Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Violating these Cyber Laws can Land you in Jail!

Pranjul Bajpai[a]

[a]Symbiosis Law School, Nagpur, India

Received 29 April 2022; *Accepted* 17 May 2022; *Published* 23 May 2022

The Internet has flipped our world on its head. It has transformed communication to the point where it is now our favourite medium of daily contact. With the advancement of technology, the need for internet access is expanding in all aspects of life. Whether it's education or banking, practically everything has gone online. On the one hand, technological development is beneficial, but it also has certain negative consequences. Cybercrime is another drawback of these technological advancements. Such criminal activities are carried out by individuals, organizations, and groups. This dramatic surge in internet use has resulted in a significant increase in the rate of cybercrime. Here the necessity for cyber law has become critical to control cybercrime. This article discusses several laws and how violating them might put you in jail. The objective of this article is to provide a basic overview of cyber laws and the meaning of cybercrimes. This paper will help you understand the different cyber laws in India.

Keywords: *cyber laws, internet, education, cybercrimes.*

INTRODUCTION

"Everyone should wish to guarantee that we have the cyber tools we need to investigate cybercrime, guard against it, and prosecute those who perpetrate it."

The Internet, which connects different networks all over the world, has eased the exchange of data and information. Security risks have developed in recent years as data and information are transported between networks in different locations. Few people have also used the internet for illegal objectives, such as unauthorized network access, fraud, and so on. These illegal internet-related behaviours are referred to as Cyber Crimes. With the increasing popularity of online activities such as online banking and shopping, it is a word that we constantly hear in the news these days. As a result, to deter and punish cybercriminals, "Cyber Law" was enacted. Cyber Law is also known as web law since it is a branch of the legal system that deals with the Internet, Cyberspace, and other legal matters such as online security and privacy. Cybercrime is defined as an illegal action that targets or uses a computer, a computer network, or a networked device. Furthermore, it is criminal conduct that entails several difficulties ranging from theft to the use of your system or IP address as a tool for executing a crime. Keeping the objectives in mind, this article has been organized into parts to offer a basic introduction to what cyber law is. The chapter also sheds insight on the various cyber laws in India.

CYBERLAW

The term "*Cyber Law*" relates to legal difficulties with the use of communication technology, namely "cyberspace," or the Internet. It is an attempt to reconcile the challenges raised by human behaviour on the Internet with the legacy legal system that applies in the actual world. The attempt to apply physical-world standards to human behaviour on the Internet is known as cyber law. In India, the Cyber legislation is known as the Information Technology Act, 2000, as amended by the IT (Amendment) Act, 2008[1]. It has a separate chapter XI titled "Offenses" in which numerous internet crimes are recognized as criminal offences punishable by imprisonment and fine. To comprehend cyber law, we must first define cybercrime, which refers to any criminal behaviour conducted via computers, the Internet, cyberspace, or the worldwide web.

[1] Information & Tchnology (Amendment) Act, 2008

CYBERCRIME

"Cybercrime" does not have a legal or regulatory definition. Everything that has to do with computers, information technology, the internet, or virtual reality is referred to as "cyber." As a result, "cyber-crimes" are now defined as crimes committed with the use of computers, information technology, the internet, or virtual reality technology. These are usually illegal activities that need the use of a computer and a network. Because it is no longer necessary for the criminal to be physically present when committing a crime, the quantity of cybercrime activities is increasing as a result of the internet's growth.

CYBER LAWS AND THEIR NEED IN INDIA

The inventors of the Internet had no notion that it would grow into an all-encompassing technology that might be misused for criminal purposes, necessitating regulation. These days, there are a lot of unsettling things going on online. Because of the anonymity provided by the Internet, it is simple to engage in a wide range of unlawful activities while remaining anonymous, and astute persons have been abusing this feature of the Internet to conduct criminal operations in cyberspace. As a result, India now has to pass Cyber laws. Both the Information Technology Act (IT Act) and the Indian Penal Code cover cybercrime. The Information Technology Act of 2000, which went into force on October 17, 2000, governs cybercrime and Internet trade. The IT Act was updated in 2008. [2]The Act defines and penalizes cybercrime. This IT Act amended the Indian Penal Code, 1860[3], and the Reserve Bank of India Act[4]. The purpose of this Act is to safeguard e-government, e-banking, and e-commerce activities.

SOME IMPORTANT SECTIONS OF THE IT ACT

[2] Information & Technology (Amendment) Act, 2008
[3] Indian Penal Code, 1860
[4] Reserve Bank of India Act, 1934

Section 65[5]: Attempting to tamper with computer source documents. If found guilty, the penalties include imprisonment for up to three years and/or a fine of up to Rs two lakh.

Section 66[6]: Unauthorized use of computer systems and networks, or hacking into computer systems If found guilty, you may face up to three years in prison and/or a fine of up to Rs 5 lakh.

Section 66C[7]: A person who fraudulently uses an electronic password or Digital Signature gave to him for authorized use in the position of servant or agent faces up to three years in prison or a fine of up to Rs. 1 Lack.

Section 66D[8]: A person who defrauds someone using a computer or a communication device might face up to three years in jail and a fine of up to one lakh INR.

Section 66E[9]: This law makes it illegal to take photos of intimate areas, publish them, or transmit them without the subject's consent. If convicted, you might face up to three years in prison and/or a fine of up to Rs 2 lakh if you are proven guilty.

Section 66F[10]: If a person denies authorized personnel access to a computer resource or attempts to penetrate/access a computer resource without authorization to endanger the nation's unity, integrity, security, or sovereignty, he or she may face life imprisonment.

Section 67[11]: It is a crime punishable by imprisonment for up to five years or a fine of up to Rs. 1 Lack. if anybody publishes or transmits any message or picture that is insulting in nature and may affect the alleged person's image in the eyes of others.

Section 71[12]: If any individual makes any deception before the Certifying Authority or conceals any material truth from them to obtain any license, they will face up to two years in prison or a fine of up to Rs. 10,000/-.

---

[5] Information & Technology (Amendment) Act, 2008, s 5
[6] Information & Technology (Amendment) Act, 2008, s 66
[7] Information & Technology (Amendment) Act, 2008, s 66C
[8] Information & Technology (Amendment) Act, 2008, s 66D
[9] Information & Technology (Amendment) Act, 2008, s 66E
[10] Information & Technology (Amendment) Act, 2008, s 66F
[11] Information & Technology (Amendment) Act, 2008, s 67

SOME IMPORTANT SECTIONS OF THE INDIAN PENAL CODE, 1860

Section 379[13]: Without the express permission of the rightful owner, anybody who unlawfully takes objects or electronic documents from his possession faces up to three years in prison, a fine, or both.

Section 420[14]**:** Under this section of the IPC, cybercrimes such as building bogus websites and cyber frauds are penalized by a seven-year prison sentence and/or a fine. This part of the IPC is dedicated to offences involving the theft of passwords to perpetrate fraud or create bogus websites.

Section 463[15]**:** It is possible to generate fake documents or electronic data. Crimes like email spoofing are now punishable by up to seven years in prison and/or a fine under this section.

Section 468[16]**:** A seven-year jail sentence and/or a fine can be imposed for forgery with the intent to deceive. One of the offences punished under this law is email spoofing.

CYBERCRIME SCENARIO IN INDIA

- ***The Bank NSP Case***

In this situation, a bank's management trainee became engaged to be married. The pair used to send a lot of emails from the company's computers. After a while, they broke up, and the young girl created a series of fictitious email accounts, such as "Indian bar organisations," and used them to send emails to the boy's abroad clients. She did this on the bank's computer. The boy's firm lost a large number of customers and went to court against the bank. The bank was held responsible for emails sent using the bank's system.

- ***Bazee.com case***

---

[12] Information & Technology (Amendment) Act, 2008, s 71
[13] Indian Penal Code, 1860, s 379
[14] Indian Penal Code, 1860, s 420
[15] Indian Penal Code, 1860, s 463
[16] Indian Penal Code, 1860, s 468

In December 2004, the Chief Executive Officer of Bazee.com was detained for selling an objectionable compact disc (CD) on the website, and the CD was also sold out in the Delhi market. The Delhi Police, and hence the Mumbai Police, were called in, and the CEO was eventually released on bail[17].

- ***Parliament Attack Case***

This case was handled by the Bureau of Police Research and Development in Hyderabad. The terrorist who assaulted the Parliament was apprehended using a laptop. The laptop confiscated from the two terrorists who were killed down on December 13, 2001, when the Parliament was under siege, was delivered to the BPRD's Computer Forensics Division. The laptop contained several proofs that affirmed the two terrorists' motives, most notably a sticker of the Ministry of Home that they had created on the laptop and affixed to their ambassador's car to gain entry into Parliament House, as well as a fake ID card with a Government of India emblem and seal that one of the two terrorists was carrying. The emblems (of the three lions) were meticulously scanned, and the seal was skilfully constructed together with a Jammu and Kashmir residence address. However, rigorous examination revealed that everything was forged and created on the laptop[18].

SUGGESTIONS

1. It is nearly difficult to use an internet platform without disclosing any personal data; thus, one should exercise caution while disclosing any personal information online.
2. It is critical to keep a lookout for bogus email communications, and such emails should not be answered if they request personal information. In addition, email addresses should be kept private.
3. When engaging in online activities, it is essential to pay attention to privacy regulations on websites and avoid bogus websites that steal personal information.

[17]*Avnish Bajaj v State (N.C.T.) of Delhi* (2004) 3 CompLJ 364 Del
[18]*Shoukat Hussain Guru v State (NCT) Delhi & Anr.* (2008) Writ Petition (Criminal) No. 106/2007

4. The reaction to transgressions against women on the internet must be viewed as part of a larger campaign against harassment and abuse. Broader initiatives should be launched because it is essentially a people-centered issue.
5. Keeping up with the rate of change is essential. Keeping up with technological changes is a task that must be solved, as most internet crimes are committed owing to a lack of information and awareness among users.
6. Promoting women's leadership and decision-making in society requires a combined effort from the media, clubs, associations, and women's media networks.
7. Effective and efficient online vigilance, monitoring, and reporting against violence and cybercrime.
8. There should be an E-portal where women may report their difficulties online without fear of being stigmatized for engaging the police. In addition, a criminal database should be kept, which might aid in law enforcement.
9. Women should be educated on how to use online media platforms and should follow proper processes. They must be informed of their legal rights on the internet.
10. Education systems must address current challenges of online crimes, and public knowledge about safe internet use should be disseminated.
11. The government should impose stricter controls on Internet Service Providers (ISPs) since they have a complete record of the data that is accused by people using the web. In addition, they should report any suspicious activity to avoid crimes at an early stage.

CONCLUSION

As a result, the term "cybercrime" refers to a very broad group of acts. Some of them are similar to non-computer offences, such as theft or fraud, except that a computer or the Internet is used to commit the crime. Others, such as hacking, are inextricably linked to computers. The government must ensure the security of the state's digital network and systems that contain critical public information and must take meaningful efforts to do so. The lockdown showed weak cyber laws and after a couple of 5% spike in cybercrime, the government switched some priority to the current side, and cyber-centres and cyber police became operational. The

government is issuing an alert to the general public to avoid falling victim to such only crimes and to take care while entering their information and passwords on internet sites. However, the government must also enact stricter laws, processes, and means to apprehend hackers. Furthermore, various security software must be implemented to protect company networks and hospital computers from hackers. These are some of the short-term answers during the lockdown, but there also has to be some modification within the present Information Technology Statute, 2000 because it is a comprehensive act that does not contain many of the opposing parts that are riddled with cyber-crime.