International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Cybercrimes and the Legal Framework of India

Foram Joshi *

Advocate and Cyber Law Advisor.

International Journal of Science and Research Archive, 2025, 17(01), 483-491

Publication history: Received on 03 September 2025; revised on 11 October 2025; accepted on 13 October 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.1.2812

Abstract

In the era of digitalization, cyberspace has become a domain of innovation, connectivity, and convenience, but also of evolving threats. Cybercrimes are rising in frequency, complexity, and impact in India, targeting individuals, businesses, and state infrastructure. This research explores the landscape of cybercrime in India, examines their modus operandi, and critically assesses the existing legal framework to contain them. Emphasis is placed on landmark judicial pronouncements that have shaped jurisprudence, and on the societal implications of cyber threats. Based on gaps and challenges, this paper proposes recommendations to strengthen prevention, enforcement, and public awareness. The research draws on secondary data, legal analysis, and graphical depiction of trends to inform policymakers, legal scholars, and practitioners.

Keywords: Cybercrime; India; Information Technology Act; Digital evidence; Landmark judgments; Legal reforms

1. Introduction

The penetration of the internet, mobile devices, and digital services in India has grown explosively over the past two decades. India's push toward the Digital India programme, the increasing adoption of e-commerce, online banking, digital payments, and remote services have exposed more citizens and infrastructure to cyber vulnerabilities. While digital transformation drives socioeconomic progress, it simultaneously expands the attack surface for malicious actors. Cybercrimes encompass a wide array of offenses (fraud, identity theft, harassment, hacking, ransomware, phishing, etc.) that exploit system vulnerabilities, human psychology, or regulatory gaps.

India has witnessed a steady rise in reported cybercrime cases. For instance, National Crime Records Bureau (NCRB) data and other sources show that cybercrime registrations have surged sharply (see Figure above). The legal architecture — especially the Information Technology Act, 2000 (and its amendments) — together with provisions of the Indian Penal Code (IPC) and the Evidence Act, provide a baseline enforcement regime. However, enforcement, capacity, legal clarity, cross-border cooperation, and awareness remain significant challenges.

This paper seeks to map the evolving threats, analyze the strengths and gaps in the legal framework, and present actionable suggestions to bolster India's cyber resilience.

1.1. Problem Statement

Despite legislative efforts and institutional mechanisms, India faces the following core problems:

- Rising incidence and sophistication: Cybercrime is growing faster than law enforcement capacities, with novel techniques (social engineering, deepfakes, ransomware-as-a-service, cloud attacks).

* Corresponding author: Mrs. Foram Joshi, Advocate and Cyber Law Advisor

- Legal gaps and ambiguities: Some offenses, jurisdictional issues, cross-border data access, and intermediary liability are not clearly addressed or litigated.
- Evidence collection and admissibility: Challenges around chain of custody, forensic capacity, and admissibility (especially of electronic evidence) hamper convictions.
- Low conviction rates and enforcement hurdles: Even when cases are registered, many stall due to procedural delays or weak investigations.
- Public awareness, capacity building, and institutional lacunae: Many victims don't report crimes, and law enforcement agencies may lack cyber forensic infrastructure or trained personnel.
- Transnational nature: Cybercrimes often transcend national borders, complicating cooperation, mutual legal assistance, and jurisdiction.

Thus, the core question is: To what extent does India's existing legal framework address the evolving nature of cybercrimes, and how can gaps be mitigated to improve prevention, enforcement, and justice?

1.2. Research Objectives

- To classify and map the major types of cybercrimes and their modus operandi in India.
- To examine the existing legal statutes, rules, and judicial interpretations relevant to cybercrimes in India.
- To analyze landmark judgments that have shaped cyber jurisprudence.
- To evaluate enforcement challenges, gaps, and institutional constraints.
- To propose policy, legal, and procedural reforms to strengthen India's cyber regime.
- To assess the societal implications of cyber threats and the need for public awareness.

2. Literature Review

A number of prior studies and surveys have examined the trajectory of cybercrime in India, the efficacy of legal responses, and comparative international best practices. A recent paper titled "A Comprehensive Survey of Cybercrimes in India Over the Last Decade" (Tripathy, 2025) reviews threat trends, typologies, and challenges in prosecution in India.

Other works emphasize the gap between legal provisions and ground enforcement capabilities, the need for advanced forensic frameworks, and improving digital literacy among users. Some focus particularly on cloud forensics and the challenges of evolving infrastructure (e.g., in Internet-of-Things domains).

Studies also highlight the interplay of constitutional rights (privacy, free speech) with cybersecurity regulation. The landmark Supreme Court decision in K.S. Puttaswamy v. Union of India (2017) affirmed the constitutional status of privacy, thereby pressing the need for robust data protection regimes.

Critical reviews point out that despite the proliferation of cybercrime, conviction rates are low, and many cases languish due to cross-jurisdictional, procedural, or technical hurdles. Some scholars suggest that the legal design (such as the safe harbor for intermediaries) needs refinement, and greater synergy between public, private, and academic actors is essential.

In sum, the literature broadly converges on three themes: (i) cybercrime is rapidly evolving and outpacing enforcement, (ii) legal frameworks have foundational strengths but suffer from ambiguities and enforcement gaps, and (iii) reform must incorporate technical, procedural, and capacity dimensions. This paper builds on these studies by combining doctrinal, empirical, and policy analysis, and suggesting a refined roadmap for India's cyber regime.

3. Cybercrimes and Their Modus Operandi in India

This section classifies various cybercrime types prevalent in India and outlines how they are executed (modus operandi).

3.1. Classification of Cybercrimes

- While classification schemes vary, a working typology can be:
- Crimes against persons / reputation: cyber harassment, stalking, defamation, cyberbullying.
- Financial and property crimes: online fraud, phishing, identity theft, credit card fraud, ransomware, business email compromise.

- Crimes targeting systems / infrastructure: hacking, denial-of-service attacks, malware, intrusion, system sabotage.
- Crimes involving content and intermediary misuse: distribution of obscene material, child pornography, content violations, illegal deepfake, domain abuse.
- Cyber terrorism, espionage, state-level attacks: attacks on critical infrastructure, data theft, ransomware directed at public utilities or government systems.

3.2. Modus Operandi and Techniques

- Social engineering and phishing: Attackers masquerade as trusted entities (e.g., banks) to trick individuals into sharing credentials or clicking malicious links.
- Malware / ransomware deployment: Using trojans, worms, or exploit kits to gain system control, encrypt data, and demand ransom.
- Credential stuffing / brute forcing: Using automated scripts or lists of leaked passwords to break into accounts.
- Man-in-the-middle (MitM) attacks: Intercepting communications between users and services to eavesdrop or manipulate data.
- Distributed Denial-of-Service (DDoS): Flooding a server with requests to make it unavailable.
- Website defacement / SQL injection: Exploiting web inputs to insert malicious SQL commands or deface content.
- Cloud attacks / server misconfigurations: Exploiting misconfigured cloud storage, APIs, or containers.
- Impersonation / identity theft: Creating fake profiles, using forged documents, or hijacking accounts.
- Deepfake / synthetic media: Creating manipulated audio/video to defame or blackmail individuals/organizations.
- Use of anonymization / botnets: Hiding origin of attacks via proxies, Tor, botnets, or compromised devices.
- Pharming / DNS hijacking: Redirecting legitimate domains to malicious servers.

3.3. Trends and Observations

From secondary sources and NCRB data, cybercrime cases in India have shown a steep upward trend (see Figure above). The shift is toward more complex, multi-vector attacks, including ransomware, supply chain attacks, and cloud intrusion. In 2021, India recorded ~52,974 cybercrime incidents, showing a ~6% annual increase.

Emerging threats include Internet-of-Things (IoT) abuse, AI-powered phishing, and zero-day exploits. Attackers now operate transnationally, accessing Indian hosts from outside and complicating jurisdictional control.

4. Laws, Provisions, and Legal Framework to Curb Cybercrimes in India

This section outlines the principal statutes, rules, and legal mechanisms India uses to regulate and prosecute cybercrimes.

4.1. Primary Statutes

4.1.1. Information Technology Act, 2000 (IT Act) and amendments

The IT Act is the primary statute for cyber law in India. It provides definitions of electronic records, digital signatures, and establishes various offenses and penalties (e.g., Section 66, 66A, 66B, 66C, 66D, 66E, 67, 69).

Amended in 2008 to include more cyber offenses and to introduce intermediary liability provisions and the concept of "reasonable security practices."

The IT (Amendment) Act added section 69 (power to intercept, block, decrypt), 69A (blocking for public interest), 69B (monitoring), and Section 79 (safe harbor for intermediaries).

The CERT-In (Indian Computer Emergency Response Team) is empowered under the IT Act (especially through rules) to mandate reporting of cybersecurity incidents.in

4.2. Bharatiya Nyaya Sanhita, 2023

Table 1 Sections related to Cyber Crimes (BNS 2023)

Provision	Subject	Notes
Section 75	Sexual harassment (including using electronic means)	BNS specifically includes acts committed by showing pornography against someone's will or making sexually coloured remarks via electronic means.
Section 77	Voyeurism	Applies to capturing or disseminating private images (often in digital / cyber contexts) without consent.
Section 78	Stalking	Cyberstalking (monitoring, following online activities) falls under this provision.
Section 79	Outraging modesty (by words, gestures or display)	Can apply to online harassment, "electronic form" insults, deepfakes, etc.
Section 111	Organised crime (continuing unlawful activity)	BNS explicitly includes cyber-crimes among the kinds of activities covered under Section 111.
Other sections	Defamation via electronic means	E.g. BNS Section 356 is said to penalize defamation including by email / electronic transmission.
Forgery / Reputation harm	BNS Section 336 (forgery harming reputation)	Digitally forged documents / images may be covered under this.

4.2.1. Bharatiya Sakshya Adhiniyam, 2023

Table 2 Sections related to Cyber Crimes (BSA 2023)

Provision	Subject	Notes
Section 61	Admissibility of electronic / digital records	States that just because something is in electronic form doesn't mean it is inadmissible.
Section 62	Contents of electronic records — proof	Provides that contents of electronic records can be proved in accordance with Section 63.
Section 63	Admissibility of electronic records / computer output	Lays down conditions under which electronic evidence (computer outputs, communication device outputs) is admissible, along with certificate requirements.
Section 63(4)(c)	Certificate requirement for electronic evidence	The "certificate" requirement (somewhat akin to old Section 65B) is part of this section.
Section 73	Proof of digital signature	Section 73 deals with how a digital signature is to be proved.

4.2.2. Rules and subordinate legislation

- Information Technology (Intermediaries Guidelines) Rules, 2011
- IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- CERT-In Rules (various rules requiring reporting, log retention, network security)
- Additional rules (e.g., blocking rules, etc.)

4.2.3. Data protection and privacy laws

Though India currently lacks a comprehensive data protection statute (until recently), the Digital Personal Data Protection Act, 2023 (DPDP Act) introduces obligations for data fiduciaries (data controllers), rights to data principals, and penalties for misuse.

The DPDP Act complements cyber laws by regulating collection, storage, processing, and retention of personal data.

4.3. Key Provisions, Liability, and Enforcement

- Safe Harbor (Section 79): Intermediaries (e.g., platforms, ISPs) are shielded from liability for third-party content if they follow due diligence and remove disputed content upon receiving court orders or government takedown notices.
- Interception and blocking powers (Sections 69, 69A): The government may block or intercept content for reasons including sovereignty, integrity, public order, or prevention of incitement.
- Penalties and offenses: The IT Act prescribes monetary and imprisonment penalties (e.g., up to 3 years, fines) for various offenses like identity theft, hacking, misrepresentation, publishing obscene material, etc.
- Incident reporting obligations: CERT-In rules mandate certain entities to report cybersecurity incidents within defined timeframes.
- Procedural mechanisms: Authorities can issue search and seizure orders, freeze bank accounts, obtain interception orders, and cooperate with foreign agencies.
- Judicial oversight and appeals: Affected persons can challenge blocking orders, takedowns, or interception via judicial review.
- Mutual Legal Assistance Treaties (MLATs) and international cooperation: India has signed MLATs and participates in treaties (e.g., Budapest Convention) via bilateral cooperation (though India is not a party to the Budapest Convention).

4.4. Gaps and Challenges in the Legal Regime

- Ambiguities and overlaps: Some provisions (e.g., “due diligence”, “reasonable security practices”, “sensitive personal data”) are not clearly defined or remain subject to jurisprudence.
- Jurisdictional and cross-border issues: The law does not fully resolve how to enforce takedowns or investigations when servers or perpetrators lie outside India.
- Admissibility and certificate constraints: Section 65B provisions are sometimes rigid and courts differ in applying them, especially around the need for a “certificate” and availability of original.
- Enforcement capacity: Many police stations lack trained cyber investigators, forensic labs, or equipment.
- Low awareness and underreporting: Many victims are unaware or reluctant to report cybercrimes, fearing complexities.
- Delay and procedural backlog: Investigations and prosecutions often suffer from delays, weakening the deterrence effect.
- Lack of proactive regulation: The framework is largely reactive; there is limited regulation on proactive cybersecurity obligations (e.g., mandatory audits for critical infrastructure).

5. Landmark Judgments on Cybercrime Cases in India

Judicial decisions have played a critical role in interpreting, refining, or invalidating statutory provisions related to cybercrimes. Below are a few landmark cases (not exhaustive).

5.1. Shreya Singhal v. Union of India (2015)

In this seminal judgment, the Supreme Court struck down Section 66A of the IT Act (which criminalized “offensive or menacing” messages) as unconstitutional, violating free speech under Article 19(1)(a). The court also read down Section 79 (intermediary immunity) and Rules under it, to require that takedown orders be accompanied by court or governmental directives rather than allowing arbitrary removal.

This judgment significantly shaped India's approach to intermediary liability, online free speech, and due process in content takedowns.

5.2. Suhas Katti v. Tamil Nadu (2004)

This was the first conviction in India for cyber harassment and obscene messages over the internet, under Section 67 of the IT Act and relevant IPC sections. The court accepted electronic evidence under Section 65B (Indian Evidence Act) and treated emails and fake accounts as forgery and defamation, awarding prison terms and fines.

It also recognized the role of intermediaries (e.g. cyber cafés) in maintaining visitor logs and records.

5.3. Aveek Sarkar v. State of West Bengal (2014)

Though not strictly a cybercrime case, this SC decision overruled the Hicklin test for obscenity (used since Ranjit D. Udeshi) and endorsed a community standards test for determining obscenity. This has relevance for online content regulation and judgments involving digital media.

5.4. K.S. Puttaswamy v. Union of India (2017)

This constitutional bench judgment affirmed that the right to privacy is a fundamental right under Articles 14, 19, and 21. This is a touchstone decision insofar as data protection, surveillance, and balancing cybersecurity powers with individual privacy rights are concerned.

5.5. Additional Cases

Other significant cases include Sabu Mathew George v. Union of India (addressing search engine regulation, content takedown) , SMC Pneumatics v. Jogesh Kwatra (on intermediary liability), Avnish Bajaj v. State (NCT Delhi) (on e-commerce liability), and CBI v. Arif Azim (Sony Sambandh case).

Collectively, these judgments have clarified constitutional constraints, intermediary liability, privacy protections, the validity of digital evidence, and the normative contours of content regulation in cyberspace.Cyber criminals are employing artificial intelligence and machine learning to create smarter phishing attacks, automate fraud detection evasion, and conduct large-scale data breaches.

6. Societal Implications

Cybercrimes impact individuals, businesses, institutions, and the broader social fabric in multiple ways.

6.1. Impact on Individuals

- Financial losses: Victims lose money through fraud, phishing, or account takeover.
- Reputational harm: Defamation, leaked private content, or misuse of personal images can cause lasting social damage.
- Psychological distress: Harassment, cyberbullying, identity theft generate stress, anxiety, and fear.
- Violation of privacy and autonomy: Unauthorized access, data breaches, or surveillance infringe on personal dignity.

6.2. Impact on Businesses and Economy

- Operational disruption: Ransomware attacks or system intrusions can paralyze businesses.
- Loss of trust and customers: A data breach diminishes consumer confidence and brand reputation.
- Cost of compliance and remediation: Firms must invest in cybersecurity, audits, insurance, and incident response.
- Innovation deterrence: Excessive liability or litigation can inhibit digital transformation.

6.3. Public Institutions and Infrastructure

- Risks to critical infrastructure: Cyberattacks on power grids, transportation, health systems, or government services can have severe consequences.
- Governance and trust: Data leaks or misuse by government systems can erode citizens' trust.
- Digital divide and inequality: Underprivileged communities may be more vulnerable due to lower awareness or resources for protection.

6.4. Legal, Ethical, and Policy Concerns

- Balance between security and rights: Interception and surveillance powers must be balanced against individual privacy.
- Chilling effect on speech: Overbroad takedown rules or liability may stifle free expression and dissent.
- Exclusion of marginalized voices: Vulnerable populations may find it harder to access remedies or understand legal recourse.
- Global asymmetry: Indian citizens may be targeted from foreign jurisdictions, while Indian laws may struggle to reach them.

Thus, the societal stakes are high: cybercrime undermines trust in digital systems and can reverse the gains of the digital revolution, unless effective law, policy, and institutional architecture keep pace.

7. Recommendations

Based on the foregoing analysis, the following recommendations are proposed to strengthen India's cyber law regime.

7.1. Legal and Policy Reforms

- Clarify and update definitions: Provide explicit definitions for "due diligence," "sensitive data," "reasonable security practices," and "intermediary."
- Strengthen proactive obligations: Mandate regular security audits, vulnerability disclosures, and minimum cybersecurity standards for critical sectors (e.g., finance, health, infrastructure).
- Revise intermediary liability: Calibrate safe harbor rules to encourage responsible behavior without undue burden — for instance, prompt takedown upon proper notice, transparency in decision-making, and accountability.
- Facilitate cross-border cooperation: Strengthen mutual legal assistance (MLAT) mechanisms, negotiate bilateral data access treaties, and consider joining international conventions (e.g. Budapest Convention) or a cybercrime protocol.
- Modernize evidence rules: Make Section 65B more flexible (e.g., allowing metadata, backups, and proofs of integrity), reduce strict certificate formalism, and provide judicial guidelines for digital evidence.
- Expedite adjudication: Create fast-track cyber courts or special benches to reduce delays in cybercrime trials.
- Safe reporting and whistleblower frameworks: Encourage victims and security professionals to report incidents with legal protections and anonymity.
- Incorporate emerging threats: Legislate against AI-driven attacks, deepfakes, algorithmic offenses, cryptocurrency-based fraud, and data poisoning.

7.2. Institutional and Capacity Building

- Enhanced forensic infrastructure: Expand and upgrade digital forensic labs across states with standardization, certification, and inter-lab networking.
- Training and specialization: Invest in specialized training for police, prosecutors, and judges on cyber investigations, digital evidence, and new threat vectors.
- Regional and state coordination: Establish cyber command centres in states (similar to Karnataka's initiative) to streamline investigations across districts. (Note: Karnataka HC recently underscored the need for a strong Cyber Command Centre)
- Public-private partnerships (PPP): Encourage sharing of threat intelligence, joint incident response, and capacity augmentation with industry, academia, and startups.
- Awareness campaigns: Conduct large-scale public education, especially among vulnerable groups (elderly, rural users), about phishing, safe browsing, and reporting mechanisms.
- Victim support and remediation: Provide victim counseling, helplines, and legal aid specifically for cybercrime victims.

7.3. Technological and Research Measures

- Threat intelligence and situational awareness: Establish a national cyber threat intelligence platform to collect, analyze, and disseminate real-time alerts to stakeholders.
- Use of AI and automation: Deploy AI to detect anomalies, spam, phishing, and early warning signals.
- Blockchain or tamper-evident logging: Use immutable logging for key systems to aid forensic integrity.
- Encourage academic research and pilot projects: Incentivize universities and research labs to test novel defenses, attack simulations, and forensic tools.

7.4. Monitoring and Evaluation

- Impact metrics: Define clear KPIs (e.g., case resolution time, conviction rate, reporting rate) and publish annual performance reports.
- Periodic review of laws: Establish a periodic legislative review committee to assess new threats, legal adequacy, and emerging technologies.
- International benchmarking: Compare India's cybercrime statutes and enforcement outcomes with peer jurisdictions to adopt best practices.

By combining legal modernization, capacity building, technological adoption, stakeholder collaboration, and continuous evaluation, India can strengthen its cyber resilience.

8. Conclusion

India finds itself at a crossroads: digital expansion promises vast socioeconomic benefits but also exposes citizens and infrastructure to growing cyber risks. The upward trend in cybercrime, as shown in national statistics, underscores the urgency of a robust and adaptive response.

The existing legal framework — comprising the IT Act, IPC, and Evidence Act — provides a foundational bedrock, and judicial decisions (such as Shreya Singhal, Suhas Katti) have helped temper statutory excesses and define key contours. However, gaps remain in clarity, enforcement, cross-border reach, forensic readiness, and balancing rights with security.

Addressing these challenges requires a holistic approach: updating legislation, empowering institutions, building forensic and investigative capacity, leveraging technology, promoting public awareness, and fostering cooperation across sectors and borders. The recommendations offered here — if adopted and implemented — can significantly strengthen India's deterrence, response, and justice mechanisms in cyberspace.

As cyber threats evolve rapidly, India must avoid complacency. Legal frameworks must evolve dynamically, institutions must stay agile, and all stakeholders (government, industry, civil society, and citizens) must collaborate in creating a resilient cyberspace. Only then can the promise of digital transformation be safeguarded against the perils of the cyber frontier.

Compliance with ethical standards

Acknowledgments

I would like to express my sincere gratitude to all the individuals and organizations that have contributed to the publication of this research paper.

First and foremost, I would like to thank my mentor Shri D D Joshi, Cyber Crime Investigator, Cyber Professional and Research Scholar as well for his invaluable guidance and support throughout the research process. His expertise and insights were instrumental in shaping the direction and focus of my research. I am also grateful to the officials of Judiciary and Lower Courts, District Courts and High court for providing me with the resources and support I needed to complete this paper.

I would also like to thank my Senior Advocates and colleagues at my work places for their feedback and support throughout the research process. In particular, I would like to thank my family members for morale support. Finally, I would like to thank all the participants in this study for their time and willingness to share their experiences. Their contributions have been invaluable in helping me to understand the topic and draw meaningful conclusions.

References

[1] Avnish Bajaj v. State (NCT of Delhi), 150 (2008) DLT 769.

[2] Aveek Sarkar v. State of West Bengal, (2014) 4 SCC 257.

[3] Central Bureau of Investigation v. Arif Azim, (2008) CriLJ 3311 (Delhi).

[4] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, Government of India.

[5] Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, Government of India.

[6] Information Technology (Amendment) Act, 2008, No. 10 of 2009, Acts of Parliament, Government of India.

[7] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India.

[8] Karnataka High Court. (2024). Judgment on establishment of cyber command centres [Unreported case reference].

[9] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[10] National Crime Records Bureau (NCRB). (2023). Crime in India 2022: Statistics. Ministry of Home Affairs, Government Sabu Mathew George v. Union of India, (2017) 5 SCC 360.

[11] Shreya Singhal v. Union of India, (2015) 5 SCC 1.

[12] Suhas Katti v. State of Tamil Nadu, (2004) 1 CTC 565.

[13] SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, (2002) (Delhi High Court).

[14] Tripathy, R. (2025). A comprehensive survey of cybercrimes in India over the last decade.

[15] Indian Journal of Cyber CERT-In. (2022). Rules and Guidelines for Reporting of Cybersecurity Incidents. Ministry of Electronics and Information

[16] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, Government of India.

[17] Bharatiya Sakshya Adhiniyam, 2023, No. 46 of 2023, Acts of Parliament, Government of India.

Author's short Biography

An author is a practising Advocate at District-Metropolitan Courts and lower courts including Labour courts, Consumer Disputes Redressal Commission, etc. She also practices in the Honourable High Court of Gujarat. She emphasizes on the cases pertaining to Cyber Crimes, Cyber investigations, Cyber law procedures. She possesses specialized qualifications in Cyber Laws & Investigations in addition to the degrees of BTS, LLB, and LLM. Her focused aim of Advocacy to address the issues of Cyber victims and the mitigating cybercrimes from the society.