THE LAWWAY WITH LAWYERS JOURNAL
VOLUME:-22 ISSUE NO:- 22 ,MAY 25, 2025
ISSN (ONLINE):- 2584-1106
Website: www.the lawway with lawyers.com
Email: thelawwaywithelawyers@gmail.com
Authored By :- VEERBHAN

CYBERCRIME IN INDIA

Abstract
Many individuals say that the internet is a fantasy tool, a fascinating location, and an impressive encounter. But who is it for? Many of us are at risk of falling victim to the increasing number of criminals who are skilled in using the internet. A few people use internet technology for illegal actions, such as unlawful access to other networks. These illegal activities are related to the internet, which is known as cybercrime. Cyber law can be described as the branch of law that addresses the internet, cyberspace and legal issues. The scope is broad and includes many additional issues such as online security, online privacy, internet access and use, and freedom of expression. This article provides a brief study of cyber law and the key legal principles that govern cyberspace. The study delves into the significance of cyber law in protecting privacy, ensuring data security, and combating cybercrime. It examines the major statutes and regulations that constitute cyber law, with a focus on international frameworks and the legal landscape in India. Through this study, the article aims to highlight the critical role of cyber law in maintaining the integrity of digital interactions and defending individual rights in the digital era.
Key Words: Cybercrime, Cyber Law, Unauthorised Access, Network, Punishment, Internet.

Introduction

Cybercrime is derived from the words “cyber” and “crime”. Cyber means the Use of the internet and computer resources, and crimes mean the activities restricted by law. It means cybercrime is a crime that is committed through the internet and computers. Cybercrime developed at the time of the Internet’s development. The internet changes everything. With the evolution of the internet, there is a growth in committing crimes and offences on the Internet. Cybercrime includes a wide range of illegal activities, such as Internet phishing, cyber theft, virus attacks, software pirating, bank robbery, illegal downloading, industrial spying, cyber stalking and child pornography. Cybercrime is rapidly increasing in India. 49 thousand complaints of cybercrime were reported in 2020 in all states, which increased to 52 thousand in 2021, and in 2022, it was 64 thousand. Cybercrime involves unauthorised access to personal data, which directly infringes individual privacy rights. Article 21 guarantees the right to life and personal liberty. The Supreme Court of India has interpreted the right to life to include the right to privacy.

Classification of Cybercrime

Cybercrime can be divided into four major categories. They are as follows:

1. Cybercrime Against Individuals
2. Cybercrime Against Property
3. Cybercrime Against an Organisation
4. Cybercrime Against Society

- **Cybercrime Against Individuals:** Cybercrimes which focus on a certain person or individual. Some cybercrimes committed against individuals are:

- **Email Spoofing:** Email Spoofing is a method of spoofing mail headers. It means a message appears from an individual or some other source that is not genuine or authentic. These strategies are often utilised in scamming or spam campaigns because people open emails or text messages that they think are from a reliable source.

- **Spamming:** Email spamming is also known as unwanted emails. The email address of the receiver is acquired by spambots, these spam bots scan the web for email addresses. Spammers use bots to build email mailing lists. Spammers are often sending millions of emails to receive even a little.

- **Cyber Stalking:** Cyberstalking is when someone follows someone using electronic communications or repeatedly attempts to contact that person for personal gain, even if the person has expressed clear disapproval, or monitors a website, email, or other electronic communication, all of which constitute harassment.

- **Cyber Bulling:** All types of bullying or harassment through the use of electronic or communication tools such as laptops, computers and smartphones.

- **Online Sextortion:** Online sexual harassment happens when someone makes threats to send private information electronically unless they provide sexually explicit images, a bribe or money.

- **Cyber Defamation:** Cyber defamation refers to the damaging of an individual's reputation in the view of others by online media. Bad comments are made to cause harm to a specific individual's reputation.

- **Phishing:** In this type of crime or spam, attackers try to obtain account details or login credentials by impersonating a famous person or address in several ways. Contact, Client ID, IPIN, debit or credit card numbers, card expiry date, and CVV number are examples of email information.

- **Cybercrime Against Property:** These kinds of cybercrimes include intellectual property, copyrights, patents and trademarks. These are those offences that have an impact on a person's property, which are as follows:

- **Intellectual Property Crimes:** Any act that results in partial or complete deprivation of the right of the owner is a crime. The most common forms of intellectual property crimes can be defined as software piracy, copyright infringement, Infringement of patents, trademarks, designs, and services, theft of code of computers, etc.

- **Cyber Squatting:** This means that two individuals claim to have previously registered a trademark, used a mark before someone else, or used a similar name previously. For instance, two similar names, www.books.com and www.boooks.com.

- **Cyber Vandalism:** Vandalism is the destruction or damage of another's property. So, Cyber Vandalism refers to the damage or corruption of data during the interruption or impact of internet service. It can include all catastrophic damage to anyone's computer. These activities can lead to theft of the computer, access to the computer's core or related to the computer.

- **Hacking Computer System:** Hacktivism involves carrying out attacks by gaining unauthorised access to/controlling computers on well-known Twitter accounts, blogging platforms, etc. Due to hacking activities, your data and computers may be lost. According to research, the primary goal of these attacks is to harm a person's or business's reputation rather than make money.

- **Transmitting Virus:** An application known as a virus attaches itself to a system or file and then propagates to other files and computers via the internet. Typically, they corrupt, alter, or remove data from your computer. Worm attacks have a significant impact on people's computers.

- **Cybercrime Against an Organisation:** Cybercrimes against organisations are as follows:

- **DOS attack:** In this crime, the criminals flood the server, system or network with heavy traffic to disrupt the victim's assets and make them unavailable or challenging to use.

- **Email Bombing:** Email bombing is also known as letter bombs. Typically, a botnet, a single actor, or a group of individuals launch email bombing assaults. In the absence of any measures to filter, moderate, or prevent the assaulting traffic, email bombing assaults can continue for several hours.

- **Salami Attack:** Another name for salami interception is salami slicing. In this assault, assailants used internet databases to obtain customer details like as banking information, credit card details, among other things. No complaints were received in this attack, and the identity of the attacker has not yet been determined because the customer is not yet aware of the breach.

- **Deleting of Data:** In this crime, criminals gain access to any data and then unauthorised change or delete the data.

- **Cybercrime Against Society:** Cybercrime against society are as follows:

- **Forgery:** Forgery is the process of creating fake documents, money notes, revenue stamps, mark sheets, and other items using computers, top-notch scanners, and printers.

- **Web Jacking:** The word "web jacking" comes from the word "hijacking." In this attack, an attacker sets up a false website, and when the user clicks on the link, a new page opens with questions asking them to select a different link. If the victim presses the seemingly genuine link, they will be taken to a phoney webpage. These assaults are designed to hack or access, and control other websites. The attacker can also change the information on the victim's website.

- **Cyber Terrorism:** Using computer resources to carry out terrorist acts and to threaten or compel others.

- **Cyber Pornography:** Pornographic magazines created with computers (for publishing and printing the content) and the Internet (for downloading and sharing pornographic images, texts, and other content) would fall under this category.

Why Cybercrime Is Rising in India: Key Factors

The reasons for the increase in cybercrime in India are as follows:

- **Rapid Digitalization:** In recent years, India has experienced a digital transformation. Nowadays, all businesses and individuals depend on the internet. Adopting new technology in all sectors creates more opportunities for cybercriminals to attack easily.

- **Lack of Awareness:** A large number of people in India remain unaware of the potential threats posed by cybercrimes. Many users and businesses do not follow strong security practices, making them an easy target for cybercriminals. Lack of regular cybersecurity training and awareness campaigns leaves both consumers and employees susceptible to social engineering and fraud.

- **Cross-Border Challenges:** It is very difficult to find cybercriminals because cybercriminals can operate from anywhere. If they are operating from outside India, then it is very difficult to arrest them.

Prevention of Cybercrimes

Several strategies for preventing cybercrimes are described below.:

1. **Use of Internet Security Suite:** An internet security program combined with an antivirus program saved you from:

- Preventing accidental harmful downloads
- Preventing harmful installations made by accidentals
- Avoiding becoming a victim of MTTM attacks.
- Protection from phishing.

1. **Use a Strong Password:** Always make sure your password is secure enough to be practically undestroyable. Strong passwords need to be at least 12 characters long and have a variety of uses of letters, symbols and numbers. Your password can be

changed often, so that the password and saved data might be hard for hackers to obtain.

1. **Keep Your Software up-to-date:** Although developers put a lot of effort into creating secure software, and this software is thoroughly tested by security teams, unfortunately, many security vulnerabilities have been introduced during software distribution. Companies are aware of this fact and frequently release updates to fix this. This is why these updates are very important, no matter how annoying they can be. They help prevent attacks that can easily bypass your computer's antivirus program.

- **Securing Your Phone:** Many individuals are unaware that malware attacks, including computer viruses and hackers, can also affect their mobile devices. Do not forget to download software from reliable sources. Avoid downloading apps or software from unidentified sources. Keeping your operating system updated is mandatory. Use a secure screen lock and make sure you have antivirus software installed. Otherwise, anyone could obtain all of your data if you misplace your phone. Hackers can use your GPS to install software that tracks your every move.

- **Avoid Identity Theft:** Aadhar card and Pan card contain every sensitive Information like fingerprints, banking details, etc. So don't share these details with anyone. Always try to avoid sharing your sensitive information on social media. Don't share any Aadhar OTP or any type of OTP with anyone.

1. **Data Protection and Backup:** Always back up important data and store backup in secure folders. Always store data in an encrypted form to safeguard sensitive data from unauthorised access.

Analysis of Cybercrime in India

Cybercrime is becoming a growing problem in India. In recent years, cybercrime has increased significantly in India. One of the most common cybercrimes in India is financial loss, such as online fraud and phishing attacks. These crimes mostly target victims who fall into the hands of fraudsters and provide their personal and financial information. Other types of cybercrime in India include cyberbullying and cyberstalking, which include sending threatening or harassing messages, spreading rumours and creating fake accounts on social media platforms.

The Indian government has taken several steps to combat cybercrime, including the establishment of the NCCRP and CCIC Under the Ministry of Home Affairs. These measures aim to increase online security awareness, as well as cybercrime reporting and investigation. Even after

taking these steps, cybercrime continues to increase in India, and more needs to be done to combat it. These include strengthening cybersecurity infrastructure, improving law enforcement, and educating the public on online security.

- **Measures taken by the Government:** India has taken several steps in previous years to handle cyber law issues and strengthen its cybersecurity posture. These initiatives include: Information Technology (IT) Act, 2000. The Information Technology (IT) Act, 2000, is the first statute in India to regulate cybersecurity. It covers mostly common cybercrimes like data breaches.

Cyber Offences Under the Information Technology Act, 2000

The IT Act described the following cyber offences and their punishments.

- **Section 43:** This section deals with those crimes in which unauthorised access, property damage or disorder of computer systems or network resources is included.

- **Section 66:** This section deals with those offences whose main intention is causing financial loss or damage, or identity theft of another person.

- **Section 66A:** This section deals with the offence of sending an offensive photo or message through communication services or apps. This section has been struck down by the Supreme Court's order on dated 24th March, 2015.

- **Section 66B:** This Section deals with those crimes in which any stolen computer resources or communication devices are accepted.

- **Section 66D:** This Section deals with those cybercrimes which are committed by personation. Personation means representing someone in behaviour or actions.

- **Section 66E:** This Section deals with crimes in which any person's private photo is captured or published without their consent. Which directly violates their right to privacy.

- **Section 66F:** This section addresses crimes related to terrorism committed using electronic devices, which directly affect the integrity, unity, and security of India.

Penalties / Punishment Under the Information Technology Act, 2000

The Information Technology Act 2000, governs all the penalties for cybercrime in India. Every specific cybercrime has a severity of penalties. Some common penalties prescribed under the IT Act as:

- **Section 43:** The punishment for illegal access or interference with the computer system or resources is a fine of up to Five Lakh Rupees or confinement of up to 3 years or both.

- **Section 66:** If the attack is done to cause unlawful or damaging damage, the offender can be given a sentence of up to 3 years in prison and a fine of up to Two Lakh Rupees.

- **Section 66C:** The punishment for cyber identity theft is a fine of up to one lakh Rupees or Confinement of up to 3 years or both.

- **Section 66 E:** The penalty for capturing, publishing the image of a person or a private image without their permission is confinement that may be extended up to 3 years and a fine.

- **Section 66 F:** The punishment for cyber terrorism is confinement, which can extend up to life imprisonment.

1. **National Cybersecurity Policy, 2013:** The National Cybersecurity Policy was launched in 2013 to create a protected cyber ecosystem. The policy includes several measures aimed at improving the country's cybersecurity infrastructure and increasing public knowledge on cybersecurity.

1. **Cyber Swachhta Kendra:** Cyber Swachhta Kendra is a cyber-attack network removal and malicious software analysis centre started by the CERT in India. The centre helps users in detecting and removing malware from their devices.

1. **National Critical Information Infrastructure Protection Centre (NCIIPC) :** NCIIPC was formed to protect the sensitive information of the country. Its mission is to identify and mitigate threats to critical information and help organisations maintain the security of their systems.

- **Cyber Pravah:** Cyber Pravah is a quarterly newsletter published by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs. It provides insights into cybercrime trends, statistics, initiatives, and awareness programs undertaken by the government to combat cyber threats.

Overall, the Indian government has taken several steps to strengthen its cybersecurity foundations and address cyber law issues. However, cyber threats continue to increase, and governments need to be vigilant and protect against these threats.

Judicial Activism to Cyber Law in India

In recent years, Indian courts have been more actively examining and evaluating cyber law, leading to a rise in judicial oversight and interpretation of digital legal frameworks. Judicial discretion refers to the inclination of judges to interpret and apply law broadly and flexibly to resolve social, economic and political issues beyond strict jurisdiction. Here are some examples of judicial decisions on Indian cyber law:

- **Right to Privacy:** The right to privacy is protected under Article 21 of the Constitution, and it is a fundamental right. The ruling plays an important role in shaping the understanding of India's cyber laws, especially the Information Technology Act, 2000.

-
    - **Intermediary Liability:** The IT Rules, 2021, which impose stricter liability on social media intermediaries, have been challenged in several courts in India. The courts are working to interpret and implement these laws and have given several decisions on vicarious liability.

- **Net Neutrality:** The Telecom Regulatory Authority of India (TRAI) published directives in 2016 that allow mobile phone users to charge different rates for different types of internet content.

These provisions have been challenged in the courts in India, which play a major role in interpreting and implementing the provisions of the Act. The growing judicial involvement in cyber law in India is shaping its evolution, with courts playing a crucial role in interpreting and strengthening legal frameworks for digital issues. The courts have taken on the task of interpreting and implementing cyber law to promote social justice, protect fundamental rights and ensure that the tools are used effectively by the public.

Conclusion

In conclusion, we would like to say that cybercrime is a developing threat in India, and the government and citizens need to take effective measures to protect themselves. Although the Indian government has passed many laws related to cybercrime, their effectiveness is still questionable. A lack of awareness and comprehension of these laws, coupled with insufficient cybercrime measures and ineffective investigations, is hindering their enforcement.. It has been involved in many international criminal cases such as drug trafficking, human trafficking, terrorism and money laundering. Digital evidence will become increasingly prevalent even in traditional crimes, and we must be ready to face this new challenge. New skills, technologies and investigative techniques must be used globally to detect, prevent and respond to cybercrime.

References

1. National Crime Records Bureau, *Crime in India 2022 – Volume 2* (Government of India, 2022) **https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf** accessed date May 3, 2025.
2. Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors. AIR 2017 SC 4161 (India).
3. Adv. Prashant Mali, "Classification of Cyber Crimes" (*Lawyers club India*, August 7, 2009) <https://www.lawyersclubindia.com/articles/classification-of-cybercrimes–1484.asp> accessed May 3, 2025
4. GeeksforGeeks, "What Is Cyber Vandalism and How to Avoid It?" (*Geeks for Geeks*, April 3, 2024) <https://www.geeksforgeeks.org/what-is-cyber-vandalism-and-how-to-avoid-it/> accessed May 3, 2025
5. GeeksforGeeks, "Web Jacking" (*Geeks for Geeks*, February 20, 2020) <https://www.geeksforgeeks.org/web-jacking/> accessed May 4, 2025
6. Agrawal A, "Cyber Crime Against Property in India" (*Law Bhoomi*, April 22, 2024) <https://lawbhoomi.com/cyber-crime-against-property-in-india/> accessed May 3, 2025
7. Next IAS, "Cybercrime in India: Types, India's Vulnerability & Solutions" (*NEXT IAS – Made Easy Learnings Pvt. Ltd.*, October 20, 2024) <https://www.nextias.com/blog/cybercrime-in-india/> accessed May 4, 2025
8. Natani S, "India Projected to Lose Rs 20,000 Crore to Cybercrime in 2025: Cloud SEK Report" (*The420.in*, March 5, 2025) <https://the420.in/india-cybercrime-loss-2025-cloudsek-report/> accessed May 4, 2025

1. GeeksforGeeks, "How to Protect Yourself From Cyber Attacks?" (*Geeks for Geeks*, October 6, 2019) <https://www.geeksforgeeks.org/how-to-protect-yourself-from-cyber-attacks/> accessed May 5, 2025
2. The Information Technology Act, 2000
3. Umar N, "Cyber Crime in India" (*International Journal of Law Management & Humanities*, July 25, 2023) <https://doij.org/10.10000/IJLMH.115512> accessed May 6, 2025.

4. Shreya Singhal vs. Union of India, AIR 2015 SC 1523.
5. Admin, "Net Neutrality – Key Facts for UPSC GS-III" (*BYJU'S*, June 3, 2016) <https://byjus.com/free-ias-prep/net-neutrality/> accessed May 6, 2025