IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Navigating Cyber Threats In India: An Analysis Of Awareness And Legal Remedies In The Digital Age

K.Kokila, Assistant Professor, Bharath Institute of Law

N.Vijay Viknesh, Student, Bharath Institute of Law

ABSTRACT

This article critically examines the rapidly evolving landscape of cybercrime in India, focusing on emergent digital threats, their underlying motivations, and the efficacy of the national legal framework in response. The digital realm presents a unique jurisdictional challenge as computers are increasingly exploited both as instruments for traditional offenses (e.g., fraud via UPI scams) and as targets of sophisticated attacks (e.g., ransomware and Web 3.0 exploits).

The paper categorizes these modern threats, highlighting the societal impact of social media-related offenses (cyberbullying, misinformation) and the financial toll of large-scale, transnational digital fraud. Systematically, it analyzes India's tripartite legal response anchored by the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information Technology (IT) Act, 2000, and the new Digital Personal Data Protection (DPDP) Act, 2023.

The article concludes that while legislative efforts have evolved, effective cybercrime prosecution is perpetually hindered by cross-border jurisdictional complexities, the volatility of digital evidence, and systemic deficiencies in specialized law enforcement capacity. Sustained legal modernization and enhanced global cooperation are imperative to secure India's digital future against pervasive cyber threats.

Key Words: Cyber Crimes, Digital Era, Data Protection, Information Technology

INTRODUCTION

In today's digital landscape, cybercrime poses a significant threat to individuals, businesses, and governments! This article dives deep into the emergent cyber-crimes in India, highlighting the double nature of cyber offenses as target computers or using them as weapons. From hacking and virus attacks to cyber terrorism and intellectual property violations, the spectrum of cybercrimes is vastly evolving, encompassing new challenges, such as social media crimes and the emergence of Web 3.0 technicalities. The legal response to cybercrime, governed by a variety of statutes and act in India, including the Indian Penal Code, the

Information Technology Act 2000, and the recently enacted [1]Digital Personal Data Protection (DPDP) Act, 2023, is crucial in navigating this digital realm! These laws provide the frameworks for prosecuted cyber offenders and protect the rights of individuals in cyberspace, with provisions addressing offenses such as

unauthorized access, data theft, cyberbullying, and online fraud! Furthermore, international organizations such as the National Institute of Standards and Technology (NIST) play vital roles in cybersecurity by providing standards and guidelines for cybersecurity best practices. By adhering to NIST frameworks such as the Cybersecurity Framework (CSF), organizations can enhance their cybersecurity posture and mitigate cyber risks effectively! Moreover, as cybersecurity becomes increasingly intertwined with our daily lives, raising awareness about safe online practices and digital literacy is paramount. Initiatives aimed at educating individuals and organizations about the risks of cybercrime, as well as strategies for prevention and response, play a vital role in mitigating the impacts of cyber threats.

EMERGING TRENDS & CHALLENGES IN CYBER CRIMES

In recent years, India has seen a surge in emergent cybercrimes, posing significant challenges to persons, businesses, and government establishments. One significant trend is the spreading of social media offenses, including online harassment, cyberbullying, and the dissemination of fake news and misinformation. The wide adoption of social media stages has given cybercriminals new pathways to exploit innocent victims and carry out crimes with secrecy and impunity.

Also, online monetary offenses and hustles have become more and more prevalent, targeting individuals pursuing convenient digital financial services. Tricks implicating UPI (Unified Payments Interface) platforms, such as deceitful transactions, phishing assaults, and unauthorized fund transfers, have turned into an expanding worry for users. Similarly, online loan tricks, where uninformed individuals are tricked into applying for fake loans or monetary assistance, have observed a sharp increase, exploiting the vulnerabilities of those in require of fast financial solutions.

Moreover, the surge of Web 3.0 advancements introduces modern opportunities for cybercriminals to exploit vulnerabilities and begin complex cyber-attacks. Blockchain, decentralized credit (DeFi), and the Internetworking of Items (IoT) are among the emergent advancements that hold immense guarantees for innovation and financial development. However, their decentralized nature and the lack of solid cybersecurity protocols make them exposed to exploitation by cybercriminals.

Moreover, the COVID-19 pandemic has escalated existing cyber threats and generated new challenges for cybersecurity professionals. The shift to remote employment and online learning has expanded the attack surface for cybercriminals, leading to an increment in phishing assaults, ransomware occurrences, and other cyber threats targeting individuals and organizations.

Handling these emergent cybercrimes requires a multi-faceted way that combines proactive awareness campaigns, technological invention, and strong cybersecurity measures. By increasing awareness almost secure online practices, enhancing cybersecurity infrastructure, and promoting collaboration between

[1]. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

government bureaus, law enforcement authorities, and industry stakeholders, India can efficiently mitigate the impact of emerging cyber threats and create a more secure digital environment for its citizens.

MAJOR FACTORS CONTRIBUTING TO THE RISE OF CYBERCRIMES IN INDIA

- **Financial gain:** can be obtained by either demanding a ransom in return for stolen data or resources or by stealing financial information, such as bank account details and credit card numbers.
- **Espionage:** Some cybercriminals commit cybercrime in order to obtain proprietary or secret information for a competitive edge or to harm an organization's reputation.
- **Political or ideological motives**: Some cybercriminals target groups or individuals for political or ideological purposes, such as to further a specific goal or cause. For instance, ISIS uses government and military websites to propagate propaganda and hate.
- **Personal motives**: Some cybercriminals commit cybercrime in order to harass, libel, or cause harm to people or organizations.
- **Opportunism:** Some cybercriminals commit cybercrime just because they can, using people's or technology's security flaws to steal data or resources.
- **Lack of Awareness:** Many cybercrimes are carried out by people who are ignorant of the repercussions of their behaviour and whether it is lawful.

CATEGORIES OF CYBERCRIMES IN THE DIGITAL ERA

1) Social Media Platforms & Financial Frauds

- **Cyber Bullying** – is a type of harassment or bullying that is carried out via electronic or communication equipment, such as a computer, smartphone, laptop, etc. It affects social isolation, mental health, and academic achievement.
- **Cyber Stalking**- is the practice of using electronic communication to follow someone or making repeated attempts to get in touch with someone in order to establish a personal connection, even when that person clearly shows no desire in doing so.
- **Cyber Grooming**- Cyber Grooming is the practice of establishing an online contact with a young person and deceiving or coercing them into engaging in sexual activity.
- **Sexting**- Sending sexually explicit digital photos, videos, texts, or emails—typically via a cell phone—is known as sexting.
- **SIM Swap SCAM:** This happens when scammers are able to obtain a new SIM card from the mobile service provider using a registered mobile number.
- **Spamming**: When someone receives an unwanted commercial communication by email, SMS, MMS, or any other comparable electronic messaging medium, it's known as spamming.
- **Credit/Debit Card Fraud:** This type of fraud entails using someone else's credit or debit card information without authorization in order to make transactions or take money out of it.

- **Impersonation and identity theft:** The act of fraudulently or dishonestly using another person's electronic signature, password, or any other distinguishing characteristic is known as identity theft or impersonation.

2) Organisation/Business/Nation targeting cyber crimes

- **Ransomware** is a kind of computer software that holds data and information hostage by encrypting files and storage media on communication devices like desktops, laptops, mobile phones, etc.
- **Pharming** A cyberattack known as "pharming" aims to divert visitors from one website to a fake one.
- **Cyber-Squatting** The act of registering, trafficking in, or utilizing a domain name with the intention of making money from the goodwill of another person's trademark is known as cyber-squatting.
- **Website Defacement** is an attack meant to alter a website's appearance and/or render it unusable. Images, messages, videos, and other content that are offensive, hostile, and vulgar may be posted by the attacker.
- **Distributed Denial of Service (DDoS)** attack seeks to disrupt the accessibility of an online service by inundating it with traffic from numerous sources.
- **Data breaches:** involve unauthorized entry and theft of confidential information, including personal and financial data.
- **Salami Slicing Attack:** funds or resources are gradually taken in small amounts, preventing any significant impact on the bank account from being noticed.

LEGISLATIVE MEASURES FOR PREVENTION OF CYBER CRIMES

The fact that billions of people utilize the internet today cannot be overstated. People use the internet practically everywhere, including at their homes, workplaces, train stations, colleges, and shops. Our economy has also grown entwined with the internet. The internet creates jobs money. Unfortunately, organized crime and hackers abuse the internet. The proliferation of the internet is directly correlated with the rise in cybercrime. As the number of people using the internet rises, so does cybercrime. The public has access to the internet, yet users are vulnerable to mental torment, financial gain through spyware, and societal evil. Therefore, industries are creating a variety of products for use in homes and businesses to identify and prevent such cyber threats, such as intrusion detection systems, firewalls, antivirus software, etc. We are unable to eradicate cybercrime in spite of all the preventative measures. Despite the fact that we are employing numerous countermeasures, cybercrime is still thriving and the issue of internet security is rapidly expanding. In order to properly administer justice to victims of cybercrime, "consequently, there was a compelling need for the cyber space authority to adopt strict laws to regulate criminal activities..." In the area of contemporary cyber technology, Cybercrimes must be regulated, and most critically, cyber laws should be tightened in the case of hackers and cyberterrorism

1) Bharatiya Nyaya Sanhita, 2023 (BNS)

- [2]**Section 356** (**Defines Defamation**) - The definition of defamation, including the ten exceptions and the meaning of "Harm," remains essentially the same. This ensures continuity in prosecuting cyber defamation cases where defamatory statements are intentionally published electronically (e.g., via social media, email, or messaging apps).
- **Section 356** (**Defamation Punishment**)- The quantum of punishment (up to two years' incarceration, or a fine, or both) is retained in the BNS.
- [3]**Section 343- Fraudulent cancellation, destruction, etc., of will, authority to adopt, or valuable security:** BNS Section 343 retains the exact substance of IPC Section 469. This provision is vital for cybercrime as it directly addresses offenses like creating fake documents or fraudulent digital certificates with the intent to ruin a person's reputation
- [4]**Section 344- Falsification of accounts:** BNS Section 344 is the direct successor to IPC Section 470. It retains the definition of a "forged document" and, critically for your article's topic, the inclusion of "electronic record".
- **Cybercrime Relevance:** This provision ensures that any false electronic record (such as a fake digital contract, fraudulent electronic signature, or doctored image/video) created wholly or partly by forgery is legally recognized as a "forged electronic record" under the penal law.

2) The Information Technology Act, 2000

The Indian Parliament passed the Information Technology Act, 2000 (IT Act-2000) to safeguard e-banking, e-governance, and e-commerce as well as to provide sanctions and penalties for cybercrimes. The Information Technology (Amendment) Act, 2008 (ITAAct-2008) made additional changes to the aforementioned Act. The term "communication devices" was added to the definition to encompass mobile phones, PDAs, and other gadgets that transfer text, video, and other data, such as those that were later marketed as iPads or other comparable devices on cellular and Wi-fi versions. The term "digital signature" was defined by the IT Act of 2000, but it was unable to meet modern demands, hence

The ITA Act of 2008 introduced and defined the term "Electronic signature" as a legitimate method of signing documents. This covers biometrics and other novel methods of producing electronic signatures, and it encompasses digital signatures as one of the signature modes.

[2]. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 356, India Code (2023). (Which covers both the definition and the punishment for defamation.)

[3]. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 343, India Code (2023). (Title: Fraudulent cancellation, destruction, etc., of will, authority to adopt, or valuable security)

[4]. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 344, India Code (2023). (Title: Falsification of accounts)

Some of the Important sections under IT ACT 2000 are given as follows:

- [5]**Section 65 – Tampering with computer Source Documents-** Anyone who wilfully hides, destroys, or modifies computer source code—including programs, computer commands, designs, and layouts—when it is mandated by law is guilty of a crime that carries a maximum sentence of three years in jail, a fine of two lakh Indian rupees, or both.
- [6]**Section 66 - Using password of another person-** A person may be imprisoned for up to three years or fined one lakh Indian rupees if they fraudulently exploit someone else's password, digital signature, or other unique identifier.
- [7]**Section 66D - Cheating Using computer resource-** A person may be imprisoned for up to three years or fined up to one lakh Indian rupees if they use a computer resource or communication device to deceive someone.
- **Section 66E - Publishing private Images of Others-** A person faces up to three years in prison, a fine of up to two lakh Indian rupees, or both if they take, send, or publish pictures of someone else's private areas without that person's knowledge or consent.
- [8]**Section 66F - Acts of cyber-Terrorism-** If someone tries to access or penetrate a computer resource without authority with the intention of endangering the nation's unity, integrity, security, or sovereignty, they risk life in jail. This offense is not subject to bail.
- [9]**Section 67 - Publishing Child Porn or predating children online-** A person may be imprisoned for up to seven years, fined up to ten lakhs INR, or both if they photograph, publish, or transmit photos of a minor engaging in a sexually explicit act or coerce someone under the age of eighteen into engaging in such behaviour.
- [10]**Section 69 - Govt.'s Power to block websites-** The government may intercept, monitor, or decrypt any information created, sent, received, or stored in any computer resource if it deems it necessary to protect India's integrity and sovereignty. The authority is contingent upon adherence to protocol. The central government may also prevent the public from accessing any material under section 69A.

[5]. Information Technology Act, No. 21 of 2000, § 65, India Code (2000). (Title: Tampering with computer source documents)
[6]. Information Technology Act, No. 21 of 2000, § 66, India Code (2000). (Title: Computer related offences)
[7]. Information Technology Act, No. 21 of 2000, § 66D, India Code (2000). (Title: Punishment for cheating by personation by using computer resource)
[8]. Information Technology Act, No. 21 of 2000, § 66F, India Code (2000). (Title: Punishment for cyber terrorism)
[9]. Information Technology Act, No. 21 of 2000, § 67, India Code (2000). (Title: Punishment for publishing or transmitting obscene material in electronic form)
[10]. Information Technology Act, No. 21 of 2000, § 69, India Code (2000). (Title: Power to issue directions for interception or monitoring or decryption of any information through any computer resource)

- [11]**Section 43A - Data protection at corporate level-** A body corporate will be responsible for paying damages to the affected individual if it is careless in putting appropriate security measures into place that result in an unjust gain or loss for any individual.

3) Government initiatives to fight against Cybercrime

Since the Citizen Financial Cyber Fraud Reporting and Management System was established, over 4.7 lakh complaints have saved over Rs. 1200 crore. To aid with filing online cyber complaints, a toll-free Helpline number, "1930," has been operationalized. The Citizen Financial Cyber Fraud Reporting Management System's State/UT-specific information from 1.1.2023 to 31.12.2023 may be found in the Annexure. According to police sources, the Indian government has blocked over 3.2 lakh SIM cards and 49,000 IMEIs thus far.

- **Cyber Crime Investigation Cell (CCIC):** is in charge of looking into cybercrime cases and offering other law enforcement organizations technical assistance.
- **National Cyber Coordination Centre (NCCC:** serves as a central hub for agencies and organizations to coordinate and exchange information about cyber security.
- **National Cyber Security Policy:2013**, The government's plan for safeguarding India's vital information infrastructure and securing cyberspace is outlined in the National Cyber Security Policy of 2013
- **CERT-In:** is the nation's nodal agency for handling incidents and threats related to cyber security. Additionally, it offers rules, advisories, and alerts for protecting networks and IT systems.
- **National Critical Information Infrastructure Protection Centre (NCIIPC):** is in charge of preventing cyberattacks on the nation's vital information infrastructure, which includes government networks, banking systems, and power grids.
- **Awareness campaigns**: The government often runs training initiatives and awareness campaigns.

4) Safety mechanisms, to avoid cyber attacks by Every Citizen

- **Antivirus and firewall software**: using antivirus and firewall software to protect against malicious software and unauthorized access.
- **Regular software updates**: keeping all software, including the operating system, up-to date to ensure the latest security patches are installed.
- **Strong passwords**: using unique and complex passwords for each online account.
- **Multi-factor authentication**: using additional methods of authentication such as a security token or biometrics to verify identity.
- **Wi-Fi in public places should be disregarded** - When utilizing public Wi-Fi, never make online payments, email personal information, or introduce crucial account passwords.
- **Unsolicited emails and SMS communications should be avoided** - Never click on a link, picture, or video sent to you by an unknown source.

[11]. Information Technology Act, No. 21 of 2000, § 43A, India Code (2000). (Title: Compensation for failure to protect data)

- **Check for spelling errors**, bad language, unusual phrasing, and urgent requests for money or action to ensure that emails are authentic. Malicious websites may appear to be identical to legal sites; however, the URL is frequently misspelt or uses a different domain.
- **Protect personal information on social media** – Cyber criminals utilize social media to gather personal information that they may subsequently exploit in phishing schemes.
- Don't use **charging/adapter** cables from strangers.

JUDICIAL APPROACH TO CYBERCRIME IN INDIA

[12]Cyber Attack on Cosmos Bank: 2018 (India's biggest Cyber Attack), In this case Eleven individuals have been convicted in the Cosmos Bank cyber fraud case, which involved the siphoning off of over Rs 94 crore through a malware attack over a two-day period in 2018. The court in Maharashtra's Pune district sentenced nine of the accused to four years' imprisonment and two others to three years, along with fines. The convictions were made under relevant sections of the Indian Penal Code and the Information Technology Act. The fraud, executed over two days in August 2018, resulted in the arrest of 18 individuals from different parts of the country. The hackers obtained information from Cosmos Bank's VISA and RuPay card customers through malware, then attacked the SWIFT system, leading to the unauthorized transfer of over Rs 94 crore on August 11 and 13, 2018. They targeted the bank's ATM switch server, withdrawing Rs 78 crore from various ATMs in 28 countries, and another Rs 2.5 crore within India. On August 13, they fraudulently transferred Rs 13.92 crore to a Hong Kong-based bank using the proxy SWIFT system, with police managing to recover Rs 5.72 crore of the stolen amount.

The crime was executed in two distinct phases over a weekend in August 2018-

1. ATM Switch Compromise: Hackers installed malware onto the bank's servers to create a proxy switch system, effectively bypassing the bank's Core Banking System (CBS) and its security checks. This proxy system fraudulently approved over 12,000 debit card transactions from 29 countries in a matter of hours, allowing criminals to withdraw approximately ₹78 crore (over $11 million) from ATMs using cloned cards.

2. SWIFT Compromise: Shortly after, the criminals initiated a separate attack on the bank's SWIFT (Society for Worldwide Interbank Financial Telecommunication) system, using malicious messages to fraudulently transfer an additional ₹13.92 crore to a bank account in Hong Kong.

The total loss exceeded ₹94 crore, highlighting the severe financial consequences of integrated malware and financial messaging attacks.

The subsequent investigation led to the arrest and conviction of eleven individuals involved in the money laundering and physical withdrawal operations; all charged under the IPC and the IT Act. While the foot soldiers were apprehended, the core masterminds of the attack, attributed by some security firms to state-sponsored groups like Lazarus, have not been officially identified by Indian authorities. The convictions

[12]. Pune court convicts 11 accused in Cosmos Bank cyber fraud case, HINDU (Apr. 23, 2023). (A news report confirming the conviction details)

demonstrated the legal system's capacity to punish those involved in the operational network of transnational cyber heists.

CONCLUSION

Society increasingly relies on technology which inevitably leads to a rise in electronic, with cybercrime quickly spreading as a consequence of widespread computer and internet usage. These criminal actions not only slow down a country's progress but also negatively impact its people and hinder economic growth. While the Information Technology Act, 2000 and the Digital Personal Data Protection Act, of 2023, act as significant tools in fighting cybercrime, it's important to note that offenses related to computers also come under the preview of the Indian Penal Code and other laws in India. However, the underreporting of cybercrimes poses a challenge, with only a fraction of incidents officially reported and even fewer making it to the courts. Challenges emerge in collecting, storing, and assessing digital evidence. Although the implementation of these laws shows promise in addressing cybercrimes and protecting victims, there is still plenty of ground to cover. Lawmakers must continuously update and strengthen existing laws to effectively tackle the changing nature of cyber threats and ensure the safety and security of society in the digital age.

[13]The landscape of cyber-jurisprudence in India, while robustly anchored by landmark judgments, remains perpetually challenged by the triumvirate of technological velocity, jurisdictional complexity, and evidentiary hurdles.

Jurisdictional and Cross-Border Hurdles- Cybercrimes are fundamentally borderless, with malicious actors often operating from foreign nations with uncooperative judicial regimes, thus complicating the identification and extradition of suspects. The investigation and prosecution process is frequently stymied by slow-moving Mutual Legal Assistance Treaties (MLATs), which delay cross-border data sharing, and by the lack of harmonized laws and data standards globally. Determining which national jurisdiction has the authority to adjudicate a case remains a persistent dilemma.

The Digital Evidence Conundrum- Digital evidence, which forms the sole basis for conviction in most cyber cases, is inherently volatile and prone to tampering. The courts face unique challenges in adhering to the strict certification requirements mandated by Section 65B of the Indian Evidence Act. Prosecutors must successfully establish a robust chain of custody for electronic records, which requires specialized forensic expertise and dedicated, well-equipped labs—resources many state law enforcement agencies currently lack.

Legislative and Institutional Gaps- Despite the introduction of the IT Act and the DPDP Act, the legal framework is often reactive rather than preventive, perpetually struggling to keep pace with advancements like Artificial Intelligence (AI) and complex DeFi exploits. There is an urgent need for legal reforms that clarify ambiguous definitions, especially concerning the determination of *mens rea* (criminal intent) in automated or remote offenses. Institutionally, an insufficient number of specialized cyber courts and a deficit in the training of judicial officers and prosecutors on digital forensics contribute to low conviction rates and delayed justice.

[13]. Kavita Rani, *Cybercrime and Legal Responses in the Indian Jurisdiction*, 1 Indian J. L. 35, 38 (2023).

In summation, India's progression towards a secure digital future rests on a concerted commitment to legislative modernization, aggressive capacity building within law enforcement units, and a judicial vigilance that continues to uphold constitutional safeguards in the face of evolving digital threats. The synergistic application of the BNS, IT Act, and the DPDP Act must be supported by streamlined international cooperation to secure the nation's digital sovereignty and ensure citizen safety.

EFFECTIVE SUGGESTIONS FOR LEGAL AND PROCEDURAL UPGRADES

The persistent challenges of technological velocity, jurisdictional complexity, and evidentiary volatility demand targeted legal and institutional reforms. The successful integration of the Bharatiya Nyaya Sanhita (BNS), 2023, and Bharatiya Sakshya Adhiniyam (BSA), 2023, provides a critical opportunity for a systemic overhaul to enhance detection and deterrence.

A. Legislative Clarity and Harmonization

1. Explicitly Criminalize Emergent Offenses (Necrophilia): The BNS, 2023, must be amended to include a specific, dedicated provision that explicitly defines and penalizes sexual offenses or gross indignity against a dead body. Relying on general sections like BNS Sec. 301 (Trespass on Burial Grounds) is legally inadequate and fails to reflect the true gravity of such crimes.

2. Mandate Time-Bound Incident Reporting: Legal frameworks should enforce mandatory obligations for Intermediaries and Body Corporates to report cybersecurity incidents to CERT-In within a strict, non-negotiable timeframe (e.g., within a few hours of detection). This ensures immediate containment and faster forensic investigation.

3. Broaden "Organised Crime" Scope: While the BNS has included cybercrime within Organised Crime, this provision should be continuously reviewed to include emerging syndicated activities like Ransomware-as-a-Service (RaaS) and complex Deepfake-driven frauds that utilize AI.

4. Strengthen Digital ID Protection: Laws must be adapted to regulate digital identity and combat spoofing techniques used in financial fraud (like UPI scams). The *Department of Telecommunications (DoT)* initiative using the Financial Fraud Risk Indicator (FRI) to classify high-risk numbers should be given statutory backing for immediate network blocking.

B. Procedural Overhaul and Evidentiary Integrity

1. Simplify Digital Evidence Admissibility: Despite the BSA, 2023, recognizing electronic records as primary evidence, the complexity of Section 63 (analogous to IPC Sec. 65B) often remains a hurdle. Detailed technology-specific protocols must be issued by the Ministry of Home Affairs to standardize the collection and certification process for cloud data, encrypted wallets, and social media posts.

2. Mandatory Forensic Protocol: For serious offenses (punishable by seven years or more), the BNSS, 2023, requires involving forensic experts. This must be enforced by mandating video recording of the search and seizure process for electronic devices, ensuring an auditable and tamper-proof chain of custody from the start.

3. Utilize Remote Testimony: The BNSS, 2023, provisions allowing audio-video communications and remote witness testimony should be actively utilized in cross-border cybercrime cases to expedite trials and reduce the reliance on slow-moving Mutual Legal Assistance Treaties (MLATs).

C. Institutional Specialization and Capacity Building

1. Establish Dedicated Cyber Courts: Create and fund Specialized Cyber Courts with judges who have mandatory, continuous training in digital forensics, blockchain technology, and IT law. This specialization is necessary to increase conviction rates and reduce the heavy technical burden on general courts.

2. Enhance Cyber Forensics Capacity: Provide robust financial support for the establishment of well-equipped cyber forensic labs across all states and Union Territories, particularly under the Indian Cybercrime Coordination Centre (I4C) framework. This includes training specialized staff to handle complex evidence from sources like the dark web and cryptocurrencies.

3. Strengthen Public-Private Collaboration: Formalize partnerships between law enforcement agencies and Internet Service Providers (ISPs), technology firms, and financial institutions. This collaboration is vital for rapid threat intelligence sharing and for implementing proactive monitoring and blocking measures against Child Sexual Abuse Material (CSAM) and financial scams.

REFERENCE

1. Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
2. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 356, India Code (2023). (Which covers both the definition and the punishment for defamation.)
3. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 343, India Code (2023). (Title: Fraudulent cancellation, destruction, etc., of will, authority to adopt, or valuable security)
4. Bharatiya Nyaya Sanhita, No. 45 of 2023, § 344, India Code (2023). (Title: Falsification of accounts)
5. Information Technology Act, No. 21 of 2000, § 65, India Code (2000). (Title: Tampering with computer source documents)
6. Information Technology Act, No. 21 of 2000, § 66, India Code (2000). (Title: Computer related offences)
7. Information Technology Act, No. 21 of 2000, § 66D, India Code (2000). (Title: Punishment for cheating by personation by using computer resource)
8. Information Technology Act, No. 21 of 2000, § 66F, India Code (2000). (Title: Punishment for cyber terrorism)
9. Information Technology Act, No. 21 of 2000, § 67, India Code (2000). (Title: Punishment for publishing or transmitting obscene material in electronic form)
10. Information Technology Act, No. 21 of 2000, § 69, India Code (2000). (Title: Power to issue directions for interception or monitoring or decryption of any information through any computer resource)
11. Information Technology Act, No. 21 of 2000, § 43A, India Code (2000). (Title: Compensation for failure to protect data)
12. Pune court convicts 11 accused in Cosmos Bank cyber fraud case, HINDU (Apr. 23, 2023). (A news report confirming the conviction details)
13. Kavita Rani, Cybercrime and Legal Responses in the Indian Jurisdiction, 1 Indian J. L. 35, 38 (2023).