International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
An International Quarterly bi-lingual Multidisciplinary Double Blind Open Access Peer Reviewed Refereed Journal
ISSN:2581-9925, Impact Factor (Cosmos: 7.555 & I2OR: 5.105), Volume 08, No. 03(II), July-September, 2026, pp. 135-138

Cyber Law as a Legal Framework Against Cybercrime

Neha Verma*

Lecturer, Department of Computer Science, Bharati College.

*Corresponding Author: urvashiverma90@gmail.com

Citation: Verma, N. (2026). Cyber Law as a Legal Framework Against Cybercrime. International Journal of Education, Modern Management, Applied Science & Social Science, 08(03(II)), 135–138. https://doi.org/10.62823/IJEMMASSS/8.3(II).9406

ABSTRACT

The moment you think you are chatting with your friend privately, stop immediately and reconsider. Noticed, whenever there is news related to cybercrime, the media and news channels sometimes show their chats and records. So, how exactly did their conversation history and records get leaked when such messaging and calling apps claim to be "private, secure and encrypted"? In India, we have stronger cybersecurity than many nations worldwide, but to eliminate cybercrime, staying alert to common threats like financial fraud, phishing, identity theft, deep fake and online scams is essential. In this paper, we will discuss how to prevent cybercrime and be aware of the cyber law.

***Keywords**: Cybercrime, Cyber Threat Software, Malware, Cookies, Laws Against Cybercrime in the Constitution of India.*

Introduction

The world of cybercrime is globally linked to the internet and digital networks, as well as to criminal marketplaces like the Dark Web. Cybercriminals can come from anywhere in the world and often operate through large-scale infrastructures like botnets, which enable them to target multiple victims simultaneously. You must have heard about ransomware attacks in the news from time to time, which not only target people but also large organisations. So, this is not about what happened yesterday, but about what is happening at present and what will happen in the future.

Cybercrime is ever evolving, and by shedding light on how they operate and use technology to take advantage and exploit their victims, our cyber threat intelligence analysts, whether in India or any other part of the world, can anticipate and defend against cyber threats by implementing security controls, monitoring systems and developing strategies to mitigate risk.

Cyber Crime

Today, defending against cybercrime is one of the most critical priorities for every individual and organisation. And only after reading and understanding the impact of cybercrimes can we comprehend how they infiltrate our lives, masquerading as viruses, Ransomware, Malware, Trojans, and phishing. These threats are not just affecting us in India, but globally. With so many options at their disposal, the cybercriminal cannot be framed in a single painting. Unlike in the past, when people used to keep a "Personal" diary to store their usernames/passwords and other daily useful info such as phone numbers, nowadays, we rely heavily on cloud storage, which helps us manage data like pictures, usernames/passwords, bank details, and documents. One wrong move while browsing online, whether on a personal or work machine, can allow cybercriminals easy access to personal information, as well as restricted or highly confidential data, client details, and business trade secrets. This affects individuals through financial loss, identity theft, and job loss, while also impacting organisations with financial penalties, reputational damage, operational disruption, and legal consequences. For example, a person,

while working on their device and browsing online, may see fake error messages claiming their device is infected with viruses or other serious issues. They might be told to contact a dedicated team immediately, with names sounding from trusted organisations. Shocked and trying to fix the problem, they may reach out to the team, who then provides a solution to an issue that doesn't exist, which is where their scam begins. Cybercriminals often ask them to download certain software so they can access their machine and supposedly fix the problem. However, by doing so and having a compromised device, they not only risk losing all the data stored there, but also expose sensitive information such as their usernames and passwords, bank card details stored in browsers and cloud saves, and cookies.

Let's discuss about some of the arsenals such cybercriminals have a bit more…

"Malware", which is malicious software designed to disrupt, damage, or gain unauthorised access to computer systems, networks, or devices, often for financial gain by stealing data, locking files (ransomware), spying (spyware), or disrupting functions (viruses, worms, Trojans). It infiltrates systems via phishing, malicious downloads, or infected websites, causing slowdowns, crashes, data theft, or financial extortion.

"Cookies", another new arsenal… Nowadays, we must have noticed that while visiting and logging in on websites, we are prompted to accept cookies, and with an option to remember and keep our session active, reducing the need to enter the password each time we log in, and just continue right where we have left off. So, while being convenient, this info is stored in the same cookies and can be used by cybercriminals on other devices to log in.

These malicious tools can be either external or internal, which are designed to exploit the system for its weaknesses and use it against the person to get access to their Network, giving them unauthorised access to steal data and cause damage. This all starts when people are unfamiliar/uneducated about cyber threats and do not install security updates on their machines to fight such threats. As cyber security companies or OS providers usually provide security updates from time to time, often every month, through Anti-Virus and other security system updates. Also, having weak passwords, unsecured connections, opening bank accounts at unofficial &unsecured URLs, downloading unsecured files from unofficial sources, opening any random advertisement that is displayed on the screen and filling out the personal details. Most of the cybercriminals are young people, often highly educated with tech skills, but are unemployed and in dire need of money, with not enough options. The global growth rate of cybercrime is categorised as a severe threat and is projected to inflict damages totalling $10.5 trillion annually by the end of 2025 globally, growing at a rate of approximately 15% year-over-year. This makes the "economy" of cybercrime larger than the GDP of most countries. Over 1.5 million.

Cyber Law in India

The internet has completely changed how we live, working its way into everything from how we talk to friends to how we handle our money. But that convenience comes with a heavy price tag: the massive spike in cybercrime. While India's Constitution is the bedrock of our laws, it was written for a different time—long before anyone worried about data breaches or online scams. So, we're essentially playing catch-up, trying to adapt our legal system to fight crimes that didn't even exist a few decades ago.

In 2012, the National Policy on Information Technology was introduced to help use tech for the country's growth. It worked, but as the IT sector boomed, so did the "dark side" of the web. We started seeing traditional crimes like theft and fraud moving online, alongside completely new problems like hacking and identity theft. That's where the Information Technology Act, 2000 comes in. It's basically the rulebook for the Indian internet. At first, it was mostly about making electronic signatures and online deals legal. But over time, especially with the 2008 amendments, it had to get much tougher. The government added stricter penalties and clearer definitions for what actually counts as a cybercrime because the old rules just weren't cutting it. If you look at the specifics, the IT Act actually has some teeth now. Section 43 is what they use to go after people who hack into systems or steal data. Sections 66C and 66D are there to tackle identity theft and those scams where someone pretends to be you to steal money. There's also Section 67, which is huge for protecting people from harassment and obscene content online. It's not just about the criminals, though; Section 79 puts some responsibility on the platforms themselves—like social media sites and internet providers—to make sure they aren't letting illegal stuff slide. It's not just the IT Act doing the heavy lifting, either. The police often use the old-school Indian Penal Code (IPC) alongside it for things like online blackmail or fraud. Plus, we are finally seeing more focus on privacy with newer data protection rules coming into play, which is a relief given how much personal info we all put out there.

To actually enforce all this, the government set up the Indian Cyber Crime Coordination Centre (I4C) to get state and national police on the same page. There's also CERT-In, which is basically the emergency response team for when big cyberattacks happen. Looking forward, it's going to be a constant battle. With things like AI and crypto taking off, the threats are only going to get weirder and harder to track. We need better international cooperation and smarter forensic tech to keep up. Right now, cyber law in India is trying to be both a shield for us regular users and a weapon for the police, but it's definitely a work in progress.

Here are some of its sections that empower internet users and attempt to safeguard cyberspace:

- **Section 65:** Tempering with Computer Source Documents- A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both. It is proposed that in Feb2026, new law will be emerged to increase security over network, there will be logout from system in every 6 hours.
- **Section 66:** Using Password of another person- If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.
- **Section 66D:** Cheating using computer resource- if a person cheats someone using a computer resource or a communication device, he/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR.
- **Section 66E:** Publishing private images of others- If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both.
- **Section 66F:** Act of Cyber Terrorism- A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or attempts to penetrate/access a computer resource without authorization, with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.
- **Section 67:** Publishing child porn or predating children online- If a person captures, publishes or transmits images of a child in a sexually explicit act or induces anyone under the age of 18 into a sexual act, then the person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both.
- **Section 69:** Government's power to block website- If the government feel it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance withthe procedure. Under section 69A, the central government can also block any information from public access.
- **Section 43A:** Data Protection at Corporate level- If a body corporate is negligent in implementing reasonable security practices which cause wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affected person.

A dedicated helpline 1930 helps immediately to the victim of financial fraud. Cyber Crime Prevention against Women and Children (CCPWC) addresses cyber fraud targeting vulnerable sections, particularly women and children. The Samanvaya platform make cyber crime investigation stronger by providing analysis based interstate linkages of criminals and crimes. **Sahyog** portal provides a centralised platform for addressing unlawful online content. **Sanchar sathi**is an app available on Play Store can be downloaded. It is an integrated space for citizen-centric service. It's subset Chakshu that report suspected communication, malicious links and unsolicited commercial communication.

Most Recent Cyber Crimes in India

Cyber Incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024. Over 9.2 lakh SIM cards and 2,63,348 IMEI's linked to cyber fraud have been blocked. In November 2025 Ransomware Attack breached data from more than 5 companies. Toyota Financial Services, Chicago Trading Company, Yamaha Motors attacked by Medusa, Lockbit Ransomware software. The All India Institute of Medical Science hit by the Ransomware last year, which forced the institute to switch on to manual mode

of operation, like other attacks, it targeted sensitive information about patients, the administrative department and research documents. The attackers used LockBit ransomware and demanded 200 Crores as cryptocurrency from AIIMS.

References

1. “Future Crimes” Inside the digital underground and the battle for our connected world by Marc Goodman.
2. ”The Antivirus Hacker’s Handbook” by Joxean Koret, Elias Backaalany
3. “Cyber law in India” Fathoming your lawful perplex by Akash Kamal Mishra
4. https://infosecawareness.in/cyber-laws-of-india.

❑❑❑