C.B.I v. Arif Azim - A Critical Analysis of Cyber Crime in India

By *Shubhi Shukla*[1]

Introduction

During the last 90s Internet was just invented and within the next two decades, it has now become an essential part of our lives. We, humans, depend on the Internet for all our requirements whether it be online shopping, food orders, connecting with friends, studying, purchasing policies, banking etc. It has now covered almost every aspect of our life. As the Internet's usage and benefits grew with time so did the idea of cybercrime. Our society develops and becomes complex at the same time. The use of the Internet did not only ease our lives but also evolved different types of cybercrimes.

What is Cybercrime?

Crimes that are committed by using a network or computer is known as cybercrime. Such criminals either use computer networks or any other networked device as a tool to commit the crime. Their Aim is to fraud, trafficking in child pornography, stealing identity's etc.

Examples of Cybercrime

I. **Malware attacks**

Under this, the networked device is infected with a virus or any other kind of malware and then used for stealing confidential data for any other criminal activity. One of the very famous incidents of it is the WannaCry Ransom Attack of 2017. By using the victim's data this malware was used to steal money from them. This attack was caused in almost 150 countries and affected 2,30,000 devices and caused a financial loss of $4 billion.

II. **Phishing**

Under this campaign, the offender sends some spam mail to your device and once you open it, this undermines the personal safety or the safety of the organisation you work at. Such links or attachments which are sent via mail asks the acceptor to provide them with some confidential information. One of the famous phishing scams of 2018 is in

[1] 1st Year Student of B.A LL.B at Amity Law School, Noida (Batch of 2026).

which that football fans were targeted with lightning up their desire for a free trip to Russia where the World Cup was being hosted. People who fell for such scams resulted in being the victim and they got all their important data stolen.

Another type of phishing campaign is called spear phishing which targeted some specific people and harm the safety of the organisation they work at. In these emails, the victims were tricked by showing it as an important mail received from their superiors.

III. **Cyber Stalking**

Cyber stalking is a crime in which criminals stalk victims' social media account intending to collect confidential information and take a benefit in their name. Sexual harassment, influence, threats are common examples of this type of behaviour.

Cybercrime Cases in India

In the year 2020, India recorded 50,035 cases of cybercrime and it was an 11.8% spike from the cases in 2019. Which amounted to 44,735 cases in a year. There are high chances for an Indian internet user to have fallen for this crime as a victim because 80% of Indian respondents claim to have such experience. U.S online users stand at a second rank with 61% of the respondents being the victim of crime every year.

In the Global Cyber Security Index (GCI) 2020 launched by the International Telecommunication Union, India was ranked as the 10th best country globally on cyber safety factors. In India, out of all the states, Uttar Pradesh reports the largest number of Cyber Crimes that is 11,097, Karnataka at second place with 10,741 cases and Gujarat was at the bottom with 12183 cases reported in the year 2020.

Cyber Laws in India

The rise of the 21st century led to the evolution of cyber law in India. The information technology act of 2000 also known as the IT act deals with several new-age crimes that are born due to computer abuse. The Indian Penal Code 1860, the banker's books Evidence Act 1891, the Indian Evidence Act 1872 and the Reserve Bank of India act 1934 were all amended by the IT act. By stringent legal reorganization, these modifications tried to fit all electronic transactions and

communications by bringing them all beneath the radar. Both IPC and IT act penalise cybercrime and many clauses of both overlaps.

Analysis of C.B.I v. Arif Azim (2013) [Sony Sambandh Case]

Facts of the Case

- In 2013, India made its first-ever cybercrime conviction. It was initiated when Sony India private limited owned website http://www.sony-sambandh.com/ and a non-resident Indian (NRI) who was the victim in the case filed a complaint.
- NRI's while using this service were able to purchase Sony products for their loved ones who reside in India, after making the payment for the purchased product online.
- Sony company guaranteed all its customers that items ordered by them will be delivered to the person whom they intend to send it.
- In the year 2000, a person with the name Barbara Campa registered on the site and ordered some products, that was a Sony colour television and a cordless headphone. She gave all the details of the credit card and also asked the firm to deliver the product to Arif Azim a resident of Noida (UP).
- The credit card company gave clearance and the transaction was complete.
- Once all the due diligence and inspection process was done by the company the products were delivered to Arif Azim.
- For records, the firm took some digital photos of Arif Azim at the time of delivery, to prove that the product was delivered as per the order.
- But after a few days, Sony company came to known about the purchase, that it was illegal and the actual owner of the card has not done any of such payment, the credit card company informed.
- The firm then reported a case of Internet cheating to the Central Bureau of Investigation (CBI).
- An investigation was initiated by CBI under section 418,419,420 of IPC.
- After the investigation, CBI found out that Arif Azim who was a resident of Noida and worked at a contact centre of the city and there he somehow obtained the credit card

number and all the required details of an American National. Which he misused and ordered the products at the company's website

- CBI had collected enough evidence to conclude the case against Arif and hence he accepted the same. He was held liable under sections 418,419 and 420 of the Indian Penal Code.

Issues Raised

I. *Whether the IPC can apply to the matters of cybercrime?*

II. *What is the severity of the offence and what is its punishment?*

Laws for Cybercrime in India

Under the Indian Penal Code, 1860

- ✓ Section 418 of IPC states that if someone cheats the other person having known that this act of his can cause unjust harm to others. So in such a case, he can be punished with imprisonment of three years or a fine or both.
- ✓ Section 419 states that whoever cheats by personalization will be held liable and shall be punished for a fine or imprisonment as described by the judge which may extend to three years or with both.
- ✓ Section 420 states that anyone who induces the victim to deliver any property to any person or to make alter or destroy the valuable security or anything that is capable of being converted Into valuable security by the means of cheating with dishonest intentions shall be punished with imprisonment as per the description of judge or for a term of up to seven years and shall be also liable to fine.

The Information Technology Act, 2000

- ✓ **Section 66** This section deals with offences related to computers and their punishment.

Judgement

Based on all the evidence and witness provided by the CBI to the court Arif Azim was held liable under sections 418, 419 and 420 of the Indian Penal Code. And found him liable for the crime of cyber fraud, however court after considering the age of the offender and severity of the offence sentenced the accused to a year of probation.

Conclusion & Recommendations

Cyber Crimes in India is attaining an alarming position now. It is a wake-up call for every individual to take proper due diligence while using the Internet, any individual who is using the Internet must know how to deal with it and keep herself protected from any cyber-attacks. People should avoid opening links and other attachments from an unknown individual or site. People should be aware of the laws available in India regarding Cyber Crime. So that if in case they suffer from any such harm they know how and whom to approach with the matter.

Moreover, I would also like to make few recommendations how one can prevent Cyber Crimes in the following manner:

- ✓ **Strong passwords:-** Usage of different passwords and username combinations that are hard to guess for another user can help in protecting you from cybercrime.
- ✓ **Private account:-** All the social networking profiles like Facebook, YouTube, Instagram etc keeping them private and being careful towards the content you post online will help in preventing cybercrime because these things posted online will be available in the public domain.
- ✓ **Securing the device:-** Your device whether it be mobile, computer or laptop it is vulnerable to some malicious software. There are certain steps to be taken to protect your device from any external intrusion. Example downloading files from a trusted source, installing antivirus software, keeping your device updated etc.
- ✓ **Protecting data and identity:-** Using encryption for important files in the device can help in protecting your important data. Also while giving your details such as your name, address, phone number etc in the public domain it is important that you make sure that the site is secure.
- ✓ **Security software:-** To maintain online security and safety software play an essential role. Such software is the firewall, antivirus etc it Keeps a check on what and who can communicate with your computer online.