Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

A Primer on Cybercrimes

Avni Mishra[a]

[a]University of Mumbai Law Academy, Mumbai, India

Received 03 August 2021; *Accepted* 23 August 2021; *Published* 01 September 2021

With evolving technology and internet space, cybercrime has become the most disruptive threat to the users of the internet. Cybercrime is also a very underrated form of crime by regulatory bodies. As individuals and organisations are more reliant on information technology and the internet, they are also exposed to various threats and crimes attached to it. This article focuses on the information and the awareness that both individuals and organisations must have regarding their cyberspace safety. Furthermore, the remedies available by the law are also briefed and this article concludes with the precautionary guidelines laid down by the National Cybercrime Training Centre for internet users.

Keywords: *cyberspace, cybercrime, information technology, internet*

INTRODUCTION

"Cyberspace", can be referred to as a virtual computer world created by the connection between two or more devices, links between computers, the internet, etc. During the earlier emergence of the internet, the term cyberspace was used for the 'location' where people connected and interacted with each other, played online games, discussed socio-economic and political opinions, etc. This location has now become a major social and commercial platform that connects people from all over the world.

From the invention of electricity to computers, smartphones, and the internet, technology has played a major role in all of our lives. How simple it is now to get connected to a friend or a family member sitting across the other corner of the world. From mere necessities to comfort and luxury, technology has made everything easier for us. Multiple examples can be given on how technology has made everything easier for us, but this article focuses on "cyberspace" and the crimes associated with it. Technology is ever developing and everything around us is evolving. We have become a generation almost utterly dependent upon the internet. From social media to simple day to day necessities like ordering groceries.

India has become the second largest online sphere in the world with over **560 million internet users** across the nation. It is also predicted that the number of internet users in India is going to rise up to 970 million by 2025[1]. With such a heavy number of people using the internet which is rising rapidly, they are also exposed to numerous criminal activities such as, frauds, threatening, blackmailing, etc happening all over cyberspace.

WHAT IS CYBERCRIME?

Cybercrime can simply be defined as criminal activity that involves the use of a computer, network or internet, technology, etc. With evolving technical space, the opportunities in every sphere are evolving. Cybercriminals are highly skilled people using their skills and proficiency for illegal and mala fide activities. The distinguishing factor between a traditional crime and cybercrime is the use of computers or technology in the commitment of the crime. Any kind of criminal activity that is executed by the use of the computer, internet, or any electronic device comes under the umbrella of cybercrime. For example, damage to personal information or data stored in a device by hacking the device is also cybercrime and online stalking on social media platforms is also a cybercrime.

Cybercrime is not defined under any statute in India. However, The Information and Technology act, 2000 came into force looking forward to the new platform that was being built, the virtual or cyber world. There are numerous ways in which a criminal can execute a

[1] J Degenhard, 'Mobile Internet Users In India 2025 | Statista' (*Statista*, 2021) <https://www.statista.com/forecasts/1144654/mobile-internet-users-in-india> accessed 25 July 2021

criminal activity just by sitting behind a device. So, it becomes very essential for every user of the internet, be it organisations or individuals, or government, to be aware of every possibility of getting online maliciously affected.

The types of cybercrimes are mostly committed against

1. **Individuals:** Cybercrimes against individuals majorly include banking fraud, hacking of personal data, cyber harassment and stalking, distribution or transmission of pornography and child pornography, personal financial fraud, identity theft, online libel, and slander.
2. **Property:** Cybercrimes against property include a computer system or computer network or communication device trespassing, vandalism, theft, etc through electronic medium.
3. **Government:** Cyber terrorism is an example of cybercrime against the government. The growth of technology and the internet has acted as another medium to threaten the government, international institutions and terrorise civilians.

TYPES OF CYBERCRIME

There exist several types of cybercrimes happening and affecting the people, organisations, or the government. Depending upon the nature of the crime and harm the victim has suffered, below listed are the cybercrimes we come across[2]:

1. **Virus Attacks:** It is a type of attack that happens to your computer system or even mobile phones via the internet. These viruses get downloaded unwantedly or automatically by just opening or clicking on some link to your devices causing theft/damage to your data, system, or software, etc. It may also cause irreversible and large-scale damage.
2. **'Hacking':** The word hacking is generally associated with malicious activities but it is not necessarily done for wrong purposes always. The distinguishing element behind ethical hacking and unethical or malicious hacking is the motive or intention of the

[2] *Ibid*

person doing it. Hacking simply means breaking into some other system or network or device. When a person is able to break into some other system or network or device, he/she is also able to access the data or information. Just like somebody breaking into your house! Now, this becomes ethical when it is done with the authorisation of the person whose device or system is to be broken into for security reasons or any general safety issue. Unfortunately, most of the hacking cases that come into sight are unauthorised, malicious, and done for illegal or wrong purposes. Stealing personal data or important financial information, using identity to do illegal activities, getting access to someone's online activities, sending bugs or viruses purposely to cause damage to a system, etc are few examples of mala fide hacking.

3. **Phishing:** Phishing is a type of cyber-attack done by sending emails or attachments, tricking the recipient to click on something, or open a link that may take the recipient to similar looking malicious websites or may ask the recipient for some confidential information like passwords or OTPs in a fake website.
4. **Cyberstalking:** When someone keeps an eye on your online activities or your social media activities and deliberately makes your feel uncomfortable or threatens you by either sending messages continuously or any such activity comes under cyberstalking.
5. **Salami Slicing:** It is a technique used by hackers to steal money or resources a little bit at a time so that it is unnoticeable in your bank account. The target people remain unaware as the amount which gets deducted is very small. Criminals do it to numerous people and over a period till a large amount of money or resources is accumulated with them. This slicing technique is mostly used to steal money.
6. **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** DoS is a type of attack meant to shut down a device or network, making it inaccessible to its users. DoS attack floods the user service with traffic, making a website or network unavailable. DoS attack is a system-to-system attack whereas, in a DDoS attack, multiple systems attack a single system. Both DoS and DDoS target a system or network aiming to cause obstruction.

7. **Ransomware:** It is a type of software attack in which the attacker usually encrypts the victim's data or information and threatens to publish or damage it if the victim does not pay him/her the ransom fee. It generally happens for money.
8. **Child Pornography:** Images or videos of children (below 18 years of age) involved in sexual activities get distributed, circulated, and traded on the internet. It is a form of child sexual exploitation and is a heinous crime.
9. **Identity theft:** An imposter or a complete stranger uses an individual's personal identification information without the knowledge or consent of the individual to commit fraud or financial harm to any person or organisation.
10. **Digital Piracy:** Imagine putting your heart and soul into a piece of music and getting it copyrighted. Now you come across someone who's stealing or copying your piece of music to distribute or circulate it on the internet or other digital platforms without your consent or knowledge. This is the act of piracy. It can also be defined as illegally reproducing copyrighted material such as music, cinematographic film, books, etc.

TYPES OF CYBERCRIMES RECOGNISED BY THE INDIAN STATUTES AND THEIR REMEDIES

With the growth of technical developments in the country, the need for a regulatory body or regulation became the priority for the legislative body of the country. The Indian Parliament enacted the Information and Technology Act in 2000,[3] looking forward to the need for regulation. Listed below are the offences defined under Information and Technology (Amendment) Act 2008,[4] along with the remedies available to us.

SECTION	OFFENCE	REMEDY
43	Damage to computer, computer system or computer network	Damages by way of compensation to the person affected not

[3] Information and Technology Act 2000
[4] Information and Technology (Amendment) Act 2008

		exceeding Rs. 1 crore
43A	Failure to protect personal data or information	Damages by way of compensation to the person affected not exceeding Rs. 5 crores
44 (a)	Failure to furnish document, return or report to Controller or the Certifying Authority	Penalty not exceeding Rs. 1,50,000
44 (b)	Failure to file any return, documents within the time specified	Penalty not exceeding Rs. 50,000
44 (c)	Failure to maintain the book of accounts, records	Penalty not exceeding Rs. 10,000
45	Contravention of any provision or rule under the IT Act	Compensation not exceeding Rs. 25,000 to the person affected or Penalty not exceeding Rs. 25,000
SECTION	**OFFENCE**	**PUNISHMENT**
65	Tampering with computer source documents	Imprisonment up to 3 years or fine which may extend to Rs. 2,00,000 or both
66	Any dishonest or fraudulent act under	Imprisonment up to 3 years or fine which may

	Section 43	extend to Rs. 5,00,000 or both
66A	Sending offensive messages, false information or causing annoyance or inconvenience through computer source or communication device	Imprisonment up to 3 years and fine
66B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years or fine which may extend to Rs. 1,00,000 or both
66C	Identity Theft: Frequently or Dishonestly using an electronic signature, password, or any other identifying information of any person	Imprisonment up to 3 years and fine which may extend to Rs. 1,00,000
66D	Cheating by personation by using computer resource	Imprisonment up to 3 years and fine which may extend to Rs. 1,00,000
66E	Violation of Privacy: Intentional capturing, publishing, or transmitting the image of	Imprisonment up to 3 years or fine not exceeding Rs. 2,00,000 or both

	private areas of any person without his/her consent	
66F	Cyber Terrorism: terror activities by use of computer resource	Imprisonment which may extend to imprisonment for life
67	Publishing or transmitting obscene material in electronic form	On first conviction- Imprisonment up to 3 years and fine which may extend to Rs. 5,00,000 On second conviction- Imprisonment up to 5 years and fine which may extend to Rs. 10,00,000
67A	Publishing or transmitting material containing sexually explicit acts in electronic form	On first conviction- Imprisonment up to 5 years and fine which may extend to Rs. 10,00,000 On second/subsequent conviction- Imprisonment up to 7 years and fine which may extend to Rs. 10,00,000
67B	Publishing or transmitting	On first conviction-

	material depicting children in the sexually explicit act in electronic form	Imprisonment up to 5 years and fine which may extend to Rs. 10,00,000 On second/ subsequent conviction- Imprisonment up to 7 years and fine which may extend to Rs. 10,00,000
67C	Failure to preserve or retain information by intermediaries in a manner prescribed by Central Government	Imprisonment up to 3 years and fine
71	Misrepresentation of material fact to Controller or certified Authority for obtaining any license or certificate(electronic)	Imprisonment up to 2 years or fine which may extend to Rs. 1,00,000 or both
72	Breach of Confidentiality and Privacy	Imprisonment up to 2 years or fine which may extend to Rs. 1,00,000 or both

Most of the cybercrimes penalised by the Information and Technology Act[5] are also covered in the Indian Penal Code. For instance, Section 378 of the IPC,[6] dealing with the theft of

[5] Information and Technology Act 2000
[6] Indian Penal Code, s 378

immovable properties can be read in parallel to Section 43 of the Information and Technology act dealing with data theft. Therefore, Criminal activities such as theft, fraud, misrepresentation, etc defined and penalised under the Indian Penal Code can also be applied to the theft, fraud, or misrepresentation of any information or data in electronic form. Crimes related to technology or committed with the help of technology can be treated as crimes recognised and defined by the Indian Penal Code.

IMPORTANT CYBERCRIME CASES

1. **Melissa Virus** (1999): Melissa virus was the first successful macro virus spread through email attachments in 1999. It was originally contained in a Microsoft Word file which emailed the virus to 50 more email addresses from the victim's address book on opening it. Though it looked like a simple virus back then, it caused damage of $80 million.
2. **WannaCry Ransomware** (2017): It was a famous ransomware attack that spread through devices operating Microsoft Windows. User's files were held as hostages and Bitcoin was demanded in exchange for those files. WannaCry ransomware attack hit around 230,000 computers globally. The ransom demanded by the attackers was $300 worth of Bitcoins which was later increased to $600. Even after paying the ransom, most of the victims didn't get their files/data back.
3. **Cambridge Analytica and Facebook data breach case** (2018): In earlier 2018, Cambridge Analytica, a UK-based analytics firm was alleged to have collected the personal data of the users uploaded on Facebook to influence elections. It allegedly involved a data theft of 5.26 lakh Indian users. Facebook CEO Mark Zuckerberg came forward to apologise for the situation with Cambridge Analytica, calling it a breach of trust and a mistake. The incident highlighted the need for Data Protection laws across the world.
4. **Sony Sambandh Case:** A complaint was filed by Sony India Pvt.Ltd, which runs a website called www.sony-sambandh.com, targeting the NRI (non-resident Indians) audience. The website enables NRIs to send Sony products to their friends or families in

India after having paid online for it. A 24-year-old boy named Arif Azam took a delivery of Sony Color Television in Noida which was ordered under the identity of Barbara Campa. She gave her credit card details and asked for the delivery to be made to Arif Azam. The transaction was processed and payment was successfully cleared by the credit card agency however, after one and a half months, the credit card agency informed the company that this was an unauthorised transaction and the real owner denied having made any such purchase.

An online cheating complaint was filed under Section 418,[7] 419,[8] and 420 of the IPC[9] at the Central Bureau of Investigation, and Arif Azam was arrested. This marked the first cyber crime conviction case in India.

5. **Prakhar Sharma vs State of Madhya Pradesh[10]**: The accused created a fake Facebook account of the victim and uploaded vulgar messages along with photos downloaded from her original Facebook account. The accused was charged under sections 66 (c),[11] 67,[12] and 67 (a) of the Information and Technology Act[13].

We come across these types of cybercrime cases on a daily basis. According to the NCRB report, around 30, 729 cases of cybercrime were reported under the Information and Technology Act and around 13, 730 cases of cybercrime were reported under the Indian Penal Code in 2019 around all States and Union Territories of India[14]. The young generation comprising OD individuals between the age group of 15-24 is more prone to cybercrime as it is the generation most active on the internet.

CHALLENGES IN COMBATTING CYBERCRIME

The key reason behind most of the cybercrime occurring all around the world is financial. Businesses, individuals, organisations are majorly suffering financial losses as an aftermath of

[7] Indian Penal Code 1860, s 418
[8] Indian Penal Code 1860, s 419
[9] Indian Penal Code 1860, s 420
[10] *Prakhar Sharma v State of Madhya Pradesh* MCRC No 377 of 2018
[11] Information and Technology Act 2000, s 66(c)
[12] Information and Technology Act 2000, s 67
[13] Information and Technology Act 2000, s 67(a)
[14] NCRB Cybercrime Report 2019

cybercrime. Along with financial losses, personal data or private information such as bank details, passwords, identification IDs, private photos or videos, etc is being endangered. It has become a major source of mental and emotional harassment, fear in the minds of people, and a negative environment. The very information technology invented to make our lives easier has become a big factor of concern regarding personal information safety, data safety, financial safety, etc.

Some major challenges that are faced in combatting cybercrime are[15]:

1. Unlike most of the traditional crimes, cybercrimes do not leave behind footprints as it is being committed in a borderless, multinational environment behind the curtains of anonymity, making it difficult to find the criminal.
2. Lack of cybersecurity awareness at both individual and organisational levels has been a major challenge.
3. Cybercriminals are highly skilled technically and this high technical skill is lacking in the implementation of counter cybercrime measures.
4. The police and law enforcement bodies are not very well acquainted with high technical skills which make it difficult for them to understand the execution of cybercrime.
5. The lack of efficient provisions and policies has acted as a challenge. For instance, there is still no regulation on the personal data privacy breach issues, regulation of social media and OTT platforms, etc. in India.

CONCLUSION

The growth and developments in Information Technology have also led to advancements in crimes. As the internet is one of the integral parts of our daily lives now, it becomes really important for every user to be aware of the crimes attached to it and take precautionary measures. With the increasing use of cyberspace, cyber crimes are rising rapidly especially against women and teenagers.

[15] *Ibid*

Here are some cyber safety guidelines by National Cybercrime Training Centre for internet users:-

1. Cyber Awareness for Parents: Parents need to have control and a watch on the internet use of children, especially teenagers.
2. Never click on suspicious links or attachments.
3. Never share your passwords or OTPs (One-time passwords) with anyone.
4. Install Anti- Virus Software and keep it updated.
5. Secure your online presence by selecting the right privacy settings and be minimal with your personal information on social media.
6. Beware of fake social media accounts and learn to block anyone who is bullying or stalking you on social media.
7. Disable location settings for social media applications, mobile devices, etc.
8. Report immediately to concerned authorities if you find any content on child pornography over social media or the internet.
9. Any complaint regarding cybercrime can be reported online on Cyber Crime Reporting Portal. (www.cybercrime.gov.in)