LEGAL AMENITY LAW JOURNAL – ISSN 3107-9148

Volume II Issue II March – April 2026

THE RISE OF CYBERCRIME: CHALLENGES TO ONLINE SAFETY IN INDIA

By: - Ishi Kumari Mahto

Law Student, KLE College of Law, Kalamboli

ABSTRACT

The quick development of digital technology has changed India's social and economic landscape, bringing with it both previously unheard-of opportunities and difficulties. The surge in cybercrime poses serious risks to national security, individual privacy, and online safety. This article explores the effects of cybercrime on individuals, organizations, and society at large in India. The backdrop and importance of cybercrime in India's digital era are first discussed in this article. After covering current legislation, noteworthy instances, and earlier studies on cybercrime, a thorough literature analysis highlights the challenges of combating this dynamic menace. The various forms of cybercrimes, such as phishing, hacking, identity theft, cyberstalking, and financial fraud, are then mapped in India. Examining the effects of cybercrime reveals the disastrous effects on people, businesses, and the economy, including monetary losses, harm to one's reputation, and endangered personal safety. The essay also examines how cybercrimes compromise social safety by fostering mistrust, anxiety, and terror in the online environment. Potential legal loopholes, difficulties for law enforcement, and social and technological elements that fuel cybercrime are all identified via a thorough examination of cyber issues. The paper emphasizes the necessity of a strong and flexible cybersecurity strategy that takes into account new threats and weaknesses. The article describes organizational and individual procedures to improve internet safety. Its goal is to enable people and organizations to defend themselves against online dangers. The article's conclusion acknowledges the necessity of a multi-stakeholder strategy to fight cybercrime and suggests tougher legislation, improved cooperation, and funding for cybersecurity education and technology. India can create a safe and robust digital ecosystem that protects its population by taking aggressive measures to address these issues.

Keywords: Cybercrime, Online Safety, India Digital Technologies, Cyber Security, Cyber Threats, Challenges, Cyber Laws, Regulations, Law enforcement, Digital Literacy Data, Cybercrime Prevention.

INTRODUCTION

With more than 600 million active users and an expanding e-commerce market expected to reach $200 billion by 2025, India's digital revolution has been nothing short of extraordinary. But this quick expansion has also made the nation vulnerable to a wide range of cyberthreats, making internet safety a critical issue. Phishing, hacking, and online harassment are examples of cybercrime, which has grown to be a serious problem for people, companies, and the government. Financial losses, harm to one's reputation, and psychological pain are only a few of the serious repercussions. India is a prime target for cyberattacks due to the absence of efficient cyber security measures, an inadequate regulatory framework, and low awareness levels that have empowered hackers.

Additionally, the growing usage of digital platforms for social interactions, e-governance, and financial transactions has led to the creation of new vulnerabilities that cybercriminals can exploit. In light of this, it is critical to assess India's internet safety issues and investigate ways to lessen these risks. By examining the present level of cybercrime in India and emphasizing the necessity of a strong cyber security ecosystem, efficient law enforcement, and individual accountability, this paper aims to add to this important discussion.

LITERATURE REVIEW

Online safety in India is severely hampered by the surge in cybercrime, despite numerous laws and regulations being in place to combat these problems. An overview of pertinent laws, cases, and research is provided below.

Laws:

- **Information Technology Act, 2000 (IT Act)**: India's main cybercrime laws address internet fraud, identity theft, data theft, and unlawful access.
- **Indian Panel Code (IPC):** Cybercrimes such as identity theft and cheating forgery are covered by Sections 420, 465, 467, and 471.

- **CERT-In Cyber Security Directions, 2022:** Six of these guidelines require incident reporting, 180-day log retention, and KYC for service providers.
- **Digital Personal Data Protection Act 2023:** controls privacy and data protection.

Notable Cases:

- **Shreya Singhal v. Union of India (2015):** The Supreme Court struck down Section 66 A of the Information Technology Act declaring it unconstitutional for being vague and overbroad, violating freedom of speech. The court held that the provision had a chilling effect on re speech and lacked a reasonable restriction under Article 19 (2). The decision emphasizes the importance of protecting online free speech.
- **Ratan Tata v. Union of India (2015):** An investigation into a fraudulent email scheme that highlights identity theft risks was ordered by the Bombay High Court.
- **State of Tamil Nadu v. Suhas Katti (2004):** This case involved a conviction under section 67 of the IT Act for posting obscene content online. The court held that the accused was guilty of publishing obscene material, emphasizing the need protect society from such content.
- **Kalandi Charan Lenka v. State of Odisha (2017):** The High Court of Odisha addressed a cyberstalking and online harassment.
- **Poona Auto Ancillaries Pvt. Ltd. V. Punjab National Bank (2018):** PNB was ordered by the IT Department to compensate a victim of phishing email scam with Rs. 45 lakhs.

Previous Researches:

- Cybercrime cases increased by 24.38% in 2022 compared to 2021, according to a National Crimes Record Bureau (NCRB) study.
- The number of cybercrimes reported by the Indian Cyber Crime Coordination Center (I4C) increased from 10.29 lakh in 2022 to 22.68 lakh in 2024.
- Research identifies deep fit technology and social engineering scams as emerging issues.

CYBERCRIME LANDSCAPE IN INDIA

Types of Cyber Crime:

1. **Phishing**: is the practice of deceiving victims into disclosing private information through fake emails or websites. Attackers frequently pose as reputable organizations in order to obtain financial information or passwords.
2. **Hacking**: Unauthorized access to systems, networks, or data is known as hacking. It is frequently done maliciously, taking advantage of weaknesses to steal data or interfere with operations for financial gain, espionage, or fame.
3. **Online harassment**: Cyberstalking, bullying, and threats via online platforms are all included. Victims may experience physical harm, reputational harm, or emotional grief. Perpetrators frequently use anonymity to hide.
4. **Data Breach**: Unauthorized access to or exposure of sensitive data is known as a data breach. Hacking or unintentional breaches can occur. Identity theft, financial loss, and harm to one's reputation are among the repercussions.
5. **Identity Theft**: It entails using someone's identity for malicious or financial advantage. Thieves take personal information, seek for credit, or carry out illegal activities.
6. **Ransomware**: Is a type of malicious software malware designed to block access to a computer system or files until a sum of money is paid. It essentially kidnaps your digital data and hold it for ransom.
7. **Cyber Extortion**: Is a broad category of digital crime where attackers demand money or other consensus by threatening to harm you your business or your reputation. Unlike a simple hack it involves a direct threat used as leverage.
8. **Online Fraud**: It includes scams via e-commerce payment gateways or financial platforms. Scammers deceive victims into transferring money or relieving sensitive information.
9. **Spoofing**: Spoofing is impersonating legitimate entities (emails websites or calls). It often perceives phishing or financial fraud.

10. **Cyber Stalking**: Cyberstalking is defined as persistent online harassment, surveillance, or threats that includes tracking online activity, sending unwanted messages, and perhaps escalating to physical harm or offline stalking.
11. **Crypto jacking**: It is the unapproved use of a person's or company's computer resources to mine cryptocurrency. Hackers usually use a malicious link in an email or JavaScript code embedded into a webpage to infect a device.
12. **DDOS Attack (Disturbed Daniel of Service)**: Overloading a website or network with fake traffic making it unavailable to users.

Consequences of Cybercrime:

1. **Erosion of trust**: Reluctance to embrace new technologies or online platforms, a decline in the growth of e-commerce and digital payments, a lack of trust in digital services and online transactions, and a rise in cynicism regarding data security and online safety precautions.
2. **Financial losses**: Direct cash theft from wallets or bank accounts, income loss from website outages or data breaches, the expense of fixing and securing compromises, and possible legal and regulatory increases in business insurance premiums.
3. **Comprised Personal Data**: Financial fraud and identity theft, illegal use of personal data for malicious intent, data misuse for phishing, spam, or blackmail, and long-term harm to one's reputation.
4. **National Security Threats**: Theft of private government information, espionage, and compromise of vital infrastructure (electricity grids, health care, etc.) Potential for terrorism or cyberwarfare, interruption of vital services, and public utilities.
5. **Psychological impact:** Long-term mental health problems may result from victims of online harassment experiencing emotional pain and trauma, anxiety, tension, and dread of online interactions, as well as a lack of trust in digital services and technology.

Cybercrimes Impact on Online Safety:

1. **Insecure Online Transactions**: Malware, phishing, and hacking make online transactions dangerous, discouraging users from utilizing digital services.
2. **Toxic Online Environment**: Cybercrimes that impair mental health and freedom of expression include online harassment and cyberstalking, which create a hostile online environment.
3. **Loss of Trust**: Frequent cybercrimes undermine confidence in digital systems, impeding their uptake and expansion.
4. **Increase Vulnerability**: Cybercrimes take use of system flaws, leaving them vulnerable to additional attacks and jeopardizing online security.

ANALYSIS OF CYBERCRIME CHALLENGES

Potential Gaps in existing laws and regulations:

Inadequate Definitions and Coverage: Cybercrimes are changing quickly, and current laws may not adequately describe or cover all forms of cybercrimes. This can cause misunderstanding among judges, law enforcement, and individuals, making it difficult to successfully prosecute cybercrimes. For example, new forms of cybercrimes that may not be specifically covered by current laws have emerged as a result of emerging technologies like AI block chain and IoT. Therefore, offenders may take advantage of these gaps to avoid accountability.

Jurisdiction Issues: Because cybercrimes frequently cross national borders, it can be difficult to establish jurisdiction and bring criminals to justice. Conflicts between the legal and regulatory systems of many nations may result from this, delaying and complicating the prosecution of offenders. For instance, a cybercrime that is committed in one nation may be prosecuted differently in another, resulting in uneven results. To solve these jurisdictional issues, international corporations and harmonization are crucial.

Lack of Harmonization: It is challenging to collaborate and coordinate efforts to combat cybercrime because different nations have different laws and regulations. Cybercriminals may choose to conduct crimes in jurisdictions with laxer rules or enforcement as a result of taking

advantage of these disparities. Global law and regulation harmonization can assist guarantee that cybercrimes are dealt with consistently and successfully.

Insufficient Penalties: Laws may not adequately compensate victims, and current punishments may not be harsh enough to discourage cybercrimes. For example, fines or imprisonments may be insufficient to discourage hackers, who may see them as a small expense of conducting business. Cybercrimes can be discouraged and accountability increased by stiffening penalties and giving victims fair recompense.

Outdated laws: Current legislation might be out of date and fail to take into consideration new technologies like block chain, artificial intelligence, and the Internet of Things. It might be difficult to apply current rules to new technology as a result of stakeholder uncertainty and confusion. Laws can be kept current and efficient in combating cybercrimes by being updated to take into account new technologies.

Lack of clarity on data protection: It may be difficult to hold companies responsible for data breaches if laws do not specify data protection requirements. This may result in uneven data security procedures, jeopardizing people's privacy and personal information. Data security and confidence in digital services can be fostered by making data protection regulations clear and holding companies responsible.

Law Enforcement Challenges:

- **Limited Resources:** Law enforcement organizations frequently lack the resources—money, manpower, and technology (needed to properly look into and punish cybercrimes).
- **Lack of Expertise**: It is challenging to prosecute cybercrimes because many law enforcement organizations lack the particular expertise and abilities needed for these offenses.
- **Anonymity and Encryption**: Law enforcement authorities find it challenging to track and identify cybercriminals because they frequently use anonymity tools and methods to conceal their identity and actions.

- **Lack of reporting**: Since many cybercrimes go unreported, it is challenging to compile information and statistics and create practical countermeasures.

Technological and social factors contributing to Cybercrime:

- **Increasing connectivity and dependence on technology**: The increasing number of internet-connected devices has given cybercriminals greater chances to take advantage of weaknesses and commit crimes. People are more susceptible to cyberattacks as they grow more reliant on technology.
- **Emerging technologies and Lack of Awareness:** Many individuals are ignorant of the threats connected to emerging technologies like AI, block chain, and IoT, which have opened up new channels for cybercrimes. Cybercriminals can more easily take advantage of these technology because of this ignorance.
- **Malware, Ransomware and Social Engineering:** The sophistication of ransomware and malware has increased, making it simpler for cybercriminals to perpetrate crimes and demand money from victims. Cybercriminals frequently employ social engineering techniques to trick people into disclosing private information or carrying out specific tasks by taking advantage of human psychology and behaviour.
- **Cybercrime-as-a-Service and Online Platforms:** Cybercriminals now have an easier time committing crimes since they can rent or purchase malware and other tools online because to the growth of cybercrime as a service models. Additionally, ransomware, phishing scams, and other cyber threats can be disseminated through online platforms and social media.
- **Lack of Digital Literacy and Skills:** Many people are at risk from cybercriminals because they lack the digital literacy and skills necessary to protect themselves online. People who lack these skills may use weak passwords, click on ads, and engage in other harmful internet actions.

MEASURES TO ENHANCE ONLINE SAFETY

Individual Precautions:

Online Hygiene:

- To create and save complicated passwords, use a password manager.
- Whenever feasible turn on boot factor stations (2FA).
- Update operating systems browsers and applications on a regular basis.
- Make use of a firewall and a reliable antivirus program.
- When opening documents or accessing links from unidentified sources, use caution.

Personal Data Management:

- Restrict the amount of personal data you disclose on social media.
- Privacy options to manage information access.
- Exercise caution while giving websites or apps personal information.
- Utilize a credit monitoring service to keep tabs on questionable activities.

Safe Online Practices:

- Use secure networks (HTTPS) for online transactions.
- Avoid using public Wi-Fi for sensitive activities.
- Use VPN when using public Wi-Fi.
- Watch out for unwanted emails and phishing scams.
- Make use of a secure browser search engine.

Device Security:

- Utilize biometric authentication or a screen log for devices.
- Encrypt private information on devices.
- Make frequent data backups
- When not in use, log out and utilize a safe lock screen.

Online Behaviour:

- Be cautious when meeting people online.
- Don't download programs from unidentified sources.
- Prior to downloading apps, read the conditions and reviews.
- When making purchases online, use a secure payment gateway.

Organizational Measures:

Employee Training and Awareness:

- Employees should receive regular cybersecurity training.
- Phishing simulation and awareness campaigns should be conducted.
- Provide staff with incident reaction and reporting training.
- Encourage staff members to report any questionable activities.

Cyber security protocols

- Put strong security rules and processes into place.
- Update and patch software and systems on a regular basis.
- For sensitive data, use encryption.
- Put multi-factor authentication and access control into practice.
- Make use of secure communication protocols, such as SFTP and HTTPS.

Network Security:

- Install intrusion detection systems and firewalls.
- You protect network standards, such as WPA2 and WPA3.
- Check for vulnerabilities and path systems on a regular basis.
- Put network isolation and segmentation into practice.

Compliance and Governance:

- Regularly review and update security policies and procedures.
- Conduct internal audits and risk assessment.

- Ensure compliance with relevant regulations and standards (eg. GDPR, HIPAA).
- Establish career roles and responsibilities for security personnel.

Third-Party Risk Management:

- Conduct thorough rigs assessments of third-party vendors.
- Implement security requirements for third-party vendors.
- Regularly review and update third-party contracts.
- Monitor third-party vendor security performance.

RECOMMENDATIONS

A comprehensive strategy that goes beyond merely developing reporting tools is needed to address the compelling problem of India's underreporting of cybercrimes. One significant issue is victims' ignorance of what constitutes a cybercrime and how to report it. Thus, it is essential to launch a national awareness campaign that targets rural and semi-urban areas and focuses on educating people about typical cybercrimes including phishing, online fraud, and cyberstalking as well as the channels available for reporting such events. More victims may come forward if the complaint filing process is made easier with user-friendly digital interfaces, such as multilingual chatbots and smartphone apps. In order to handle cybercrime complaints sensitively and effectively while guaranteeing that victims feel supported throughout the process, law enforcement organizations must also have the required training and resources.

The necessity of strong data protection management systems is another urgent problem. India needs a comprehensive data protection law that guarantees data localization, sets obligations for data handlers, and offers remedies for data bridges in light of the country's growing digitization. It should be mandatory for organizations that handle sensitive data to reinstate security measures and swiftly notify authorities and impacted persons in the event of a breach. Additionally, closing the skills gap in cybersecurity is essential for India's digital development. This can be accomplished by incorporating cyber security education into college and school curricula, encouraging industry-academia collaborations for skill development, and providing cyber security experts with incentives and certifications. These talent shortages can also be

addressed by encouraging women and underrepresented groups to pursue careers in cybersecurity.

India must also concentrate on encouraging enterprises to have a cultural knowledge of cyber security. Because many SMEs disregard fundamental security procedures, fraudsters can easily target them. The nation's overall cyber resilience can be greatly increased by offering reasonably priced service security solutions and resources designed specifically for SMEs, as well as tax breaks for putting security measures in place.

These steps, along with more robust public-private partnerships for proactive monitoring and threat intelligence sharing, can assist India in more successfully combating the growing wave of cybercrime.

CONCLUSION

The growing threat of cybercrime poses serious implications to national security, business operations, and individual privacy as India continues to spearhead digital transformation and increase its online footprint. By promoting a culture of cybersecurity awareness, establishing regulatory frameworks, and utilizing technology and partnerships, stakeholders (including government agencies, organizations, and individuals) must collaborate to build a secure and resilient digital ecosystem in order to reduce these risks and protect India's digital future. Beyond short-term fixes, India's long-term cybersecurity policy focuses on developing a strong ecosystem that foresees and responds to new threats. This advances research into cutting-edge cybersecurity solutions, such as block chain-based data protection and AI-driven thread detection, while simultaneously encouraging citizen digital literacy. India can turn obstacles into opportunities and guarantee a safe, inclusive, and prosperous digital feature for everyone by including cybersecurity into its story of digital growth. The success and safety of India's digital journey will ultimately depend on our combined efforts in cybersecurity.