Page 2015 - 2024 **DOI:** *https://doij.org/10.10000/IJLMH.1110059*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Cybercrime in India Legal Framework and Enforcement Challenges

TEESHA AGARWAL[1]

ABSTRACT

With the rapid expansion of internet access and digital services across India, cybercrime has emerged as a serious and growing threat. From financial fraud and identity theft to cyber stalking and online harassment, digital offences are affecting not just individuals but businesses and government systems alike. As people increasingly rely on digital platforms for everything from banking to communication, the risks associated with cybercrime have multiplied. India primarily relies on the Information Technology Act, 2000, as its key legal response to cyber offences. This law, alongside relevant provisions of the Indian Penal Code, 1860—such as those dealing with cheating, intimidation, and obscenity—forms the backbone of the country's cybercrime legislation. However, enforcing these laws presents several challenges. A major problem is that law enforcement lacks technical skills. Many officers aren't adequately trained to deal with complex digital evidence or trace cybercriminals who often operate anonymously across borders. The shortage of advanced tools and standardized protocols across states further hampers investigations. Compounding this, the cross-border nature of many cyber offences makes it difficult to pursue legal action or cooperation internationally. Public response to cybercrime is another concern. Many victims, especially those targeted through personal data breaches or online abuse, hesitate to report incidents due to shame, fear, or distrust in the system. The lack of awareness about legal rights and available remedies also discourages people from coming forward. To fix these issues, India needs a better and more united plan. This includes better training for police and judicial officers, modern investigative infrastructure, and more robust cooperation between national and international agencies. At the same time, efforts to raise public awareness about cyber safety—especially among vulnerable groups like women, children, and the elderly—are critical.

I. INTRODUCTION

In recent years, the way we live, work, and communicate in India has changed dramatically, thanks to the rise of digital technology. From paying bills and booking tickets to chatting with friends or running businesses online, the internet has become a part of everyday life. But with

[1] Author is a Student at Mahatma Jyoti Rao Phoole University, India.

 [ISSN 2581-5369]

[2]all these conveniences come new dangers—cybercrime is growing just as fast as our use of technology.

Whether it's someone losing their savings to online fraud, facing harassment on social media, or having their personal data stolen, these crimes are affecting people across the country. As one of the world's largest internet-using populations, India has seen a sharp increase in cyber-related offences. Unfortunately, catching and prosecuting cybercriminals isn't easy. The online world allows offenders to hide behind screens, often from outside our borders, making the job of law enforcement and the courts incredibly tough.

To deal with these challenges, India relies mainly on the Information Technology Act, 2000, supported by parts of the Indian Penal Code. These laws aim to punish online crimes and protect users. However, having laws on paper isn't enough. Many police officers and legal officials aren't trained to handle the technical side of cybercrime, and in many places, the tools needed for proper investigation just isn't there. On top of that, many people still don't know what their rights are or how to report a cybercrime.

This paper takes a closer look at India's cybercrime laws, the challenges in putting them into action, and what we can do to make things better. From improving training and infrastructure to encouraging public awareness, we need a joint effort to build a safer digital space for everyone.

II. HISTORIC BACKGROUND OF CYBER LAW IN INDIA

Public Cybercrime in India has grown alongside the country's digital revolution. Back in the late 1990s, when internet access was still new and limited, incidents of cybercrime were rare and relatively simple—mostly website defacements and basic hacking. But as technology became more accessible and everyday life moved online, the opportunities for digital mischief turned into serious threats. With the rise of online banking, e-commerce, and social media in the early 2000s, cybercrimes quickly evolved in both scale and complexity.

To respond to this growing challenge, the Indian government passed the Information Technology Act, 2000—a landmark move that formally recognized cyber offences and gave legal weight to digital transactions. It was the first structured attempt to tackle issues like hacking, identity theft, and cyber stalking, while also laying the foundation for e-governance and electronic commerce through provisions for digital signatures and contracts.

Still, the law had its limitations. Technology was moving faster than legislation could keep up, and

[2] Hindustan Times, India lost over ₹11,000 crore to cyber scams in first 9 months of 2024.

many forms of cybercrime hadn't even been imagined when the Act was first written. To plug the gaps, older laws like the Indian Penal Code, 1860 were adapted to cover online wrongs—sections [3]related to cheating, criminal intimidation, and defamation were now being applied to fraud, cyber bullying, and online harassment. But this mix-and-match approach wasn't always effective.

In 2008, a significant amendment to the IT Act was passed to bring it more in line with the realities of a digital age. The Information Technology (Amendment) Act, 2008 expanded the scope of cybercrime legislation, introducing new provisions to deal with cyber terrorism, child pornography, data breaches, and privacy violations. It also increased penalties for several offences, signaling a more serious approach to digital threats.

Yet, even with improved laws on paper, enforcement lagged behind. In many regions, police officers weren't trained to handle digital evidence or investigate complex cyber cases. Most districts lacked dedicated cybercrime units, and technological infrastructure was often outdated or missing. As a result, many victims chose not to report cyber offences—either because they didn't trust the system or felt ashamed, particularly in sensitive cases like online blackmail or harassment.

Over time, though, awareness has grown. Law enforcement agencies are slowly building capacity, with more officers receiving training in cyber forensics and more cyber cells being established. Public awareness campaigns are helping citizens recognize threats and protect themselves. And on a global level, India has started collaborating with other countries to tackle cybercrimes that cross borders—because in the digital world, crime rarely stays local.

All in all, the journey of India's cybercrime laws reflects an ongoing effort to catch up with the fast-changing tech landscape. From basic hacking to highly sophisticated attacks, the legal system has had to constantly evolve—and will need to keep doing so as new threats continue to emerge.

III. COMMON FORMS OF CYBERCRIME IN INDIA

Common Forms of Cybercrime in India: Trends and Realities (2024)

Lately, India has been witnessing a sharp rise in cybercrime, affecting more and more people in their everyday lives. With over 1.7 million complaints filed in 2024 alone, it's clear that while our digital ecosystem has grown, so too have the threats lurking within it. From fraudulent trading apps to emotionally manipulative romance scams, cybercriminals are getting smarter — and bolder.

1. Financial Fraud: The Most Widespread Threat

Digital wallets and online banking have made life easier, but they've also made financial

[3] CloudSEK,India to lose Rs 20,000 Crore to Cybercrime in 2025, 2024

scams frighteningly common. In 2024, Indians lost an estimated ₹33,165 crore to cyber fraud [4]— with ₹22,812 crore lost in that year alone. Phishing links, fake banking portals, and deceptive investment pitches are just a few tools in the fraudster's kit.

2. Investment & Trading Scams: If It Sounds Too Good to Be True...

Fraudulent investment platforms and cloned trading apps have become a goldmine for scammers.

Fake Investment Schemes duped thousands with fake promises of high returns, causing a loss of ₹3,216 crore across 1 lakh+ cases.

Clone Trading Apps mimicked real trading platforms, conning users out of ₹1,420 crore through 20,043 cases.

3. Digital Arrest Scams: Fear as a Weapon

A terrifying trend in 2024 was the rise of digital arrest scams — where criminals posed as police or government officials. Victims were tricked into believing they were facing legal trouble, then coerced into paying huge "penalties." There were over 63,000 reported cases, with ₹1,616 crore lost.

4. Phishing & Identity Theft: More Sophisticated Than Ever

The days of badly written spam emails are a thing of the past. Today's phishing scams use AI-generated messages, deep fakes, and even spoofed official domains to trick victims into giving away sensitive data — from Aadhaar numbers to OTPs. The stolen identities are then used to drain bank accounts or commit fraud in someone else's name.

5. Online Harassment & Cyber stalking: A Hidden Crisis

Unfortunately, social media and messaging platforms have turned into spaces where harassment can easily grow. Increasingly, women, teenagers, and other vulnerable individuals are being subjected to cyber bullying, blackmail, and stalking. Sadly, many of these incidents are never reported, often because victims feel scared, embarrassed, or lack faith in the legal system.

6. Data Breaches: The Cost of Weak Defenses[5]

In 2024, India witnessed a major breach when hackers used Telegram bots to leak sensitive data from Star Health, one of the country's largest insurers. Millions of customer records,

[4] Ritesh Tripathi , Indians lost over ₹1,750 crore to cyber fraud in first four months of 2024, The Economic Times, May 27, 2024.
[5] A comprehensive survey of cybercrimes in India over the last decade, International Journal of Science and Research Archive, 2024.

 [ISSN 2581-5369]

including health and financial details, were compromised — exposing the urgent need for stricter data protection.

7. Romance & Sextortion Scams: Playing with Hearts and Finances

One of the most heartbreaking forms of cybercrime is the growing spread of romance scams. In these schemes, criminals create false relationships, earn their victims' trust, and then exploit them by coercing them into sending explicit material or money.

IV. AWARENESS AND PREVENTION OF CYBERCRIME IN INDIA

In today's digital world, staying safe online isn't just about using technology—it's about knowing how to protect yourself. While law enforcement agencies and specialized units are crucial in handling cybercrimes after they happen, the most powerful defense is often prevention, which begins with awareness. Educating people—whether they are citizens, businesses, or government bodies—on how to protect themselves from digital threats is key in reducing the risks of cybercrime. Here's how we can strengthen awareness and prevention efforts:

1. Public Awareness Campaigns

The first step to protecting ourselves from cybercrime is understanding the risks we face when we go online. In India, both government bodies and private organizations have been working to spread awareness through cyber security campaigns. These campaigns focus on helping people recognize common threats, such as:

- Phishing Attacks: Learning how to spot fake emails or messages that trick you into revealing personal information like passwords or bank account details.
- [6]Malware and Ransom ware: Understanding the dangers of harmful software that can lock your files or steal your personal information.
- Secure Online Transactions: Teaching people how to protect themselves when shopping or banking online by using secure websites, strong passwords, and two-factor authentication.
- Protecting Personal Data: Raising awareness about the importance of privacy settings on social media and keeping personal information safe from identity theft.

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

2. Digital Literacy Programs

One of the biggest barriers to preventing cybercrime is the lack of digital literacy, especially in rural areas where many people are still not fully aware of how to protect themselves online. To bridge this gap, digital literacy programs have been rolled out to improve citizens' understanding of the internet, online safety, and responsible digital behavior.

Community Outreach: Local workshops and awareness drives help people understand how to secure their devices and protect their online activities.

School and College Programs: Many schools now include cyber security in their curriculum, teaching students how to navigate the internet safely, use social media responsibly, and understand the legal consequences of online behavior.

Partnerships with NGOs: Non-governmental organizations are crucial in reaching out to underserved communities, particularly in rural areas, to help them become more aware of digital threats.

3. Cyber Hygiene and Best Practices

[7]Just like we take care of our personal hygiene to stay healthy, keeping up with good cyber hygiene is crucial for staying safe online. Adopting a few simple habits can go a long way in protecting ourselves from cybercrime. Here's what we should all be doing:

- Strong Passwords: Make sure your passwords are unique and strong for each account. A password manager can make it a lot easier to keep them organized and secure.
- Two-Factor Authentication (2FA): By turning on 2FA, you add an extra layer of protection to your accounts, making it significantly harder for hackers to gain access.
- Regular Software Updates: Keeping your devices updated with the latest software helps close security holes that hackers might exploit.
- Safe Browsing: Be cautious about clicking on links from sources you don't trust, and think twice before downloading any files or attachments.
- Anti-virus Software: Installing reputable security software on your devices can catch threats before they cause harm.

4. Cyber security in Schools and Colleges

Educational institutions have an important role in preparing students to stay safe online. Schools and colleges are increasingly introducing cyber security training programs to ensure

[7] Avnish Bajaj v State (N.C.T) of Delhi, 2004 SCC ONLINE DEL 1160

that students have the knowledge to navigate the digital world securely.

Workshops and Webinars: Many schools now invite cyber security experts to run workshops, [8]teaching students about online threats like cyber bullying, identity theft, and online scams.

Social Media Awareness: Students are taught how to maintain privacy and what to share (or not share) online to protect themselves from potential harm.

Online Ethics and Cyber bullying: Discussions around online behavior and the consequences of cyber bullying help students understand the serious impact of their actions in the digital space.

5. Corporate and Workplace Cyber security

Businesses are also prime targets for cybercriminals, and it's essential that companies take steps to protect their data and that of their customers. Here's what businesses can do:

Employee Training: Companies should organize regular training sessions for employees to help them recognize common cyber security threats, like phishing emails or data breaches.

Data Protection Policies: Businesses need to have clear policies in place to ensure that their employees are following best practices for data storage, file sharing, and online communication.

Incident Response Plans: It's crucial for companies to have a clear plan in place for responding to cyber incidents. A prompt, organized response can help minimize damage in case of a breach.

6. Role of Law Enforcement in Prevention

While law enforcement agencies are mainly responsible for investigating and prosecuting cybercrimes, they also play a critical role in prevention. Here's how:

Cybercrime Awareness Campaigns: Police departments and cybercrime cells run campaigns to alert the public about specific cyber threats that may be circulating at any given time.

Collaboration with Tech Companies: Police often work with technology companies to ensure platforms remain secure and to investigate suspicious online activities quickly.

Community Outreach: Cybercrime units organize local events to inform citizens about the latest scams or online threats, helping them stay ahead of potential dangers.

[8] Ajayakumar v State of Kerela 2019 SCC ONLINE KER 15889

 [ISSN 2581-5369]

7. Future of Cybercrime Prevention

The future of cybercrime prevention relies on staying ahead of cybercriminals by adapting to new technologies. With the growing use of AI, block chain, and other emerging tools, it's important for both law enforcement and the public to stay informed and prepared.

AI and Machine Learning: AI-powered tools are becoming increasingly effective at spotting suspicious patterns, detecting fraud, and identifying phishing emails before they cause harm.

Cyber security Education: As cybercrime continues to evolve, it's important that education programs do the same, helping people stay one step ahead. Schools, universities, and organizations will continue to adapt their curricula to teach future generations how to protect themselves in an increasingly digital world.

V. CONCLUSION

As our world becomes more and more digital, the fight against cybercrime has never been more important. While law enforcement agencies, like cybercrime cells and specialized task forces, are essential in investigating and bringing offenders to justice, the real power lies in awareness and prevention. Educating people—whether they're individuals, businesses, or government bodies—about the risks of the digital world and teaching them how to protect themselves is a critical part of building a safer online space.

Campaigns that raise awareness, digital literacy programs, and simple cyber security best practices are the foundation of any effort to reduce cybercrime. But it's not just about educating individuals; it's also about collaboration between the public and private sectors, and having schools and universities teach safe online habits. Together, these efforts help foster a culture of cyber security that empowers everyone to stay safe.

There are still challenges to overcome—like improving infrastructure, handling jurisdictional issues, and staying ahead of emerging cybercrime tactics. But with continued investment in resources, training, and public outreach, we can face these challenges head-on. As technology evolves, our approach to cyber security must evolve too, ensuring that prevention and awareness stay at the heart of India's strategy for protecting its cyberspace.

Ultimately, a comprehensive approach that blends education, prevention, and collaboration is the key to effectively combating cybercrime. By working together, we can ensure that the digital world remains a safe, secure place for everyone.

*****

 [ISSN 2581-5369]

VI. BIBLIOGRAPHY

1. National Cyber Crime Reporting Portal (NCRP). Ministry of Home Affairs, Government of India. Retrieved from https://cybercrime.gov.in.— This official portal allows citizens to report cybercrimes, playing a critical role in India's response to digital threats.
2. The Role of Cybercrime Cells in India. (2023). Cyber security Research Journal, Vol. 5, Issue 2. — A detailed study on how specialized cybercrime cells contribute to investigations and digital crime control across the country.
3. CERT-In: Strengthening India's Cyber security Infrastructure. Ministry of Electronics and Information Technology. Available at https://www.cert-in.org.in.— This government body is key in managing cyber threats and issuing alerts about vulnerabilities.
4. Cybercrime and Its Impact in India. (2024). India Cybercrime Report, Cyber Crime Division, CBI.— Offers insights into trends, challenges, and case studies related to cybercrime investigated by the CBI.
5. Cyber security in India: Challenges and Solutions. (2024). National Institute of Cyber Security.— A comprehensive review of India's cyber security landscape and what can be done to strengthen it.
6. India's Response to Cybercrime: A Legislative Overview. (2023). Legal Insights Journal.— This article breaks down key laws and policies tackling cyber offenses in India.
7. Public-Private Partnerships in Cyber security. (2024). Cyber security Collaborations: A Global Perspective, Vol. 8, Issue 3.— Explores how collaboration between government and industry can lead to stronger cyber security defenses.
8. Understanding Digital Fraud and Financial Crimes in India. (2023). Financial Security Journal.— Looks into how cybercriminals target financial systems and what steps are being taken to prevent it.
9. Digital Literacy and Cyber Awareness Initiatives in India. (2023). Cyber Awareness Bulletin.— Highlights national efforts to promote digital education and safe online practices.

 [ISSN 2581-5369]

10. Indian Government's Role in Combating Cybercrime. (2024). Government Policy Review, Volume 12, Issue 1— Analyzes various policy-level initiatives and how they've evolved in response to rising cyber threats.
11. The Rise of Cyber stalking and Harassment in India. (2024). Indian Journal of Digital Law and Ethics.— Sheds light on the growing issue of online harassment, especially targeting women and young users. National Cyber Security Policy 2020.

*****

 [ISSN 2581-5369]