# CYBERCRIME AND CYBER SECURITY: LEGAL CHALLENGES AND POLICY RESPONSES

*By Isha Jain* & Dr. Jyoti Panchal Mistri***

**ABSTRACT**

*We live in the era of computer and internet. This era known as Digital Era where everything is available on fingertips, whatever we want available online the advance technology including Artificial Intelligence, E commerce and high speed internet like 5th generation connectivity made this environment. But this era raises some serious concern like increasing in cybercrimes we can say that in digital era leads to digital crimes referred as cybercrime. Our data now a days have most valuable assets. By the help of this research paper, I want to throw light on this serious issue by which we can see how this cybercrime increases, reason behind it, how government can deal with and how people can aware about this. Cyber laws are indispensable for creating a secure environment, but it also faces certain legal challenges like new techniques of crime. A comprehensive policy framework is required to ensure security and confidentiality in cyber space. However, India's cyber laws help in addressing cybercrime issues for sustainable growth.*

**Keywords**: Cybercrime, Cyber Security, Data Protection, Cyber Laws, Cyber Attacks, Internet.



* Research Scholar, Institute of Law and Legal Studies, Sage University, Indore. Email: ishajain056@gmail.com.
** Supervisor, Associate Professor, Institute of Law and Legal Studies, SAGE University Indore. Email: jyotipanchalmistri@gmail.com.

## I. Introduction

More dependency on cyber space whether of individual or organisations is harmful, it increases cybercrimes, children are addicted to online game, young people are addicted to social media how it could not them fall easy prey to cybercrimes. Changes in patterns of crime needs changes in law and government policies also.

The rapid digitisation of governance, commerce, education and social interaction has fundamentally transformed modern society, making cyberspace an indispensable part of everyday life. From online banking and e-commerce to digital governance and social networking platforms, individuals and institutions increasingly rely on information and communication technologies. However, this growing dependence has simultaneously widened the scope for cyber vulnerabilities. Cybercrime has emerged as one of the most pressing challenges of the digital era, transcending geographical boundaries and traditional notions of crime. Unlike conventional offences, cyber-crimes are often anonymous, transnational, technologically sophisticated and capable of affecting a large number of victims within a short span of time, thereby posing serious threats to privacy, financial security, public order and national security.

In response to the escalating menace of cybercrime, cyber security has assumed critical importance as a legal, technical and policy concern. While India has enacted several legislative measures, including the Information Technology Act, 2000 and subsequent amendments, the evolving nature of cyber offences—such as phishing, ransomware attacks, identity theft and data breaches—continues to expose gaps in the existing legal framework.



The emergence of advanced technologies like artificial intelligence, cloud computing and high-speed internet connectivity has further complicated the regulatory landscape. These developments necessitate continuous legal reforms, effective enforcement mechanisms and enhanced public awareness to ensure a secure digital ecosystem. This paper, therefore, seeks to examine cybercrime and cyber security from a legal perspective, analyse the challenges faced by the existing laws and policies, and suggest policy responses to strengthen India's cyber security regime in an increasingly digitalised world.

## II. Identification of Statement of Research Problem

Despite having cyber laws in India, the rate of cybercrime is increasing continuously government, law enforcement agencies often faced so many challenges in combating it. There is a lacuna in present cyber security laws. It is not effective to counteract with new techniques of cybercrime, also the legal challenges faced required new policy reforms in law and legislation. How badly it impacts the society is to be looked into and awareness should be raised among people regarding new cybercrime.

### A. *Research objectives*

The following research objectives are:-

- To analysis various aspects of cybercrime.
- To evaluate the cyber security and its awareness among people.
- To critically examine the legal development of cyber security laws and regulations.
- To recommend the policy measures to combat cybercrimes and increase cyber security in digital ecosystems.
- To assess the impact of cybercrime on society.

### B. *Research Hypothesis*

The present laws protecting cyber security is not enough to prevent cybercrimes. India's legal framework and judicial precedents are insufficient to eradicate cybercrimes and ensure cyber security, thus necessitating additional legislative and policy reforms. This approach guarantees a comprehensive and multi-dimensional analysis of cybercrime, cyber security and cyber laws in India, what are the legal challenges of cybercrimes to be dealt with and policy reforms needed to combat cybercrimes.

## III. Research Methodology

The methodology of the research titled "Cybercrime and Cyber Security: Legal challenges and policy responses" is of doctrinal nature. It includes a comprehensive, complete, critical and multi-dimensional scenario of cybercrimes, laws and regulations against it, factors influencing cybercrimes and cyber security measures. Primary and secondary sources are used. It includes legal texts, books, articles, reports, case studies, judgments, research papers, newspaper. This paper analysed the National Crime Records Bureau data.

## IV. Analysis & Findings of the Research

### A. *Cybercrime*

A crime in which computer is the medium of crime or the computer is used as a tool to commit that crime is called cybercrime. Similar to physical crime the intention of cyber criminal to harm the victim physically or mentally or by damage their reputation. Cybercrime is not new erose crime , first cybercrime was reported in year 1820 which is difficult to believe and first hacking was reported in year 1960 and first computer virus was reported in the year 1980. The 1990's marked a shift as cybercrimes became rampant and financially motivated. With the rise of internet and e-commerce, cyber criminals exploited vulnerabilities in online systems for activities like online scams, e-mail spoofing etc. Early 2000's saw a rapid increase in cyber-attacks targeting government data, large business houses and confidential data.

### B. *Classification of Cybercrimes*

The classification of Cybercrime helps to understand varied nature of cyber threats in a systematic way.

*1. Target Based Cybercrime*

- Individuals: - Cybercrimes committed against individuals includes harassment via e-mail (*State of Tamil Nadu v. Suhas katti,* CC No. 4680/2004), cyber-stalking, defamation, cheating fraud exploitation, transmitting virus & discrimination & obscene material, intellectual property crimes and so on.
- Organizations: - It includes cybercrimes such as unauthorised access over data system, corporate espionage, financial frauds, ransomware attacks, forgery, theft of intellectual property.
- Government: - Cybercrimes against government includes cyber terrorism, hacking of system and targeting government entities with the aim of compromising national security, public service and democratic processes.

*2. Method Based Cybercrime*

- Hacking: unauthorised access to computer system or networks to steal data or disrupt operations or implant malicious software. Hence, it tightly is an attempt to bypass the security mechanisms of information system.

- Malware: the dissemination and deployment of trojans, and ransomware to compromise computer systems, extract data, or extort ransom payments.
- Phishing and Social engineering: Deceptive methods to trick individuals or organisations into divulging sensitive information, such as login details or financial data, via fraud emails, website or message.
- Financial fraud: online scams, phishing schemes, credit card fraud etc.
- Identity theft: unauthorised use of credit card details, and passwords to assume other's identity for fraudulent purpose.

C. *Causes of cybercrimes*

India is developing country, so illiteracy is common problem in India that is the main reason of increasing cybercrime in India. People especially from rural areas and some backward areas are not familiar with such aspects. Cyber-crime is totally different from physical crime in every aspect, some can easily say that it doesn't need any physical equipment to commit this only need mobile phone and good internet but the effect of cybercrime is more broad than physical crime, a physical crime may be difficult to commit but affect to induvial or some organisation rather than cybercrime is easy to commit but affect large populations sometime it beyond physical boundaries of a country.

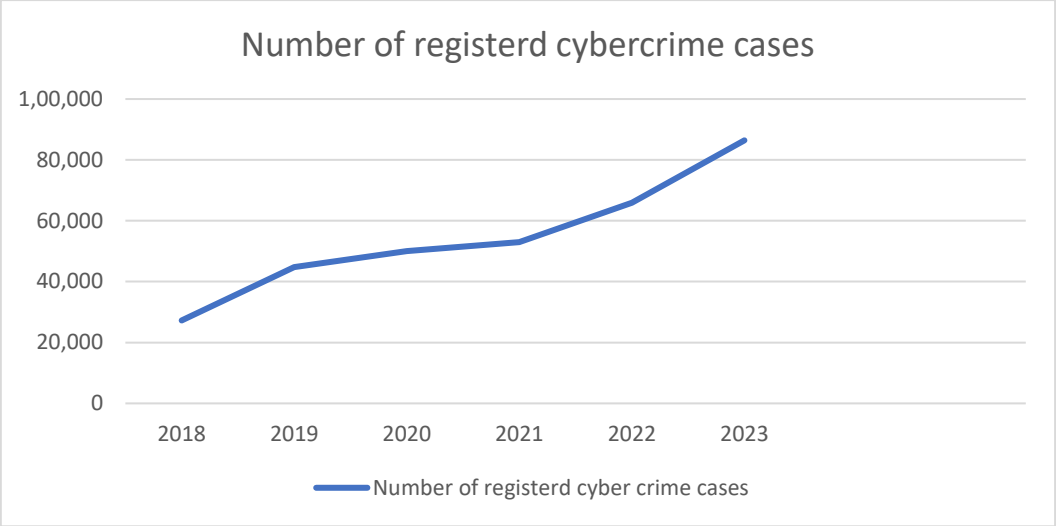
Sometimes cybercriminal have more knowledge of computer and its network, and their soft targets are women, children and old age people who don't aware about cybercrimes.

Sometimes people's own negligence caused cyber-attacks like people never change their passwords for long times, they click on unsafe links, they regularly share their information on social platform (*Shreya Singhal vs Union of India* (2015) 5 SCC 1) this lead them for cybercrime activity.

D. *NCRB Data*

Latest data released by National Crime Records Bureau (NCRB) provides cybercrime in India saw a sharp surge of *31.2%* in 2023 with majority of cases involving fraud, extortion and sexual exploitation. Nearly *69%* of all cybercrime incidents involves financial fraud related offences causing growing concern over digital security and cyber vigilance across the country. The national rate of cybercrime rose to 6.2 cases per lakh population, up from 4.8 the year before. But the spread was not uniform. Just five states – Karnataka, Telangana, Uttar Pradesh, Maharashtra and Bihar have three fourths of all cyber offences.

The cases registered under the cybercrime category from the year 2018 to 2023 are as follows:




The graph shows a steady increase in cybercrime cases in six years, by highest jump between 2022 and 2023.

E. *Impact of Cybercrime*

Cybercrimes leads detrimental Consequence it impacts society by:-

- Financial Loss: It causes financial losses as criminals steal money directly from bank accounts. It is now a days very common by getting otp or just hacked someone's mobile phones.
- Data Leaks: In this digital era this is the most common aspect of cybercrime the Data leaks on internet, and it affect every age group and in the era of Artificial Intelligence it becomes more harmful specially for teenagers' girls to famous celebrities. Some personal data leaks affected to companies that affect their good will and their market caps and caused huge financial loss. Sometimes this data leaks affect deeply to their social lives and affect increasing suicide among peoples.
- DOS: Denial of service attacks are more common now a days, now wars are not limited to boarder areas now some battels are Faught on internet, by this they can harm every aspect of common areas for example now a day dos attacks occurred in Aviation industries, it affect all over country where common people affected.

F. *Cyber Security*

According to Section 2(1)(nb) of Information Technology Act, 2000 the term "cyber security" means protecting information, communication device from unauthorised access, modification or destruction. Data plays important role in today's life, peoples data is more valuable then

themselves so to protect this data in today's digital environment is the key aspects. That's why Indian Ministry of Law and Justice passed an Act on 11th August 2023 for safeguarding related to personal Data of people of India by this the main focus was to protect people's data from unauthorised sources.

G. *Findings of the Research*

The study highlights various loopholes in the legal framework and government policies. Government has to amend this law to conquer cyber-crimes in this generations. Now cybercrime leads to huge financial loss by different criminal activity like phishing or spoofing. They mainly target people who have less knowledge about internet functionality like old age peoples. Now a days people's personal data is most valuable thing so government will take some major steps for safeguarding this data. Cybercrimes have no boundaries, no nation they have only criminal intention so sometimes some international cyber criminals involved init.

H. *Recommendations*

Some key aspects should be taken by government to protect people from cybercrimes. Government have to start awareness campaign on social media platform to aware young generation about cybercrimes. And its duty of citizens to be careful about what they share online, where they share and with whom they share. They have to show some smartness about which website they visit, the link in which they click, what material they downloaded from internet.

## V. Conclusion

Main advantage that cyber criminals have is they have vast knowledge about computer and cyber system so they use different techniques to do these criminal activities by which it is so difficult to analysis their pattern. Different independent research shows in recent five years cybercrime activity increasing day by day and government have to take some major steps under Indian cyber law to conquer them.

*******

**References**


1. Sehgal, M., & Sharma, M. (2024). Protecting victims in the digital age: Online harassment and cyberstalking laws. *Burnished Law Journal*, *5*(2)
2. Gaur, K. D. (2016). *Textbook on Indian Penal Code* (6th ed.). Universal Law Publishing.
3. Myneni, S. R. (2013). *Information technology law (Cyber laws)*. Asia Law House
4. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cybercrime and cyber laws of India. *International Research Journal of Engineering and Technology*, *4*(6), 1634–1640
5. Tuli, B., Kumar, S., & Gautam, N. (2022). An overview on cybercrime and cyber security. *Asian Journal of Engineering and Applied Technology*, *11*(1), 36–45.
6. Jain, N., & Shrivastava, V. (2014). Cybercrime changing everything: An empirical study. *International Journal of Computer Application*, *1*(4), 31–36.
7. Ghosh, P., & Kapoor, P. (2024). Guardians of the digital vault: A comprehensive examination of financial cybercrime legislation and enforcement strategies. *Abhidhvaj Law Journal*, *2*(2)
8. Pandey, J. N. (2015). *Constitutional law of India* (52nd ed.). Central Law Agency.
9. Kabi, A., Marisport, A., Gori, S., & Tomar, A. S. (2022). The facets of cybercrimes against women in India: Issues and challenges. *Journal of Positive School Psychology*, *6*(8), 11467–11475
10. Jain, N. K., & Shrivastava, V. (2014). Cybercrime changing everything: An empirical study. *International Journal of Computer Application*, *1*(4), 31–36
11. Lakhina, K., & Vashishtah, A. (2024). Digital menace: The pervasive threat of cybercrime on society. *Indian Journal of Integrated Research in Law*, *4*(2), 853–867.


*******