REFORMING CYBERCRIME INVESTIGATION IN INDIA: A FORENSIC AND LEGAL FRAMEWORK APPROACH

Jayaditya Sharma, Symbiosis Law School, Hyderabad

ABSTRACT

In this information-drenched research paper, we explore the integration of digital forensics within India's evolving legal landscape, particularly under the newly introduced Bhartiya Nyaya Sanhita and other laws, which expand the scope for the admissibility of electronic evidence. The study focuses on the probity and procedural integrity of digital evidence, identifying the strengths and gaps in India's legal infrastructure for cybercrime prosecution. With the Bhartiya Sakshya Adhiniyam (BSA) recently classifying electronic evidence as Type 1 evidence, its role in enhancing evidentiary weight in cybercrime investigations has gained renewed significance. This classification underscores the critical need for standardized forensic protocols to ensure the reliability and admissibility of digital traces, in alignment with both Indian and international legal frameworks. The paper employs a doctrinal method, analysing relevant provisions of the Information Technology Act and other statutory frameworks governing electronic evidence. It further compares India's legal mechanisms with global best practices, emphasizing how collaborations with organizations like the BSA Alliance have bolstered enforcement efforts. In light of rising cybercrime, this paper argues that India's legacy systems are struggling to adapt to the dynamic nature of digital offenses. The conclusion highlights the legislative and procedural lacunae that persist, asserting that without targeted reforms and capacity-building measures, India's justice system will remain inadequately equipped to handle the complex demands of digital-age crimes. As India stands on the brink of a full-fledged digital transformation, the legal framework must evolve in tandem to ensure that justice mechanisms remain agile, credible, and technologically robust. The paper also highlights the urgent need to institutionalize uniform standards for the collection, preservation, and presentation of electronic evidence in Indian courts, ensuring consistency and reliability across jurisdictions. This becomes imperative as cybercrimes increasingly exploit jurisdictional gaps, anonymity tools, and cross-border platforms to evade detection and prosecution within traditional investigative frameworks.

Keywords: Digital Forensics, BSA Alliance, Electronic Evidence, Cyber Crime, Bhartiya Nyaya Sanhita, Information Technology Act, Type 1 Evidence, Criminal Justice System, Cyber Law, Evidentiary Standards.

1. Introduction

Primarily, in this article, we will all be exposed to different facets of cybercrimes and their recalibration with the newly enacted (BSA) Bhartiya Sakshiya Adhiniyam 2023[1], which has brought a landmark and indeed pivotal change mandating electronic evidence to be admissible as f**irst-stage or** primary evidence status, rather than being treated as secondary proof as before. Section 61(2) of Bhartiya Sakshya Adhiniyam, 2023[2], explicitly states that "All electronic records produced for the inspection of the Court shall be deemed to be documents and primary evidence." It is a direct legal recognition of electronic evidence (such as emails, digital files, server logs, CCTV footage, WhatsApp messages, etc.) as admissible without needing conversion or additional corroboration, provided authenticity is established.

This research paper will mainly focus on Cyber blockchain violation, which leads to cybercrimes, and digital evidence to support administering justice. Even before the newly enacted criminal laws, cybercrime was dealt with by the Information Technology Act, 2000[3], and the Indian Penal Code (IPC). In the Information Technology Act, 2000, cybercrime is not explicitly defined succinctly; however, it provides many measures countering cyber crimes faced by the general public, given from section 43 that is Unauthorized access, data theft, introducing malware, and damaging systems, section 66E that is Violation of privacy through capturing, publishing, or transmitting images without consent, Sec 67A & 67B that is Publishing sexually explicit content or child pornography[4] and etcetera. All these sections govern the legal framework of this country, administering justice to the culprits and victims of cybercrimes, and will be applicable in the future vis-à-vis working in corroboration with Bhartiya Sakshiya Adhiniyam 2023.

[1] The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Acts of Parliament, 2023 (India), available at: https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf
[2] The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61(2), Acts of Parliament, 2023 (India), available at: https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf.
[3] The Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India), available at: https://www.indiacode.nic.in/handle/123456789/1999.
[4] The Information Technology Act, No. 21 of 2000, §§ 43, 66E, 67, Acts of Parliament, 2000 (India), available at: https://www.indiacode.nic.in/handle/123456789/1999

While maintaining both analytical and critical tonality, this research paper will not lose the grasp of the schemes that the government has come up with to help the citizens of this country to combat cybercrime, e.g., Cyber Surakshit Bharat (2018 – present), To strengthen the cybersecurity ecosystem in India, especially in government departments and estabilishing salient institutions like National Critical Information Infrastructure Protection Centre (NCIIPC), Indian Cyber Crime Coordination Centre (I4C) to reduce the tantamount effects of cybercrime jeopardizing both citizen and national security. One of the foremost roles played by the legislative members of this country is implementing schemes, policies, and regulations, expediting digital awareness, and calling for action against surging cybercrimes.

2. Operational Dynamics of Cybercrime: From Phishing to Blockchain Abuse

Cybercrime is any unlawful activity performed via an electronic device like a computer or any digital device, involving a synchronized network and web, and its operational dynamics refer to how it is planned, executed, and monetized. Legal definitions of organized crime exhibit significant variations, shaped by the particular criminal contexts within different countries and periods. How the law defines organized crime and membership in such criminal groups is paramount. These baseline definitions profoundly influence the endeavours of law enforcement agencies.[5] As defined by the United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 in November 2000, an "organized criminal group" is described as;

"a structured group of three or more persons, existing for some time and acting in concert to commit one or more serious crimes or offences established by this Convention, to obtain, directly or indirectly, a financial or other material benefit (article 2(a))"[6]. Cybercrime in India operates through a multi-layered structure, often involving both local and transnational **actors**. These crimes range from basic phishing and identity theft to sophisticated financial frauds and critical infrastructure attacks. Cybercrime varies heterogeneously, ranging from financial to data stealing, and may include personal mala fide intentions which might channelize through different mediums, phishing, smishing, vishing, fake email logs, fake calls, sim swapping, UPI

[5] Suleman Lazarus, *Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity*, 45 Deviant Behav. (forthcoming 2024), https://doi.org/10.1080/01639625.2024.2352049.

[6] Suleman Lazarus, *Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity*, 45 Deviant Behav. (forthcoming 2024), https://doi.org/10.1080/01639625.2024.2352049.

fraud, and many more to be followed in the future as cyber-related activity accrues in this world. Cyber-attacks can be bifurcated into many phases, formats and types, which are as follows:

2.1 Reconnaissance (Planning Phase)

In this stage, attackers identify their targets: individuals, organisations, big business tycoons, and government entities. They collate information through social engineering, studying the demands in the markets, public social media profiles, leaked databases, and network scanning tools like Nmap. A foremost example of this is the infamous Cosmos Cooperative Bank Cyber Attack, Pune (2018)[7]Hackers infiltrated the ATM server of Cosmos Bank using **malware**, which allowed them to bypass the bank's core banking system (CBS**)**. The attackers then conducted a synchronised international ATM withdrawal operation which resulting in just two days, over 14,000 ATM transactions being carried out across **28 countries**, including Canada, Hong Kong, and the UK. In this stage, the attackers meticulously plan their plan of action to breach or ambush the planned website or data log and supplant various types of malwares, with ransomware, Trojans, and infostealers being among the most common. These malware types are often delivered through phishing emails, malicious websites, or deceptive software downloads.

2.2 Delivery of the weaponized medium onto the targeted system or individual

This stage includes a crucial step for the attackers to finally complete their aim by finally supplanting the malware or dangerous component into the targeted system to achieve their purpose. Sending the malicious tool to the target via: Phishing emails, Malicious links on websites or social media, USBs or external devices, Infected mobile apps. There are multiple hacking techniques that attackers use, like Brute Force**:** Brute forcing is a password hacking technique that requires the hacker to guess the user's password. This is possible because many users have weak passwords that follow specific patterns, such as "Password123". This can be done manually or with the use of automated tools[8]. The most dangerous method attackers use

[7] *Cosmos Cooperative Bank Ltd. Cyber Heist*, Pune Police Crime Reg. No. 3030/2018 (India), investigated under §§ 43, 66, 66B, 66C, 66D of the Information Technology Act, 2000 & §§ 409, 420, 120B of the Indian Penal Code (IPC), available at https://www.thehindu.com/news/national/other-states/hackers-steal-over-94-crore-from-cosmos-bank/article24694654.ece.

[8] North East Business Resilience Centre, What Techniques Do Hackers Use to Steal Information?, NEBRC (2024), https://www.nebrcentre.co.uk/what-techniques-do-hackers-use-to-steal-information/.

to supplant (plant) malware on someone's device is through drive-by downloads — a stealthy, highly effective, and often invisible method. A drive-by download is when malware is automatically installed or downloaded into a victim's device without their knowledge or consent, just by visiting a compromised or malicious website.

2.3 Command & Control (C2)

In cybersecurity and hacking, Command and Control (C2), also written as C&C, refers to the infrastructure and mechanisms used by cyber criminals to communicate with and control a compromised system (bot or infected machine) in a target network Once a device (like a PC or server) is infected with malware, the attacker needs a way to send instructions to it (e.g., steal data, spread malware, run commands, or exfiltrate data). This communication happens through the Command-and-Control server. This is the chronology in which it works; the victim downloads or is infected with malware, then beaconing, malware calls home to the C2 server to say "I am here", then the attacker sends a message via the C2 server, such as start keylogging, take screenshots, send stolen data back and etcetera, then he finally executes by letting the infected system operate and perform its task. The main purpose of the C2 server is to exfiltrate sensitive data (files, credentials), control a botnet (network of infected computers), deploy ransomware or wipers, and maintain persistence in the target system.

There are different types of C2 channels, such as HTTP/HTTPS, disguised as normal web traffic, IRC (Internet Relay Chat) – an older method, still used, and Peer-to-Peer (P2P) – no central server, more resilient, and many more.

3. Digital Currencies and National Security: Analysing the Use of Cryptocurrency by Terrorist Networks

A cryptocurrency is a digital or virtual currency that uses cryptography for security, making it nearly impossible to counterfeit or double-spend. It is typically decentralized and based on blockchain technology—a distributed ledger enforced by a network of computers (called nodes). The word "cryptocurrency" is a combination of *cryptography* (method of securing information) and *currency* (a medium of exchange). However, there is no single global definition, but it has been explained by different individual entities like Satoshi Nakamoto (2008–2009), the pseudonymous creator of Bitcoin. Nakamoto introduced the concept in The Bitcoin Whitepaper titled "Bitcoin: A peer-to-peer version of electronic cash would allow

online payments to be sent directly from one party to another without going through a financial institution." [9]This is considered the first formal articulation of what we now know as cryptocurrency. IMF (International Monetary Fund) described it as "A digital representation of value that is issued by private developers and denominated in their unit of account. Cryptocurrencies are not backed by any government or central bank."[10]

In India, cryptocurrencies are not illegal, but are not recognised as legal tender. The RBI (Reserve Bank of India) lifted its 2018 banking ban in 2020 (Supreme Court ruling), but the government still debates full regulation or prohibition. Cryptocurrencies are not specifically defined or categorized as legal tender and fall outside the scope of "currency" under the Foreign Exchange Management Act, 1999 (FEMA)[11]They are now subject to taxation under the Income Tax Act. Cryptocurrencies are not considered legal tender because they lack sovereign backing, stability, and regulatory oversight. Legal tender refers to currency that must be accepted for the repayment of debt and is officially issued by a country's central authority, such as the Reserve Bank of India (RBI). In contrast, cryptocurrencies like Bitcoin or Ethereum are decentralized digital assets that are not issued or regulated by the government. In India, although trading and investing in cryptocurrencies is not illegal, they are categorized as Virtual Digital Assets (VDAs) and taxed under specific provisions, but they do not hold the status of legal tender under the law.

There are various sections of statutory laws that do not recognize cryptocurrencies as legal tenders, hence are inconsistent with many legal provisions across the country, for eg Coinage Act 2011 defines the coins and currency legally recognized in India. Again, cryptocurrencies are not included; hence, they are not legal tender under this law. RBI Act, 1934 (Section 26) and Coinage Act, 2011 define legal tender, and crypto is excluded. Any violation of an individual's financial rights involving cryptocurrency may not be adequately redressed under existing Indian currency laws, as cryptocurrencies are not recognized as legal tender under Indian law. Consequently, protections and remedies available for fiat currency transactions may

[9] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf.
[10] International Monetary Fund, *Virtual Currencies and Beyond: Initial Considerations*, at 8 (June 2016) (defining "virtual currencies" as "digital representations of value, issued by private developers and denominated in their own unit of account"), https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.
[11] Foreign Exchange Management Act, No. 42 of 1999, § 3, INDIA CODE (1999), https://www.indiacode.nic.in/handle/123456789/1986.

not apply to transactions involving virtual digital assets[12].

Cryptocurrencies have been used by terror groups as a central source for their funding. Due to their covert and pseudonymous nature, ease of cross-border transfer, and lack of centralized oversight which cryptocurrencies are exploited for terror financing. We will elucidate the following with some of the milestones and credible cases, U.S. Treasury Department Evidence (2020)[13], In August 2020, the US Department of Justice (DOJ), in collaboration with the Department of Homeland Security (DHS) and IRS criminal investigation, dismantled the terror financing campaigns by Al-Qaeda, ISIS, HAMAS Military wing (al-Qassam Brigades) groups used cryptocurrency wallets to solicit and transfer funds for operational use. Cryptocurrencies have been actively used by terrorist organizations such as ISIS and Hamas for financing operations. International law enforcement agencies and intergovernmental watchdogs like the FATF have confirmed their use of virtual assets due to anonymity and global reach, posing a significant national and financial security risk.

4. Evolving Framework of Cybersecurity and Data Protection Laws in India: From the IT Act to the Digital India Era

India's journey into the digital era has been accompanied by accruing cyber threats and growing concern over personal data privacy. From the foundational Information Technology Act 2000, to recent advancements like the Digital Personal Data Protection ACT, 2023, India's legislative skeleton is undergoing rapid transformation to address evolving discrepancies of cyberspace. Now we will scrutinize various legal remedies available for cyberspace violations

4.1 DPDP Act, 2023: Bridging the Legal Gap in India's Data Governance

The DPDP Act, 2023, though primarily aimed at data privacy and regulation of data processing, indirectly contributes to India's fight against cybercrime, particularly in data breaches, identity theft, phishing, unauthorized profiling, and financial fraud. However, its impact on the broader cybersecurity ecosystem is complementary rather than comprehensive, leaving some critical gaps. Consent-Based Data Processing ensures that data collection and sharing occur only with

[12] See Reserve Bank of India Act, No. 2 of 1934, § 26(1), INDIA CODE (1934), https://www.indiacode.nic.in/handle/123456789/1938; see also Coinage Act, No. 11 of 2011, INDIA CODE (2011), https://www.indiacode.nic.in/handle/123456789/2051

[13] "Terrorist networks have adapted to technology, conducting complex financial transactions in the digital world, including through cryptocurrencies. Today's action demonstrates our ongoing commitment to disrupt and dismantle these networks."— *U.S. Attorney General William Barr*, U.S. Department of Justice, Aug. 13, 2020

valid consent, reducing the risk of unlawful data harvesting by scammers and attackers. The DPDP Act also provides that entities must take reasonable security safeguards under section 8 to prevent unauthorised access and data breaches—a common vector for cybercrime[14]. DPDP enacts Breach Notification, Section 8(6) mandates prompt notification of personal data breaches to the Data Protection Board of India (DPBI) and affected individuals, ensuring transparency and faster response to cyber threats. DPDP Act issues a penalty for data breach that is Severe financial penalties (up to ₹250 crore) act as deterrents against data leaks caused by negligence or wilful misconduct by data fiduciaries. Despite its relevance DPDP Act has not been designed as an anti-cybercrime law, which limits its effectiveness in direct cybercrime enforcement. The DPDP Act, 2023, while groundbreaking for personal data protection and privacy, should not be viewed as a cybercrime law in itself.

4.2 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

One of the pivotal features of the 2021 rules is the redefinition of the role of intermediaries (platforms like WhatsApp, Facebook, YouTube, etc in cybercrime prevention and cybercrime investigation. Due Diligence Obligations: Rule 3(1)(b) mandates intermediaries to publish clear user agreements and enforce restrictions against content that is defamatory, obscene, promotes hate, or violates law, thus aiming to reduce the circulation of harmful or illegal material[15]. The most aidful and Stupendous feature of the 2021 rules is the Grievance Redressal Mechanism, in which the rule explicitly states that every platform must have a Grievance officer to resolve user complaints within 15 days, ensuring a structured response mechanism for issues like cyberstalking, harassment, or identity theft.

Not only mandating such rules for every platform but also putting radar on the big intermediaries like intermediaries with over 5 million users are categorised as Significant Social Media Intermediaries (SSIMs) are obliged to have Chief Compliance Officer that Ensures compliance with Indian laws—critical when tackling issues like coordinated cyberattacks, radicalization, or financial frauds. Another important appointment that should also be sustained within these (SSIMs) are Nodal Contact Officers who are available 24/7 to

[14] The Digital Personal Data Protection Act, No. 22 of 2023, § [relevant section], Gazette of India, Aug. 11, 2023, https://egazette.nic.in/WriteReadData/2023/248049.pdf.
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Feb. 25, 2021 (issued under the Information Technology Act, No. 21 of 2000), https://egazette.nic.in/WriteReadData/2021/225464.pdf.

coordinate with law enforcement agencies in case of cybercrime investigations, content takedowns, or urgent threats. (SSIMs) are mandated to have Traceability Mandate rule 4(2) [16]that states Messaging platforms must enable the identification of the first originator of a message, especially in cases involving cybercrime, fake news, or national security threats, though this has sparked debates over end-to-end encryption and privacy rights.

Rule 3(1)(d) mandates platforms to disable access to unlawful content within 36 hours upon receiving a legal order. This rapid takedown framework is key in limiting the viral spread of cybercrime-enabling material like phishing websites, revenge porn, and doxxing[17]. The IT Rules 2021 explicitly prohibit intermediaries from hosting or publishing pornographic content, including Child Sexual Abuse Material (CSAM). This unjust and unruly act is sporadically linked with the dark web. This crucial IT Rule 2021 is highly beneficial for combating cybercrime in India, putting big and small, and every intermediary under ethical hegemony.

4.3 CERT-In Directions, 2022 (Cybersecurity Incident Reporting Guidelines) and their print on cybercrime

The directions were issued under Rule 12 of IT (Amendment) Rules[18], 2009 by the Indian Computer Emergency Response Team (CERT-in), effective from June 28, 2022. The CERT-In directions aim to strengthen India's Cybersecurity by standardizing cyber incident reporting timelines and formats, ensuring prompt threat intelligence exchange, enhancing coordination between stakeholders during cyberattacks, and holding service providers and intermediaries accountable. According to our analysis, we will triangulate the content within prevention, detection, and prosecution.

Prevention will include early detection of threats. The 6-hour rule in the clause of this directive ensures proactive containment of malware, phishing, ransomware, and network intrusions[19].

[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2), G.S.R. 139(E), Gazette of India, Feb. 25, 2021, https://egazette.nic.in/WriteReadData/2021/225464.pdf.
[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(b), G.S.R. 139(E), Gazette of India, Feb. 25, 2021, https://egazette.nic.in/WriteReadData/2021/225464.pdf.
[18] Ministry of Electronics & Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, https://www.meity.gov.in/content/notification-intermediary-guidelines-and-digital-media-ethics-code-rules-2021
[19] Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, CERT-In, Direction No. 20(3)/2022-CERT-In, ¶ 4 (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_2022.pdf.

Deterrence for VPN Misuse ensures that with mandatory KYC and retention, anonymity abuse via VPNs (common in cyberstalking, child pornography, and dark web crimes) is curbed[20]. The 180-day log mandate issued by the directive is pivotal in preventing repeated intrusions and identifying patterns.

Detection will include real-time monitoring and surveillance of the timeline of data breach, type of malware (especially for ATPs and ransomware), which ensures visibility of the root cause and remedies given proportionally to the attack, and an institutional overview of threats.

Prosecution will include Forensic Evidence, such as Logs, IP addresses, and synchronized data act as critical digital evidence in courts, under Section 66, 66C, 66D, 66E (IT Act) [21]of the IT Act work as crucial legal aid for preserving one's rights, and Sections 379, 420, 468, 469, 471 (IPC) [22]of the old law Indian Penal Code, Accountability of Intermediaries is Failing to comply attracts penalties under Section 70B(7) of the IT Act (up to 1 year imprisonment and/or fine).

5. *Modus Operandi* in Addressing and Remedying Cyber Law Violations under Bharitya Sakshya Adhiniyam (BSA).

The newly enacted criminal law Bhartiya Sakshya Adhiniyam (BSA) has incorporated electoral evidence as stage-1 evidence and will be hitherto treated as crucial evidence while the actual remedies are available under Bhartiya Nyaya Sanhita (BNS), Information Technology Act 2000, Bhartiya Nagrik Suraksha Sanhita (BNSS) and CERT-In guidelines, but to prove a cybercrime, electronic device is crucial which has been added in (BSA) – and that is where BSA comes to rescue. We will discuss how one can access the remedies if threatened with cyber rights violations:

5.1 Forensic Acquisition of Electronic Evidence in Cybercrime Investigations

Under Section(61–90)of the BSA[23]Electronic records (emails, WhatsApp chats, log files,

[20] Id. ¶ 6(i)–(iii) (mandating data centres, VPNs, and cloud service providers to retain validated customer information, including name, address, contact numbers, email ID, and IP logs, for five years or longer after cancellation or withdrawal of service).
[21] The Information Technology Act, No. 21 of 2000, §§ 66, 66C, 66D, 66E, 66F, INDIA CODE (2000), https://www.indiacode.nic.in/handle/123456789/1999.
[22] The Indian Penal Code, No. 45 of 1860, §§ 379, 420, 468, 469, 471, INDIA CODE (1860), https://www.indiacode.nic.in/handle/123456789/2263.
[23] The Bharatiya Sakshya Adhiniyam, 2023, §§ 61–90, No. 47, Acts of Parliament, 2023 (India), https://egazette.nic.in/WriteReadData/2023/248601.pdf.

screenshots, server logs, etc.) are admissible. There are several methods of forensic acquisition, like disk imaging, which is by bit copy of a storage medium using tools like FTK Imager, mobile forensics, extracting data from tools like Celebrite and etcetera. You must ensure the authenticity of digital records (hash values, metadata, timestamps, Section 63 [24]talks about the presumption of integrity in digital records from secure systems.

5.2 Certificate of Authenticity

Provided under section 63(4)[25], that is, if you submit electronic evidence (e.g., hard drive, server logs), you need a Section 63(4) certificate, previously under Section 65B[26] of the Evidence Act. The aforementioned certificate should state that: the source of the evidence, that the source was taken from a reliable computer system, and that the signature of a competent person is present.

5.3 Use in Court for Remedies against Cybercrime

Based on the evidence accepted under Bhartiya Sakshya Adhiniyam, 2023, the after procedure is to file an FIR or lodge a cybercrime complaint (via https://cybercrime.gov.in) [27]. Present your evidence in court (criminal case or civil damages), use logs, CCTV, server IP traces, emails, and more as admissible proof. In gist of it this is the *modus operandi* first is to File a complaint at local police station or cybercrime portal then Collect emails, screenshots, chats, IP address, bank transfer records, Take hash values of original files and generate a Section 63(4) certificate, Submit evidence to court/police with BSA-compliant certificate, Court examines evidence under BSA for admissibility, Prosecution under IT Act or BNS 2023, depending on offence, Remedies provided to you would be Arrest, injunction, damages, conviction, blocking orders, etc.

[24] The Bharatiya Sakshya Adhiniyam, 2023, § 63, No. 47, Acts of Parliament, 2023 (India), https://egazette.nic.in/WriteReadData/2023/248601.pdf.
[25] The Bharatiya Sakshya Adhiniyam, 2023, § 63(4), No. 47, Acts of Parliament, 2023 (India), https://egazette.nic.in/WriteReadData/2023/248601.pdf.
[26] The Bharatiya Sakshya Adhiniyam, 2023, § 65B, No. 47, Acts of Parliament, 2023 (India), https://egazette.nic.in/WriteReadData/2023/248601.pdf.
[27] National Cyber Crime Reporting Portal, Cyber Crime, Ministry of Home Affairs, Gov't of India, https://cybercrime.gov.in

6. Doctrinal Insights from Case Laws

The case of *Shreya Singhal v. Union of India (2015)* [28]by the Supreme Court challenged the constitutional validity of section 66(A) of the Information Technology Act, 2000, which penalized sending "offensive" messages via communication services. The section was vague and led to arbitrary arrests for social media posts. In the final judgement Supreme Court struck down Section 66A as unconstitutional, holding that it infringed upon the freedom of speech and expression under article 19(1)(a) The Court observed that the terms used in the provision—such as "grossly offensive" and "menacing"—were undefined and subjective, leading to potential misuse.

In the case of *State of Tamil Nadu v. Suhas Katti (2004)*[29]Cyberstalking and defamation were involved. The accused posted obscene and defamatory messages about a woman in a Yahoo message group, and the victim filed a complaint with the cyber cell. Later, the court gave its judgement hereby holding the accused guilty under section 67 of the IT Act, 2000[30], and sections 469 [31]and 509 of the then IPC[32]. The court found that the accused had deliberately posted offensive content to harass the woman. Notably, it was the first conviction in a cybercrime case in India, completed in just seven months.

In the case of *State of Tamil Nadu v. S. Murugan (Job Scam via Cyber Fraud)* [33]the accused created fake government websites and offered fraudulent job opportunities. Victims were lured into paying fees for non-existent recruitment processes. The accused was convicted under Section 66D of the IT Act[34] (cheating by impersonation using computer resources) and relevant IPC provisions. The court found overwhelming evidence, including a digital trail of payments and emails, that confirmed the accused's involvement.

Now we will scrutinize and analyse some international and pivotal cases,

---

[28] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
[29] *State of Tamil Nadu v. Suhas Katti*, Case No. 4687 of 2004 (Mag. Ct. Chennai) (India).
[30] The Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India), https://legislative.gov.in/sites/default/files/A2000-21.pdf.
[31] The Indian Penal Code, 1860, § 469, No. 45, Acts of Parliament, 1860 (India), https://legislative.gov.in/sites/default/files/A1860-45.pdf.
[32] The Indian Penal Code, 1860, § 509, No. 45, Acts of Parliament, 1860 (India), https://legislative.gov.in/sites/default/files/A1860-45.pdf.
[33] *State of Tamil Nadu v. S. Murugan*, C.C. No. 346 of 2004 (Mag. Ct. Egmore, Chennai) (India).
[34] The Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India), https://legislative.gov.in/sites/default/files/A2000-21.pdf.

In the case of *United States v. Kevin Mitnick (1999),*[35] Aaron Swartz, a digital activist, downloaded millions of academic articles from JSTOR using MIT's network without authorization. He was charged under the 'Computer Fraud Abuse Act' (CFAA). Unfortunately, before the trial could proceed, Swartz died by suicide, and the case did not reach a final judgment but sparked global outrage. This case resulted in reiterating the relevance of 'Intent and Motive' should be crucial element in determining cybercrime prosecution.

In the famous *United States v. Gary McKinnon* case[36]. Also known as the NASA hacker case, McKinnon was accused of hacking into 97 U.S. military and NASA computers, disabling critical infrastructure, deleting files, and causing damage estimated at $700,000. The extradition request was blocked in 2012 by then-Home Secretary Theresa May, citing human rights concerns, especially McKinnon's diagnosis of Asperger's syndrome and severe depression. This brought global attention to international cybercrime jurisdiction and gave new direction for nations to create a safe anti-cybercrime policy. As we discussed, various planning stages of an attacker and the procedure followed by law enforcement afterward are very much involved in McKinnon's case is that Investigators used forensic tools to trace IP addresses, logins, and **electronic footprints** across multiple U.S. federal networks, hence there forth showcasing the importance of digital evidentiary importance in justice system.

7. Conclusion

The rise of cybercrime in India and across the globe has necessitated a parallel evolution in both legal and investigative frameworks. This paper has highlighted the critical role of forensic acquisition in securing electronic evidence that is not only admissible in court but also essential for achieving successful convictions. Furthermore, we have thoroughly examined the anatomy of cybercrimes—tracing their planning, tools, and tactics used by perpetrators to breach digital privacy and exploit victims emotionally, financially, or socially.

As cybercrime grows in complexity and scale, the importance of robust criminal laws and responsive judicial mechanisms becomes even more crucial. Landmark judgments such as *State of Tamil Nadu v. Suhas Katti*, *Shreya Singhal v. Union of India*, and international cases like *United States v. Kevin Mitnick* demonstrate the judiciary's increasing engagement with

[35] United States v. Mitnick, No. CR 94-00722 (C.D. Cal. 1999).
[36] *United States v. McKinnon*, Indictment, No. 04-10053-WGY (D. Mass. Nov. 12, 2002).

digital offenses and the evolving interpretation of cyber laws. Yet, several challenges persist, including jurisdictional hurdles, technological obsolescence, and the ongoing need to balance personal privacy with lawful surveillance.

With the implementation of frameworks such as the IT Rules 2021, CERT-In Guidelines 2022, and the Digital Personal Data Protection Act, 2023, India is taking concrete steps toward building a stronger cyber-legal ecosystem. However, the current legislative efforts must not overlook the foundational role that cyberspace and cybersecurity will play in shaping the infrastructural, cultural, and legal landscape for future generations. The urgent need for consolidated, forward-looking legislation—such as the proposed Digital India Act—cannot be overstated, especially in matters concerning the acquisition, preservation, and admissibility of electronic evidence.

This study has also explored the key preventive and remedial measures essential for safeguarding individuals' digital rights, and the central role digital evidence plays in judicial and prosecutorial processes. In light of the rising number of cybercrime cases, the public must be made aware of not only their rights but also the protective measures available to them under the law. Awareness, preparedness, and timely response to such offenses are critical to ensuring justice is neither delayed nor denied.

Ultimately, the battle against cybercrime will not be won by technology alone. It demands stronger laws, trained enforcement agencies, active citizen participation, and a system-wide commitment to justice. Only by aligning legal reform with technological innovation can we create a secure and just digital future.