STRENGTHENING CYBERCRIME PROSECUTION THROUGH FORENSIC EVIDENCE: A STUDY ON HARASSMENT AND DECEPTION

Sanjana Ranjan, CHRIST (Deemed to be University), Delhi NCR, Contact

ABSTRACT

Cybercrime has emerged as a pressing challenge in the digital era, with online harassment and digital deception posing significant threats to personal security, dignity, and public trust in technology. The increasing sophistication of offenders, who exploit encrypted platforms, deepfake technology, and anonymization tools, has made the prosecution of such crimes heavily dependent on the credibility of forensic evidence. This research critically examines the role of cyber forensics in strengthening the prosecution of harassment and deception cases, with particular emphasis on the evolving legal framework under the Bharatiya Nagarik Suraksha Sanhita, 2023, and its provisions on electronic evidence.

The study explores the pivotal function of digital forensics in addressing core evidentiary challenges such as maintaining the chain of custody, safeguarding metadata integrity, and ensuring admissibility of evidence before courts. It further highlights emerging tools, including AI-based forensic analytics for detecting deepfakes and abusive content, and blockchain-enabled systems for preserving the authenticity of digital records. These technologies, while promising, demand significant infrastructural investments, enhanced forensic capacity in laboratories, and systematic training for investigators and judicial officers to translate scientific evidence into successful convictions.

A critical dimension of this research focuses on bridging the gap between law and technology by aligning forensic innovations with judicial processes, thereby addressing evidentiary vulnerabilities that often lead to acquittals in cybercrime trials. Comparative insights are drawn from international practices, demonstrating the need for India to build resilient forensic systems capable of withstanding global standards of scrutiny. By fostering an integrated, technologically advanced, and legally robust approach, this study underscores that forensic science is not merely supportive but essential to delivering justice in cases of online harassment and deception, ultimately strengthening confidence in the digital justice system.

Keywords: AI-based forensics, Bharatiya Nagarik Suraksha Sanhita 2023, blockchain authentication, cybercrime, cybercrime prosecution, digital deception, forensic evidence, metadata integrity, online harassment.

I. Introduction:

Navigating the Digital Evidentiary Crisis

The rapid and comprehensive digitalisation of society has yielded enormous socioeconomic advantages, yet simultaneously, it has created a volatile new frontier for criminal activity. Among the most pervasive and damaging manifestations of this evolution are crimes of online harassment and digital deception, offences that strike critically at personal dignity, financial security, and fundamental public trust in electronic communication. These crimes, which range from sophisticated financial fraud and identity theft to the insidious creation and spread of non-consensual sexual imagery utilizing advanced deepfake technology, present the criminal justice system with an acute, unprecedented evidentiary crisis.[1] The core challenge lies in the nature of digital evidence itself: it is inherently volatile, easily manipulated, often ephemeral, and frequently traverses international borders, allowing perpetrators to operate with relative impunity.[2]

The complexity of these digital trails—often stored on decentralized cloud servers or encrypted communications—renders traditional investigative methods largely ineffective.[3] Adding to this complexity is the existential threat posed by generative Artificial Intelligence (AI) and deepfakes. These AI-generated videos, images, and audio simulate reality so accurately that they threaten the foundation of all visual and auditory evidence, exploiting fundamental

cognitive biases such as the "seeing is believing" heuristic.[4] Alarmingly, pornographic material constitutes approximately ninety-eight percent of deepfakes, directly impacting cases of cyber harassment and abuse and making the authentication of incriminating content a formidable task for prosecutors and courts alike.[5]

Historically, the Indian criminal justice system struggled to cope with this burgeoning digital reality. The colonial-era Indian Evidence Act (IEA) of 1872 proved largely obsolete in the digital communication era, resulting in significant judicial uncertainty and inconsistency, which damaged the efficiency and credibility of the justice delivery system.[6] This failure was most pronounced in the contested area of electronic evidence admissibility, where a lack of

clarity regarding whether a digital record constituted primary or secondary evidence, and the requisite certification required, led to a cascading effect of confusion, multiplied disputes, and hampered prosecutions.[7] Indeed, research under the old regime indicated major procedural gaps, with the adequacy of evidence collection procedures found lacking in nearly half of the analyzed cybercrime cases, often complicating foundational Chain of Custody (CoC) claims.[8]

In response to this systemic vulnerability and the perceived need for comprehensive reform, the Government of India introduced a transformative legislative package: the Bharatiya Sakshya Adhiniyam (BSA), 2023, and the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023. These new codes mark a decisive attempt to integrate technology into the very mechanisms of criminal procedure and evidence law. The BSA, replacing the IEA, broadens the definition of 'Documents' and 'Evidence' to explicitly include electronic and digital records such as server logs, messages, locational evidence, and documents stored on various digital devices, providing the necessary legal foundation for tracing cybercriminals.[9]

Furthermore, the BSA offers a crucial mechanism to streamline admissibility: Section 57 now stipulates that an electronic or digital record produced from **proper custody** shall be considered **primary evidence** unless its genuineness is actively disputed.[10] This provision places a clear onus on law enforcement to uphold meticulous forensic protocols. Complementing this, the BNSS modernizes procedural law by mandating the use of electronic means, notably requiring that the process of search and seizure, including the preparation of the list of seized items, **shall be recorded through audio-video electronic means**, providing an indispensable layer of procedural transparency to support the initial establishment of the Chain of Custody.[11]

However, the efficacy of this modernized framework hinges entirely on operational capacity and technical adherence. This paper posits the central thesis that the successful implementation and resultant strengthening of cybercrime prosecution under the BSA and BNSS require a coordinated and simultaneous commitment to three pillars: **infrastructural capacity building** across forensic science laboratories (FSLs), the universal **adoption of rigorous forensic technical standards** that enforce metadata integrity, and **judicial and investigative literacy** in complex digital authentication methods. This commitment is particularly vital given the BSA's replacement of the frequently litigated Section 65B with Section 63, which mandates the technical inclusion of the **HASH value** of the electronic record in the admissibility

certificate—a requirement that elevates cryptographic verification from a forensic best practice to a legal necessity.[12]

This comprehensive analysis proceeds in five main parts. Section II provides a detailed examination of the new legal architecture (BSA and BNSS). Section III delves into the foundational requirements of forensic integrity, focusing on the historical challenges of the Chain of Custody and the necessity of cryptographic hashing. Section IV assesses the contemporary authentication crisis, analyzing the deepfake dilemma and the judicial challenge posed by Artificial Intelligence-generated evidence. Section V presents a comparative study contrasting the Indian framework with established legal standards in the United States and the European Union. Finally, Section VI concludes with prescriptive and actionable recommendations designed to bridge the gap between ambitious legislative intent and the realities of forensic implementation, ensuring that technical evidence serves as the bedrock for successful prosecution.

II. The New Legal Architecture: Harmonising Law with Digital Reality

The **Bharatiya Sakshya Adhiniyam (BSA), 2023**, represents a critical legislative intervention designed to supplant the outdated Indian Evidence Act (IEA) of 1872.[13] This reform is an explicit acknowledgment that traditional principles of documentary proof are largely obsolete in the modern era of electronic communication and volatile digital records.[14] The new framework attempts to provide a clear and conducive mechanism for handling electronic evidence in judicial proceedings, directly addressing the legal uncertainty that previously plagued cybercrime trials.[15]

2.1. Modernizing the Definitions of Evidence

A foundational step taken by the BSA is the explicit expansion of core legal definitions to encompass the digital ecosystem. The definition of "Documents," established in **Section 2(1)(d)**, now unambiguously includes electronic and digital records, electronic statements, and digital records produced for the court's inspection.[16] This expansive definition covers sources critical for cybercrime investigations, such as server logs, documents on computers, messages on smartphones, locational evidence, and voicemails stored on digital devices.[17] Furthermore, the definition of "Evidence" (Section 2(1)(e)) has been broadened to permit the appearance of

witnesses, accused, experts, and victims through electronic means, thereby streamlining the trial process and preventing logistical delays.[18]

2.2. The Primary Evidence Rule and Proper Custody

The BSA introduces a mechanism to streamline the admission of authenticated digital evidence. **Section 57** of the BSA stipulates that an electronic or digital record produced from **proper custody** is considered **primary evidence** unless its genuineness is disputed.[19] This provision is revolutionary: it elevates a properly forensically acquired digital record—such as a bit-by-bit image—to the standing of an original document. The implication is that if law enforcement meticulously demonstrates that the digital record was seized and preserved following strict forensic protocols (i.e., maintained in "proper custody"), the evidentiary presumption shifts, placing the burden on the defense to prove the record's lack of genuineness.[20] This clarity is essential for prosecuting cases of digital deception and harassment where authenticity is paramount.

2.3. The Admissibility Mandate: BSA Section 63 (Replacing 65B)

The most litigated and arguably the most ambiguous provision under the old IEA was **Section 65B**, which required a specific certificate for the admissibility of electronic evidence. This rule led to widespread judicial confusion and inconsistency, contributing significantly to delays and high attrition rates in cybercrime cases.[21]

The BSA addresses this uncertainty by replacing Section 65B with **Section 63**.[22] Section 63 governs the admissibility of "Computer Output" (electronic records printed or stored in digital media) without requiring the original device, provided specific procedural conditions are satisfied, such as regular use of the device and ensuring that any malfunction did not materially affect the record's accuracy.[23]

A. The Mandate for Hash Values: Technical Integrity as Law

Crucially, **Section 63(4)** outlines stringent certification requirements. The necessary certificate must identify the electronic record, describe its production method, provide details of the devices involved, and be signed by the person in charge of the computer and an expert.[24] Beyond these procedural demands, the new **Section 63(4)(c)** imposes a critical technical requirement previously absent in law: the certificate must include metadata and the **HASH**

value of the electronic/digital record, obtained through a specified cryptographic algorithm (such as SHA1, SHA256, or MD5).[25]

This mandate legally enforces the use of cryptographic hashing, a core principle of digital forensics. By mandating that law enforcement document this unique digital fingerprint at the point of collection, the BSA legally enforces the need for proof of **metadata integrity** and guarantees against subsequent data tampering. This rigorous technical standard directly supports the prosecution by ensuring the evidence presented is the exact, unaltered replica of the data seized, moving the standard of admissibility from a mere procedural formality to a scientifically validated process.[26]

2.4. Procedural Safeguards in the Bharatiya Nagarik Suraksha Sanhita (BNSS)

The **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023**, complements the BSA by fundamentally integrating technology into criminal procedure, thereby enhancing transparency and aiding in the initial establishment of the Chain of Custody (CoC). **Section 105** of the BNSS specifically provides that the process of conducting search and seizure—including the preparation of the list of seized items and the signing by witnesses—**shall be recorded through audio-video electronic means**, preferably using a cell phone.[27] This recording must be forwarded to the relevant Magistrate without delay.[28]

This provision directly assists the prosecution by providing contemporaneous documentary proof of the circumstances of the seizure, clearly identifying who collected the evidence, which is an indispensable element of the CoC.[29] The effective implementation of these procedural requirements, coupled with the technical integrity standards laid down in the BSA, is instrumental in creating a modernized, structured legal response to the mounting challenges of cybercrime.[30]

III. Foundational Challenges: Forensic Integrity and the Chain of Custody

The evidentiary framework established by the BSA, while technologically forward-looking, is only as strong as the physical and procedural infrastructure supporting it. The ability to secure convictions in cases of cyber harassment and deception rests entirely upon the capability of forensic agencies and law enforcement to meet the highest standards of integrity, traceability, and authentication.[31] The meticulous preservation of the digital crime scene is the bedrock upon

which the entire legal process is built.

3.1. The Criticality of Chain of Custody (CoC)

Chain of Custody refers to the meticulous documentation that tracks the sequence of control, transfer, analysis, and disposition of digital evidence from the precise moment of its seizure until it is presented in court.[32] For digital evidence, which is uniquely susceptible to alteration—often requiring remote collection or subject to metadata modification—the integrity of this chain is paramount. The essential requirements for a viable CoC process are fourfold: **Integrity** (irrefutable proof the evidence has not been altered or corrupted), **Traceability** (the ability to track the evidence from collection to destruction), **Authentication** (irrefutable proof of identity for all entities interacting with the evidence), and **Verifiability** (the entire process must be independently auditable).[33] This documentation must meticulously record the date of receipt, the person and method of data reception (including whether the data was received via email and who was copied), confirmation of whether files are original forensic extractions or processed data, and the specific path to access the data in the system.[34]

3.2. Historical Procedural Gaps in Indian Case Law

Judicial analysis under the old IEA regime consistently highlighted significant procedural gaps in maintaining the CoC for digital evidence. Research indicates that disputes over evidence admissibility were predominantly centered on challenges to access to data, featuring in **sixty-two percent** of analyzed cybercrime cases, while the adequacy of evidence collection procedures was found lacking in **forty-seven percent** of circumstances.[35] This historical procedural failure is the primary reason the BSA was compelled to introduce the stringent hash value mandate in Section 63. While the BNSS Section 105 mandates the audio-video recording of the *physical* seizure, documenting *who* collected the evidence, this does not, by itself, guarantee the *technical* integrity (the hash value) required by the BSA.[36] This operational divide—between documenting physical custody and guaranteeing technical integrity—is where most prosecutions fail. The subsequent failure to demonstrate **"proper custody"** (BSA Section 57) or produce the Section 63 certificate with the correct hash value often leads to the exclusion of critical evidence, fatally undermining the prosecution's case and resulting in significant administrative and logistical burdens for law enforcement agencies.[37]

3.3. Future-Proofing CoC: The Blockchain Paradigm

To overcome the systemic procedural challenges and inherent vulnerabilities of traditional, paper-based CoC documentation, advanced technological solutions are emerging globally. **Blockchain-based Chain of Custody (B-CoC)** systems offer a robust mechanism to guarantee data immutability, cryptographic security, and enhanced reliability for forensic evidence management.[38]

These B-CoC systems operate by utilizing distributed ledger technology, which involves creating an immutable Evidence Log on a permissioned peer-to-peer network composed of authorized forensic entities (validator nodes).[39] Every changeover of the evidence, or even simple access to it, must be executed by an authorized entity and is recorded as a cryptographically secured transaction on the ledger.[40] This approach guarantees a tamper-proof, auditable record that aligns perfectly with the BSA's demand for both a verifiable custody chain and the technical integrity enforced by the hash value mandate.[41] By employing B-CoC, law enforcement can provide mathematical proof of integrity, proactively countering historical defense challenges concerning data custody and enhancing the privacy, security, and dependability of forensic evidence handling.[42]

3.4. The Infrastructure and Capacity Chasm

The legislative ambition embedded in the BSA, particularly the mandate for compulsory forensic examination in all cases where the offense attracts punishment of seven or more years of imprisonment, is severely undermined by critical limitations in operational capacity.[43] This increased demand places enormous pressure on the already constrained infrastructure of Forensic Science Laboratories (FSLs), demanding significant financial investments in video conferencing technology and cyber security measures.[44]

A review of forensic practices in India highlights significant disparities in resources and infrastructure across states, with many district-level or rural facilities lacking basic equipment, updated forensic tools, and necessary software.[45] This deficit is compounded by high vacancy rates among scientific officers, bureaucratic delays, budget underutilization, and substantial case backlogs.[46] These systemic operational deficiencies lead to critical delays in generating forensic reports, compromising the timely use of digital evidence, and eroding the credibility of the entire justice system. The failure to address these infrastructural and logistical burdens

fundamentally threatens the effective implementation of the BSA's rigorous forensic standards, as investigators struggle to meet the mandatory deadlines and technical requirements of the hash value certificate.[47]

IV. The Crisis of Authentication: Deepfakes in Harassment and Deception

The most pressing and technologically sophisticated challenge currently facing digital evidence authentication in cases involving online harassment and deception is the proliferation of deepfakes—AI-generated media (videos, images, and audio) that realistically simulate or fabricate content.[48] This generative technology is rapidly advancing, moving from requiring powerful proprietary tools to being executable with free mobile applications and limited digital skills, making accurate detection increasingly difficult, especially for complex audio deepfakes.[49]

4.1. The Malicious Application of Generative AI and Evidentiary Failure

The malicious use of deepfakes poses a profound legal threat by enabling the swift spread of false narratives, the creation of highly realistic non-consensual imagery, and a general erosion of trust in all digital media.[50] Alarmingly, pornographic material accounts for approximately **ninety-eight percent** of all deepfakes, directly intersecting with severe cyber harassment and sexual abuse cases, including the manipulation of images of young girls or the generation of synthetic imagery with a "high level" of realism resembling real children and minors.[51]

Deepfakes create unique evidentiary problems that the BSA's procedural safeguards cannot fully resolve. While the **BSA Section 63** certificate verifies the device's custody and the file's integrity on that device (via the hash value), it cannot certify the *content's* origin or genuineness if the malicious fabrication occurred *before* the file was stored.[52] The core dilemma is that the mere act of possession or transmission of the deepfake becomes the prosecutorial focus, but the authenticity of the alleged *event* depicted is fundamentally called into question. This lack of certainty regarding the factual basis of the digital record damages witness credibility, increases litigation costs, and creates a wider erosion of trust in digital evidence generally, necessitating profound adjustments to discovery rules and procedural fairness.[53]

4.2. Forensic Countermeasures and the "Black Box" Problem

Forensic science has attempted to respond to this crisis by leveraging AI for deepfake detection.

However, these detection systems introduce their own set of legal complications. Many sophisticated AI models used in forensic analysis are inherently "black box" systems, meaning their decision-making processes lack the requisite transparency for judicial scrutiny.[54] When a forensic expert relies on such an AI tool to testify that content is authentic or fabricated, the defense often lacks the necessary technical capacity to adequately scrutinize the reliability of that AI model, raising the fundamental legal challenge in court: "Why is this image classified as fake?"[55]

This lack of transparency concerning AI models raises serious constitutional concerns regarding a defendant's right to confrontation in court, as limitations could negatively impact a defendant's capacity to test the reliability of an AI model.[56] For digital evidence proffered by AI algorithms to be admissible, the process and logic of that AI must be transparently scrutable and verifiable. This necessitates the immediate adoption of **Explainable AI (XAI)** principles in the forensic domain, ensuring that the methodologies used can be tested and verified by opposing parties and subjected to objective, scientific scrutiny.[57]

4.3. Judicial Gatekeeping and Scrutiny of AI Evidence

In jurisdictions such as the United States, the rising sophistication of deepfakes has demonstrated that existing authentication standards (like Federal Rule of Evidence 901) are often insufficient to detect complex falsifications.[58] This compels judges to expand their traditional role as gatekeepers, ensuring AI-generated or manipulated evidence is subjected to rigorous scrutiny before admission to prevent the exploitation of cognitive biases among jurors.[59] For example, in the US, Rule 702 (Expert Testimony) standards, particularly the **Daubert standard**, are applied to assess the scientific validity of AI-derived conclusions, ensuring that machine output does not evade reliability requirements.[60]

In the Indian context, the provision for consulting an Examiner of Electronic Evidence (**BSA Section 39**) must be critically refined to demand XAI transparency from experts analyzing deepfakes.[61] Without clear statutory guidance on the admissibility and scientific reliability of AI-based detection, the judiciary must establish a rigorous standard, akin to the US *Daubert* standard, to assess the scientific validity of the forensic methodology used, rather than relying solely on the procedural certification under Section 63. This necessary judicial intervention ensures that the scientific validity of novel AI evidence is vetted prior to presentation to the court, upholding the fundamental right to a fair trial.

V. Comparative Jurisprudence and the Global Dimension

Cybercrime is fundamentally borderless. The perpetrators of harassment and deception often operate across multiple jurisdictions, meaning the successful prosecution of these transnational offenses requires India not only to strengthen its domestic evidentiary standards (as achieved via the BSA) but also to align its protocols with international best practices and participate robustly in global cooperation mechanisms.

5.1. United States: The Reliability-Focused Framework

The United States legal system, governed primarily by the Federal Rules of Evidence (FRE), mandates proof of reliability and a clear Chain of Custody for digital evidence.[62] FRE 902 simplifies the admission of routine electronic records, allowing them to be **self- authenticating** if accompanied by proper certification, a rule introduced specifically to streamline the admission of electronically stored business records.[63]

The critical difference between the US system and the Indian BSA lies in the treatment of expert testimony regarding novel scientific evidence. The US system employs the **Daubert standard** (or the *Frye* standard, depending on the jurisdiction) under FRE 702 to assess the reliability and scientific validity of expert opinions.[64] For forensic experts utilizing AI for deepfake detection, the *Daubert* standard requires them to satisfy rigorous criteria regarding the testability of the method, the known or potential error rate, peer review status, and general acceptance within the relevant scientific community.[65] This reliability-focused system provides courts with significant flexibility to scrutinize novel scientific evidence, allowing for rigorous challenges to the underlying AI methodology itself—a crucial safeguard against the "black box" problem that is often raised when challenging AI-generated evidence. This flexibility complements the procedural certainty offered by India's BSA Section 63 certificate but focuses more acutely on the scientific *process* used to reach the forensic conclusion.

5.2. European Union and the Dignity Standard

In Europe, the legal framework for cyber harassment is often built upon the principle of human autonomy and dignity. The primary cause of action for cyber-related violations of privacy is often the **Misuse of Private Information**, a tort developed to incorporate the rights guaranteed by Article 8 (Right to respect for private and family life) of the European Convention on Human

Rights (ECHR).[66] European jurisprudence emphasizes a two-stage process: the claimant must first establish a reasonable expectation of privacy in the information, and then the court balances that right against Article 10 (Freedom of Expression).[67]

Regarding evidence admissibility, specific European statutory bases are scarce, leading to greater reliance on the jurisprudence of the European Court of Human Rights (ECtHR).[68] The overall focus is on the relevance of the data and the reliability of the system used to generate or collect it, while also ensuring that expert evidence respects stringent privacy rights, such as those governed by the General Data Protection Regulation (GDPR). The EU's legal trajectory highlights the imperative for common admissibility criteria for digital and forensic evidence, reflecting a growing need for specific rules at the European level.[69]

5.3. Cross-Border Data Access and Jurisdiction

The greatest operational impediment to prosecuting transnational harassment and deception is the challenge of obtaining digital evidence held by Online Service Providers (OSPs) in foreign jurisdictions, particularly those based in the United States. International cooperation is strained by conflicting legal mandates, such as the EU General Data Protection Regulation (GDPR) and the US Stored Communications Act (SCA), which can legally forbid US-based OSPs from providing data access unless a specific executive agreement exists.[70] This jurisdictional friction undermines the ability of nations to trace deception and harassment across digital borders.

Global efforts, including the EU–US Mutual Legal Assistance (MLA) Agreement and the proposed United Nations Convention on countering ICT crimes, underscore the global necessity for harmonizing evidence exchange procedures.[71] The US Department of Justice has stressed the need for improved funding, communication, and standardized protocols to fight crimes involving digital assets and money laundering, acknowledging the reluctance or sheer inability of some foreign jurisdictions to tackle complex digital investigations independently.[72] Furthermore, accession to international treaties like the **Budapest Convention on Cybercrime** provides a framework for collecting digital evidence in emergencies and directly from service providers, offering extra-territorial powers that are crucial for modern cybercrime investigation.[73] Best practices adopted internationally for documenting online harassment evidence emphasize victim-led collection using standardized protocols, including recording threats, screen-grabbing evidence, identifying perpetrators using geolocation information and

forensic techniques, and meticulous documentation of usernames, ensuring that foundational data aligns with evidentiary standards like the BSA's.[74]

VI. Strengthening Prosecution: Strategic Recommendations and Future-Proofing

The BSA and BNSS provide the necessary legislative foundation for a modernized digital justice system. However, the successful implementation of this vision against increasingly sophisticated cybercrime requires immediate and targeted strategic interventions across infrastructure, judicial procedure, and international cooperation, transforming legislative intent into operational reality.

6.1. Judicial and Law Enforcement Capacity Building

A massive, sustained investment in capacity building is mandatory to overcome the current chasm between legislative intent and operational reality. Courts, prisons, and police units require urgent infrastructural enhancements, including secure authentication methods and technology upgrades, along with significant financial investments in video conferencing technology and robust cyber security measures, to support the digital mandates of the new codes.[75]

Law enforcement agencies, in particular, need vastly improved digital forensics capabilities and adherence to stricter, standardized protocols for evidence gathering.[76] Judicial officers must undergo intensive, specialized training focused on the rigorous technical requirements of **BSA Section 63**. This training must move beyond a general appreciation of digital data to a deep understanding of complex concepts like metadata, cryptographic hash values (SHA1, SHA256, MD5), and forensic best practices. Recognizing that the compulsory forensic examination mandated for serious offenses attracting punishment of seven or more years directly strains already limited **Forensic Science Laboratory (FSL)** capacity, immediate strategies must be deployed to fill high scientific officer vacancy rates, improve equipment access, and systematically reduce substantial case backlogs to ensure timely justice.[77] The failure to address the infrastructural deficiencies, including the lack of basic equipment in rural facilities, will fundamentally compromise the implementation of the BSA's rigorous standards.[78]

6.2. Mandating and Integrating Future-Proofed CoC

To address the historical failure rate in Chain of Custody (CoC) documentation, which has

previously compromised the majority of cybercrime prosecutions (with data access disputed in 62% of analyzed cases), the government must move decisively toward digital, immutable systems.[79] A strategic recommendation involves the governmental piloting and ultimate mandatory adoption of permissioned **Blockchain-Based Chain of Custody (B-CoC) systems**.[80]

These B-CoC systems utilize cryptographically secured ledgers to provide verifiable evidence logs from the point of collection (which is recorded by **BNSS Section 105** audio-video means) through to the trial.[81] By automating the recording of access, transfer, and verification—crucially including the required hash values—such a system proactively enforces the technical integrity required by **BSA Section 63**, drastically reducing the vulnerability of evidence to tampering claims.[82] This approach strengthens the prosecution's case under the BSA's 'proper custody' rule by providing mathematical proof of integrity, enhancing the security and dependability of forensic evidence handling.[83]

6.3. Legislative and Judicial Clarity for AI Evidence

Given the existential threat posed by deepfakes to the integrity of evidence (especially where 98% of deepfakes are pornographic), the legal system must rapidly establish clear standards for evaluating expert evidence derived from forensic AI tools.[84] This paper recommends that the judiciary adopt mandatory guidelines—perhaps modeled after the stringent US **Daubert criteria**—that demand forensic experts adhere to **Explainable AI (XAI)** principles when presenting findings based on AI detection models.[85]

This adherence ensures that the methodology underlying the expert's conclusion can be scrutinized for its testability, error rate, and acceptance within the scientific community, thereby satisfying the defendant's constitutional right to confrontation (a vital consideration when an AI model proffers inculpatory evidence).[86] This scrutiny prevents experts from evading reliability requirements and ensures that the role of the Examiner of Electronic Evidence (**BSA Section 39**) is informed by transparency.[87] Furthermore, specific regulatory frameworks must be established to align with international precedents (like Interpol's recommendations) that recognize high-realism synthetic content, particularly sexually abusive material, as unlawful, providing a firm legal footing for its vigorous prosecution.[88]

6.4. Accelerating International Cooperation and Jurisdiction

The successful prosecution of transnational cyber harassment and deception mandates accelerated accession to and active implementation of international treaties. The **Budapest Convention on Cybercrime** offers a vital framework for emergency collection of digital evidence and direct cooperation with service providers, granting extra-territorial powers essential for tracking digital assets.[89] Harmonization of evidence exchange procedures—the key to overcoming jurisdictional hurdles and data location conflicts (such as between the EU GDPR and the US SCA)—must be prioritized through frameworks like the UN Convention on countering ICT crimes and the EU–US MLA Agreement.[90] The US Department of Justice has stressed the need for improved funding, communication, and standardized protocols to fight crimes involving digital assets and money laundering, highlighting the global deficiency in tackling complex digital investigations independently.[91] Additionally, the adoption of international best practices for victim-led evidence collection—including standardized protocols for recording threats, using geolocation information, and meticulous documentation of usernames—ensures that foundational data aligns immediately with the high evidentiary standards required by the BSA.[92]

VII. Conclusion

The legislative reforms embodied by the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, and the **Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023**, signify a pivotal and necessary step toward modernizing India's criminal justice response to the acute challenges of cybercrime. By mandating the technical verification of digital evidence, specifically through the inclusion of cryptographic hash values in the admissibility certificate (**BSA Section 63**), and by elevating properly collected digital records to the status of primary evidence (**BSA Section 57**), the new framework correctly identifies **forensic integrity** as the mandatory technical prerequisite for the admissibility and reliability of digital evidence in court.[93] This shift proactively addresses the historical failure points in Indian case law, where chain of custody and data access were the predominant grounds for disputing electronic evidence.[94]

However, the efficacy of this ambitious legal structure is currently undermined by profound operational realities. The legislative intent to enforce rigorous forensic standards is severely hampered by systemic infrastructural deficiencies, most notably chronic **Forensic Science Laboratory (FSL)** backlogs, high vacancy rates for scientific officers, and a pervasive lack of

up-to-date equipment in many regional facilities.[95] This capacity gap is compounded by the mandate for compulsory forensic examination in all cases involving severe punishment, placing untenable pressure on the already strained forensic ecosystem and potentially compromising the timely administration of justice.[96]

Furthermore, the technological advancement of deepfakes introduces a crisis of authentication that goes beyond procedural compliance. These AI-generated fabrications threaten to render traditional authentication methods obsolete and demand that courts adopt a far more rigorous, scientific scrutiny of AI-based evidence. The current legal framework must be complemented by judicial guidelines, perhaps modeled after the US *Daubert* standard, that specifically demand **Explainable AI (XAI)** transparency from expert witnesses, thereby safeguarding the defendant's constitutional right to confrontation against the opacity of "black box" detection systems.[97]

Effective prosecution of cyber harassment and deception is fundamentally dependent on transforming legislative mandates into operational excellence. This requires a concerted national investment in resource injection to fully staff and equip FSLs; the institutional adoption of future-proofed Chain of Custody (CoC) technologies, such as **Blockchain-Based CoC (B-CoC)**, to provide immutable, mathematical proof of data integrity; the establishment of clear XAI-based judicial standards; and aggressive participation in harmonized international cooperation frameworks, like the **Budapest Convention**, to overcome cross-border data access hurdles.[98] By fostering an integrated, technologically advanced, and legally robust approach, India can ensure that forensic science moves beyond a merely supportive role to become the indispensable cornerstone for delivering timely and credible justice in the digital age, thereby strengthening confidence in the entire criminal justice system and upholding the rule of law against sophisticated digital perpetrators.[99]

Endnotes:

1 Report on Digital Evidence Admissibility in Indian Courts, Vintage Legal (Oct. 2024)

2 Journal Article on BSA and BNSS, Law Journals (May 2025)

3 Id.

4 European Parliament Briefing, Deepfakes and the Challenge to Regulation (Feb. 2025); Rebecca A. Delfino, Deepfakes on Trial, 74 Hastings L.J. 293 (2023)

5 European Parliament Briefing, Deepfakes and the Challenge to Regulation (Feb. 2025)

6 Journal Article on BSA, IJFMR (May 2024)

7 Report on Digital Evidence Admissibility in Indian Courts, Vintage Legal (Oct. 2024); Hindustan Times, Electronic Evidence on Trial (Oct. 2024)

8 Report on Digital Evidence Admissibility in Indian Courts, Vintage Legal (Oct. 2024)

9 B.P.R.D. Report: Use of Technology in Investigation, Trial and Court Proceedings

(2024); Journal Article on BSA & BNSS (May 2025)

10 B.P.R.D. Report (2024); Bharatiya Sakshya Adhiniyam, 2023, § 57

11 Search & Seizure by Electronic Means, MHA (Dec. 2024); Journal Article on BNSS (May 2025)

12 CEAC, Section 65B → Section 63 Certificate (Mar. 2024); Ksandk.com Note on BSA §63 (Feb. 2024)

13 Journal Article on BSA, IJFMR (May 2024)

14 Hindustan Times, Electronic Evidence on Trial (Oct. 2024)

15 Id.

16 B.P.R.D. Report (2024); Journal Article on BSA (May 2025)

17 B.P.R.D. Report (2024)

18 Id.

19 Bharatiya Sakshya Adhiniyam, 2023, § 57; B.P.R.D. Report (2024)

20 Journal Article on BSA, Law Journals (May 2025)

21 Report on Digital Evidence Admissibility in Indian Courts (Oct. 2024); Hindustan Times (Oct. 2024)

22 CEAC, Section 63 Certificate (Mar. 2024)

23 Ksandk.com Legal Note on BSA §63 (Feb. 2024)

24 Ksandk.com Legal Note on BSA §63 (Feb. 2024)

25 BSA Section 63(4)(c) Certificate Draft, Scribd (Aug. 2025)

26 Ksandk.com Legal Note on BSA §63 (Feb. 2024)

27 BNSS, 2023, § 105; MHA Search & Seizure Guide (Dec. 2024)

28 MHA Search & Seizure Guide (Dec. 2024)

29 Journal Article on Metadata Integrity, Law Journals (May 2025)

30 Id.

31 Journal Article on BSA, Law Journals (May 2025)

32 National Judicial Academy, Digital Forensics: Chain of Custody (2021)

33 IEEE Publication, Blockchain-Based Custody Evidence Management (2025)

34 Advisory on Chain of Custody, Pipara.com (2025)

35 Report on Digital Evidence Admissibility (Oct. 2024)

36 MHA Search & Seizure Guide (Dec. 2024)

37 Journal Article on BSA, IJFMR (May 2024)

38 Drops.dagstuhl.de, Blockchain-Based Custody Systems (2019)

39 Id.

40 Id.

41 Id.

42 IEEE Publication, Blockchain-Based Custody Evidence Management (2025)

43 B.P.R.D. Report (2024)

44 Journal Article on BSA, IJFMR (May 2024)

45 ORFOnline, India's Cyber Forensics Push (Feb. 2024)

46 Science.thewire.in, India's Forensic Science Shortcomings (June 2024)

47 Journal Article on BSA, IJFMR (May 2024)

48 European Parliament Briefing (Feb. 2025)

49 Id.

50 Id.

51 European Parliament Briefing (Feb. 2025); Interpol, Beyond Illusions (2024)

52 ISBA Journal Article on Deepfakes (Mar. 2025)

53 Id.

54 Interpol, Beyond Illusions (2024)

55 Id.

56 Journal Article on AI Forensics Limitations (2022)

57 Interpol, Beyond Illusions (2024)

58 Thomson Reuters Post (Apr. 2025)

59 Rebecca A. Delfino, Deepfakes on Trial (2023)

60 Quinn Emanuel Article (2024); Maryland Bar Association (Mar. 2025)

61 Journal Article on BSA (May 2025); Quinn Emanuel Article (2024)

62 Scoredetect.com Guide on Digital Evidence (Oct. 2024); Fed. R. Evid. 901 & 902

63 Scoredetect.com Guide (Oct. 2024)

64 Maryland Bar Association (Mar. 2025)

65 Quinn Emanuel (2024); Maryland Bar Association (2025)

66 Pinsent Masons Guide to Misuse of Private Information (Jan. 2025); ECHR Art. 8

67 Pinsent Masons Guide (Jan. 2025)

68 Cambridge Handbook of Digital Evidence (2025)

69 Id.

70 Journal Article on Cross-Border Cooperation, Oxford (Dec. 2022)

71 Id.

72 DOJ Report on Digital Asset Crime (June 2022)

73 Oxford Journal Article (Dec. 2022)

74 WAN-IFRA, Global Guidelines for Monitoring Online Violence (Oct. 2023)

75 Journal Article on BSA, IJFMR (May 2024)

76 Journal Article on BSA, IJFMR (May 2024)

77 B.P.R.D. Report (2024); Science.thewire.in (2024); IJFMR BSA Article (2024)

78 ORFOnline Report (Feb. 2024)

79 Report on Digital Evidence Admissibility (Oct. 2024)

80 Drops.dagstuhl.de Blockchain Article (2019)

81 Drops.dagstuhl.de (2019); MHA Search & Seizure (2024)

82 Drops.dagstuhl.de (2019)

83 IEEE Publication (2025)

84 European Parliament Briefing (Feb. 2025)

85 Interpol Report (2024); Maryland Bar Association (2025)

86 Journal Article on AI Forensics Limitations (2022); Interpol Report (2024)

87 Journal Article on BSA (May 2025); Quinn Emanuel Article (2024)

88 Interpol Report, Beyond Illusions (2024)

89 Oxford Journal Article (Dec. 2022)

90 Oxford Journal Article (Dec. 2022)

91 DOJ Report on Digital Asset Crime (June 2022)

92 WAN-IFRA Guidelines (Oct. 2023)

93 BSA §57; CEAC Note (Mar. 2024)

94 Report on Digital Evidence Admissibility (Oct. 2024)

95 Science.thewire.in (June 2024); ORFOnline (Feb. 2024)

96 B.P.R.D. Report (2024)

97 Interpol Report (2024); AI Forensics Limitations Article (2022)

98 Blockchain-Based Custody Systems (2019); Oxford Journal (Dec. 2022)

99 Journal Article on BSA, IJFMR (May 2024)