand Mangaldas Blog, 2022.
[11] "Admissibility of Electronic Evidence." National Judicial Academy, 2019.
[12] "Electronic Evidence: Old Statute vs New Proposed Bill, India." Law Journals, 2024.
[13] "Admissibility of electronic evidence: an Indian perspective." MedCrave Online, 2017.
[14] "Appreciation of Electronic Evidence by the Courts." National Judicial Academy, 2016.
[15] "Landmark Judgment on Admissibility of Electronic Evidence." TaxTMI, 2024.
[16] "SOP of Audio-Video Recording for Scene of Crime." BPRD.
[17] "Admissibility of Digital Evidence under Bharatiya Sakshya Adhiniyam." SSRN, 2024.
[18] "Electronic Evidence: Navigating Legal Shifts Under BSA 2023." SCC Online, 2024.
[19] "Cyber Crimes And Digital Evidence In India's New Criminal Laws." IJLLR, 2024.
[20] "Role of Digital Forensics and Criminal Investigation in India." IJRPR.
[21] "Revisiting the Admissibility of Scientific Evidence in Criminal Trials." IJRPR, 2025.