JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# CYBER CRIME AND CYBER SECURITY: AN INDIAN PERSPECTIVE

**Dr. Jyoti Arora**
Assistant Professor
Department of Public Administration
Mehr Chand Mahajan DAV College for Women, Chandigarh

## Abstract

Even though technology make life easier and faster, they are also under threat from the deadliest sort of criminality known as "Cybercrime." The benefits of computer technology are not without demerits. With data and information being transferred between networks at distant locations, security issues have become a major concern from the past few years. Without computers, whole businesses and government functions would nearly cease to exist. The widespread availability of inexpensive, powerful, and user-friendly computers has enabled an increasing number of people to use and, more significantly, rely on computers as part of their everyday lives. Criminals are making technological tools to deceive public easily with this helping tool and make benefits out of it. The paper has made an endeavor to alleviate the evil of cyber crimes and solution to cyber crime, the Cyber security laws helps in preventing or reducing large scale damage to cyber-crime activities and protects access to information, privacy, communications, intellectual property (IP) and freedom of expression in relation to the use of the Internet, computers, websites, and email mobile phones, software and hardware, such as data storage devices.

**Keywords:** E-Governance, Information Technology and Cyber Crime

## Introduction

Cyber crime is a contemporary and pervasive issue that involves criminal activities conducted through computers, internet, or other related technologies. It is a alarming warning in India, where criminals exploit the anonymity provided by technology. Cyber Crime encompasses a wide range of illegal activities, including cyber-terrorism, email spoofing, cyber-stalking, cyber pornography and cyber-defamation, as well as traditional crimes committed online. Although cyber crime is not explicitly defined in Indian legislation, it is broadly understood as any illegal act where computers or the internet is either a tool or a target. As dependence on digital technology increases, so does the potential for misuse, making cyber crime an uncontrollable threat that requires urgent attention and regulation.

### Definition of Cyber Crime

The laws don’t provide the exact definition of Cyber crime, even the information Technology Act, 2000; which deals with cyber crime doesn’t define the term of cyber crime. However in general the term cybercrime means any illegal activity which is carried over or with the help of the internet or computers.

### Cyber Crime Rate

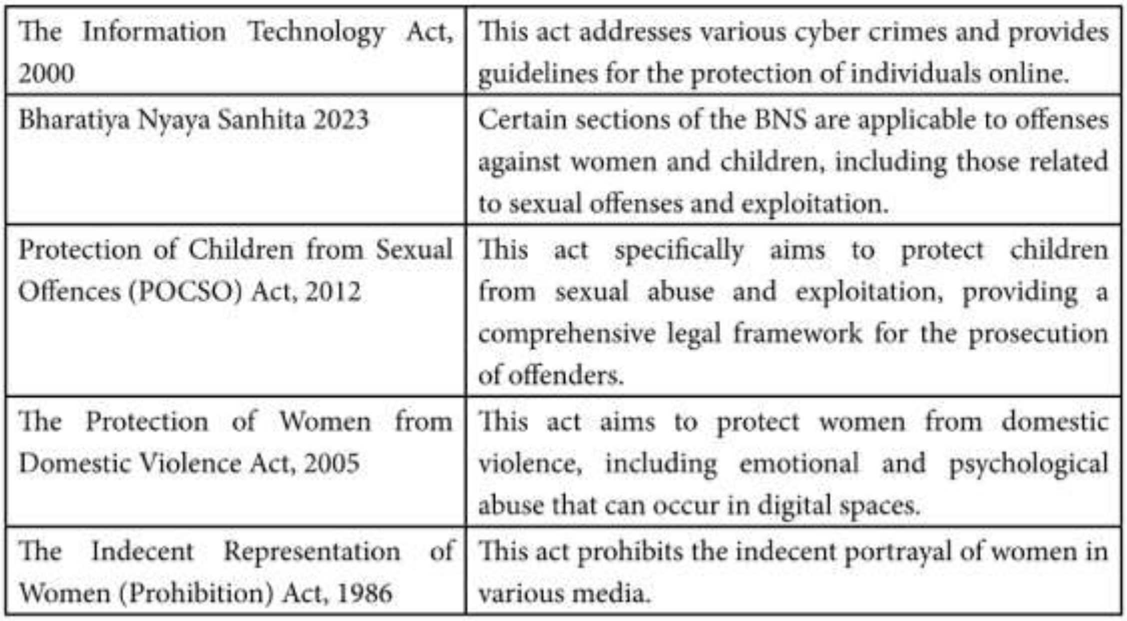
The year 2024 has marked a new high in cyber crimes in India. As per data, the number of average complaints has increased to 7000 per day. This number is around 113.7% more in comparison to 2021-2023 and 60.9% higher than 2022-23. In just the first 4 months, around 7,40,000 cases were registered on the Cyber Crime portal, and this number increased to 12 lakh by September 2024. Beyond the shocking case numbers, there are huge losses of capital too. Victims have collectively lost over Rs 120 crores to cyber frauds in the first nine months of 2024 alone. This depicts that cybercrime in India is increasing significantly, demanding immediate attention and action. While rising cybercrime cases have become a cause for concern for the Centre, out of the total 1.67 lakh cases registered between 2020-22 in all 28 states, only 2,706 persons (1.6%) have been convicted under these offences.

### Rising Statistics of Cyber Offences against Women and Children

Recent data from the National Crime Records Bureau (NCRB) highlights the alarming trend of increasing cyber crimes against both women and children. The statistics reveal a staggering 32% rise in cyber crimes against children from 2021 to 2022, with over 19,000 cases reported in 2022, a significant portion involving online sexual exploitation and abuse. Similarly, crimes against women have also seen a notable enhance, with a 4% increase in overall cases reported in the NCRB 2023 report. This increase underscores the urgent need for effective measures to safeguard these vulnerable populations in the digital landscape.

### Legislative Framework

To combat these growing threats, India has established a robust legal framework aimed at protecting both women and children from cyber crimes. Key legislations include:



| | |
|---|---|
| The Information Technology Act, 2000 | This act addresses various cyber crimes and provides guidelines for the protection of individuals online. |
| Bharatiya Nyaya Sanhita 2023 | Certain sections of the BNS are applicable to offenses against women and children, including those related to sexual offenses and exploitation. |
| Protection of Children from Sexual Offences (POCSO) Act, 2012 | This act specifically aims to protect children from sexual abuse and exploitation, providing a comprehensive legal framework for the prosecution of offenders. |
| The Protection of Women from Domestic Violence Act, 2005 | This act aims to protect women from domestic violence, including emotional and psychological abuse that can occur in digital spaces. |
| The Indecent Representation of Women (Prohibition) Act, 1986 | This act prohibits the indecent portrayal of women in various media. |

**Classifications of E-crimes**

Computer crime: Using of direct electronic operation that can attack security to obtain data and information illegally.

**High-tech crime:** A broad range of criminal activities that penetrate computers, illegally in violation of country laws, or federal laws. These crimes are done by hacking, money laundering, malware, harassment, electronic, and identity theft.

**White-collar crime:** A crime committed by a person of respectability and high social, status in the course of his occupation to obtain money.

**Hacking (Section 45, 63 and 66)**

Hacking refers to gaining unauthorized access to someone else's computer, similar to phone-tapping by exploiting weaknesses in the computer's security. Hackers identify vulnerabilities in a system and find ways to infiltrate it. There are several tools like firewalls and intrusion detection systems which are used for prevent hacking.

**Cybercrime:** It is a criminal activity that is done by using computers and the internet including anything from illegal downloading of music files and games to stealing millions of dollars from online accounts. Also non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on internet through music and game files.

**Cyber terrorism (Section 66 F) :** Premeditated and politically motivated attack against information, computer systems, computer programs, and data, which results in violence against civilian targets (Brokenshire, 2013). Possible cyber terrorism targets include the banking industry, military installations, power plants, air traffic control centers.

### Impact of E-crimes

- Loss of online business and consumer confidence in the digital economy.
- The potential for critical infrastructure to be compromised affecting water supply, health services, national communications, energy distribution, financial services, and transport.
- Loss of personal financial resources and the subsequent emotional damage.
- Loss of business assets
- Costs to government agencies and businesses in re-establishing credit histories, accounts and identities,
- Costs to businesses in improving cyber security measures,
- Stimulating other criminal activity, or
- Costs in time and resources for law enforcement agencies.

### Impact of Cyber Crime over Youth

Society's newest mode of interaction is cyber communication. Users can contact with people all around the world through social networking websites, text messages, and emails. Teenagers, in particular, spend a significant amount of time online each day, either on computers or on portable electronic devices.

**Friendships** According to Family-rescource.com, 48% of teenagers believe the Internet helps their friendships. With the rise in popularity of social networking sites, young people can keep in touch with both real and virtual pals. Some teenagers believe that having cyber connections gives them the confidence to be themselves. Instant messaging apps, which are used by an estimated 13 million teenagers, allow them to have real-time interactions with their pals. Friendships with other teens from all over the world can be formed via online communication technologies.

**Writing** According to Family-resource.com, 48% of teenagers believe the Internet helps their friendships. With the rise in popularity of social networking sites, young people can keep in touch with both real and virtual pals. Some teenagers believe that having cyber connections gives them the confidence to be themselves. Instant messaging apps, which are used by an estimated 13 million teenagers, allow them to have real-time interactions with their pals. Friendships with other teens from all over the world can be formed via online communication technologies.

**Cyber Bullying :** Cyberbullying is a detrimental side effect of teenage contact online. Victims of cyberbullying are frequently subjected to rumours and misinformation posted on social media sites. Bullies may upload images of their victims that are improper or embarrassing. Another facet of cyberbullying is the use of harassing text texts. According to the National Crime Prevention Council, cyberbullying affects over half of all American teenagers. Teens have taken their own lives as a result of internet bullying in certain extreme circumstances.

**Sexual Solicitation** : For kids who use forms of cyber communication, sexual solicitation is becoming a significant concern. It could happen in chat rooms or on social media platforms. When an adult or a peer attempts to engage in a sexual connection over the internet, this is known as sexual solicitation. A teen can be urged to reveal personal information, watch pornography, or talk about something sexual over the internet. Girls account for over 70% of those who are sexually solicited online. Teens should exercise caution while sharing suggestive photos on the internet or conversing with strangers in chat rooms.

**Cyber Security and Cyber Law**

Information Technology Act, 2000 The monitoring, decryption, and information gathering related to digital communications in India are heavily regulated by the Information Technology Act, 2000 (the "IT Act"). The Central Government and the State Governments may give directives for the monitoring, interception, or decryption of any information communicated, received, or stored through a computer resource, according to section 69 of the IT Act. In comparison to the Telegraph Act, Section 69 of the IT Act broadens the grounds for which interception may occur. Therefore, Section 69 interception of communications is done in the interest of

- The sovereignty or integrity of India;
- Defense of India;
- Security of India;
- Friendly relations with foreign States;
- Public order;
- Preventing incitement to the commission of any cognizable offense relating to the above; and
- For the investigation of any offense.

**How to improve cyber security and cyber laws awareness among the people?**

For a solid cyber security policy to be successful, every corporation needs to train its employees about cyber security, corporate regulations, and incident reporting. The finest technology measures may be breached by staff members who engage in negligent or malevolent behavior, costing a lot of money in security breaches. To decrease security infractions, it is helpful to provide workers with security training and awareness through seminars, lectures, and online courses.

- Update your operating system and software to take advantage of the most recent security patches. This is the most common safety precaution.
- Using antivirus software to identify and get rid of undesirable threats from your device is also helpful. To ensure the highest level of safety, this software is constantly updated. To identify security issues early in a secure environment, every firm makes sure to conduct regular security inspections of all software and networks. Application and network penetration testing, source code reviews, architecture design reviews, and red team evaluations area few common types of security reviews.
- Furthermore, enterprises should prioritize and address security vulnerabilities as soon as they are found. It is advised to always use lengthy passwords with numerous letter and symbol combinations. It ensures that the passwords are difficult to guess.

- Cyber security professionals always warn against opening or clicking email attachments from unknown senders or unfamiliar websites because they could be malware-infected. Additionally, you should be cautioned against using unsecured networks because they put you at risk for man-in-the-middle assaults.
- Every firm needs to regularly back up its data to prevent sensitive information from being lost or recovered after a security breach. Backups can also assist in preserving data integrity during cyber attacks like SQL injections, phishing, and ransom ware. To summarize, while a crime-free society is ideal and merely a dream, there should be a continuing effort to keep criminalities at a minimum by the application of rules. Crime based on electronic law-breaking is expected to increase, especially in a society that is becoming increasingly reliant on technology, and lawmakers will have to go the extra mile to keep impostors at bay.
- Technology is always a two-edged sword that may be utilized for both good and evil purposes. Steganography, Trojan Horses, Scavenging (and even Dos or Don'ts) are all technologies that are not crimes in and of themselves, but when they fall into the wrong hands with the purpose to exploit or misuse them, they fall under the category of cyber-crime and become serious offenses. Now, this is the time for governments around the world, including India, to understand that both emerging and developed countries would benefit from a secure cyberspace. Governments urgently need to implement well-developed cyber security policies in light of the fast expanding risks to national security in cyberspace. The national cyber security policy should include education, research and development, and training in cyber security.

## Conclusion

The enactment of Bhartiya Nyaya Sanhita (BNS), Bhartiya Nagrik Suraksha Sanhita (BNSS) and Bhartiya Sakshya Adhiniyam is a recent example of lawmaking note of technological advancements and use and abuse of technology by common man. These three laws will not only help investigators and adjudicators, but the interpretation of newly introduced provisions of these enactments by the Courts in the future will not only help to enrich the legal wisdom of the stakeholders but will also help in implementation of laws to achieve the object of administration of justice and crime control. The only need is to focus on capacity building in a techno legal environment for handling the challenges posed by latest technological advancements and increasing use of technology by the society. The proper appreciation of evidence will always remain the most crucial tool for achieving the object of justice in the changing legal scenario. ` The best defense against cyber risks is a combination of cyber security measures and educated and informed users. rulers and lawmakers must work hard to guarantee that technology grows healthily and is used for legal and ethical economic progress rather than illegal behavior. The three stakeholders, namely the rulers, regulators, lawmakers, and agents, should be responsible for it.

## References

1. Cyber Offences : Issues, Challenges and Solutions : Judical Academy Jharkhand, 23 February, 2025.
2. Cyber Crime in India: A Comparative Study M. Dasgupta, 2009
3. https://www.researchgate.net/publication/331914032_On_Cyber_Crimes_and_Cyber_Security (last accessed 15 September, 2025)
4. https://in.search.yahoo.com/search?fr=mcafee&type=E211IN826G91248&p=cyber+crime+and+cyber+security+in+india%2C+pdf (last accessed 16 September, 2025)
5. https://www.researchgate.net/publication/370654418_Cyber_Security_and_Indian_Cyber_Laws
6. (last accessed 18 September, 2025)