

# CYBER LAWS IN INDIA

SAKSHI SAKPAL

KERALEEYA SAMAJAM MODEL COLLEGE , DOMBIVLI

## 1]ABSTRACT

Cyber Law is like a legal rule or policy which should be followed in our daily life to stay out of any kind of trouble. In the following research we are going to focus on the importance of Cyber law and its features, how it operates around the three major categories of cyber crime; against individuals, against property, against the Government and how half of the users are unaware about cyber crime and cyber laws.

**KEYWORDS:** Cyber Law, Features, Objectives, Cyber Crime, Cyber Laws in INDIA.

## 1] INTRODUCTION

The use of internet and computer technology in our daily life has taken a rise over the past few years which has led to the rise in a new form of crime i.e. Cyber Crime. Cyber law protects the users from any harm that can take place because of any online criminal activity. Cyber Law is crucial as it focuses on almost every aspect of activities done on Internet, World Wide Web and Cyber space. It has given a legal definition to the idea of secure digital

signatures that might be required to be passed through a system.

Cyber crime is complex as there are no geographical boundaries to the cyber world. The primary source of cyber law in India is the Information Technology Act, 2000. The importance and scope of cyber law is ever increasing as we become more and more dependent on the internet and technologies related for our day to day life.



## 2] BACKGROUND

### Cyber Crime?

Any crime with the help of computer and telecommunication technology.

### Categories of Cyber Crime

#### 1. Against a Person

- Cyber stalking
- Impersonation
- Loss of Privacy
- Transmission of Obscene Material
- Harassment with the use of computer

#### 2. Against Property

- Unauthorized Computer Trespassing
- Computer vandalism
- Transmission of harmful programs.
- Siphoning of funds from financial institutions
- Stealing secret information & data
- Copyright

#### 3. Against Government

- Hacking of Government websites
- Cyber Extortion
- Cyber Terrorism
- Computer Viruses

### Need For Cyber Law

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet

was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum. When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

## 3] DATA & RESULT

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

List of offences and the corresponding penalties.

Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyber terrorism	Imprisonment up to life.
67	Publishing information which	Imprisonment up to five years,

	is obscene in electronic form.	or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to ₹100,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.

71	Misinterpretation	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to ₹500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to ₹100,000
74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to ₹100,000

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgement found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new

cyber laws. Hence, the need for enactment of relevant cyber laws.

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace

### Importance of Cyber Laws

- We are living in highly digitalized world.
- All companies depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in cyber crime cases, important evidence is found in computers/ cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.
- Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber law is extremely important.

#### **4] CONCLUSION**

To sum up, though a crime free society is perfect and exists only in illusion, it should be constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay.

Hence, it should be the tenacious efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes. It should be the duty of the three stake holders viz. i) the rulers, regulators, law makers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.

#### **ACKNOWLEDGEMENT**

This research paper belongs to a "correspondence study". I would like to express my sincere thanks to all the teachers who helped us throughout

I am also grateful to, Head of Department. This acknowledgment will remain incomplete if I do not mention the sense of gratitude towards our

esteemed Principal who provided me with the necessary guidance, encouragement, and all the facility available to work on this project.

Last but not least I would like to thank my classmates who have helped me a lot with moral support and encouragement.

#### **REFERENCES**

1. <https://www.infosecawareness.in>
2. <https://www.meity.gov.in/content/cyber-laws>
3. <http://www.legalserviceindia.com/>