CYBER CRIME VICTIMIZATION AND LAW

Humaira Gull,

PhD Scholar,
School of Law, University of Kashmir, J&K, India.

Abstract

India's internet usage is on the rise. It has opened up new avenues in every industry, from entertainment to business to sports. Using the internet comes with its own set of positive as well as negative aspects, with cybercrime being one of the most troubling.[1] Increasingly, cyber crime is becoming a big problem. International governments, law enforcement agencies and intelligence units began to respond. Cross-border cyber security initiatives are taking form. The Indian police have set up specific cyber units all around the country and have begun training its officers and agents in cybercrime awareness. This article aims to shed light on cybercrime in India by providing a brief overview. It is based on a number of stories from various media outlets and online portals.

Keywords: **Cyber crime, Internet, Hacking, Victimization, Phishing, Vishing, Morphing**

I. INTRODUCTION

India made the decision to go digital, which gave the country access to new power. Exploration is made possible thanks to the internet, which has made life more convenient. As they go into the unknown, they're able to connect with people from all over the world at any time. Therefore, cyber thieves have gained access to the digital sphere.[2] Law enforcement organisations around the country are grappling with a growing problem: cybercrime. The use of cyber platforms by criminals to harass a victim is on the rise. The creation of Digital India is the result of a number of technology and innovation advances. Many people do not use computers, the internet, or other technologies such as social media (Facebook), chat rooms, Skype or WhatsApp because they do not see the need in doing so. It's a double-edged sword: On one one, digitization has improved India's economy, education, and government, but on the other, it has introduced a slew of cybercrimes. As new channels for cybercriminals to target customers open up, the concept of cybercrime continues to develop. The launch of the internet and other technologies was aimed at facilitating human research and improving the quality of human life.[3]. The demand for Indian cyber rules increased as the number of Indians utilising the internet climbed. Because of the anonymity provided by the internet, it is quite simple for criminals to perform their crimes online. A big number of people are able to abuse this feature.As a result, there is a pressing need to create knowledge and consciousness among individuals about the dangers of using the internet, as well as effective counselling if they ever encounter cybercrime. In addition, India faces a grave need for education and training in the field of cybercrime prevention. Here, we'll look at how cyber law is implemented and what kinds of cyber crimes there are, as well as the holes that need to be filled from time to time by enacting authorities.

EVOLUTION OF CYBER LAW IN INDIA

Even the Information Technology Act, 2000, which deals with cybercrime, does not provide a precise definition in the Indian legislative system. Any criminal activity carried out via or with the assistance of the internet or computers is generally considered a form of cybercrime. Cyber law does not exist as a separate body of legislation in the country of India. Contract, intellectual property, data protection, and privacy regulations are all involved. A strong cyber law was required as computers and the internet began to permeate every area of our lives. As far as cyber law is concerned, it governs everything from software and information security to electronic commerce and money exchanges. As far as I know, tIn this country, there is no legislation addressing cyber security specifically. The Information Technology Act of 2000 (the IT Act) and its rules and regulations govern cyber security and cybercrime. Security measures for computer systems and electronic data, information, or records are included in the IT Act's provisions. Many cybercrimes are criminalised under the IT Act, such as hacking and denial-of-service assaults, as well as phishing and virus-related offences.

Thus, the Information Technology Act, 2000[4], or also known as the Indian Cyber Act or the Internet Law came to force in India. All electronic records and online/electronic actions have been brought into legal status by the Indian Internet Laws since their introduction.It also addresses security issues, which are critical for electronic transactions to run smoothly. While the Indian Internet Laws affirm the existence of digital signatures, they also provide guidance on how to validate documents that have been accepted and generated with the help of digital signatures. It deals with a wide range of modern-day crimes. This type of crime is both perpetrated and perpetrated by computer technology.
The Information Technology Law was changed under the IT Act, which is a cyber security law designed to protect cyberspace.;

---

[1] Justice Yatindra Singh, *Cyber Laws* 36 (universal law publishing, Delhi, 6th edn., 1998)

[2] B. Swaathi and M. Kannappan, "Cyber Crime-An Indian Scenario"119 ISSN 1053 (2018)

[3] Dr. Faruq Ahmed, Cyber Law in India 67 (New Era Law Publication, Ahmedabad, 3rd edn., 2002)

[4] Information Technology Act 2000, India, available at: http://www.mit.gov.in/itbill.asp (last visited on March 7, 2019.

The Indian Penal Code
The Indian Evidence Act
The Banker's Book Evidence Act
The Reserve Bank of India
The prime focus of cyber law in India is to prevent:
Crime through the use of a computer
Fraudulent use of electronic records and data
Transacting electronically
In 2008, modifications were made to the Information Technology Act of 2000. In light of the IT Act, 2000, and the IT Act, 2008, which govern cybercrime, these decisions were made.. As of the beginning of 2009, they were enacted to improve the cyber security laws. Modifications made to the Information Technology Act of 2008, including new definitions for devices used for communicating, included.

Information Technology Act of India's objectives as outlined below:
To ensure that all electronic transactions are protected by law.
Accepting online agreements with the use of legitimate digital signatures that have been granted legal recognition as such
Recognize the use of electronic accounting records by financial institutions and other businesses.
the prevention of cybercrime and the preservation of users' privacy on the internet
Cybercrime prevention and privacy protection
As a result of Indian IT law, both the Reserve Bank of India Act and the Indian Evidence Act were amended. Almost all online activities are now subject to inspection because of the development of cyber legislation. Certain aspects of cybercrime in India are exempt from the country's cybercrime laws, including:
Other than a cheque, a negotiating instrument
Power of Attorney
Will
A document or transaction notified by the Central Government regarding the contract for the sale or transfer of immovable property
IT Act consists of 12 chapters and 4 schedules:[5]
Chapter 1 of the Act contains section 1-2 deals with Definition clauses and application and extent of the Act. (Section 1-2)
Chapter 2 has to do with digital signatures and e-signature authentication. (sections 3)
Chapter 3 concerns itself with e-governance There is discussion of the legal recognition of electronic records and digital signatures by government agencies and the employment of this technology in these institutions.. To regulate digital signatures, it empowers the federal government. (Section 4 – 10)
Chapter 4 focuses on electronic record attribution, acknowledgment, and transmission.(Section 11 – 13)
Chapter 5 security and digital signatures for electronic records. (Section 14 – 16)
Chapter 6 regulates certifying authority regulation. Controller functions and certification authority powers are discussed, along with the appointment of a controller. (Section 17 – 34)
Chapter 7 deals with Digital Signature Certificates. (Section 35 – 39)
Chapter 8 emphasis on Subscriber Duties. (Section 40 – 47)
Chapter 9 dealings with the Appellate Tribunal for Cyber Regulations. (Section 48 – 64)
Chapter 10 deals with Offence s. (Section 65 – 78)
Chapter 11 In some circumstances, Network service providers will not be held liable. (Section 79)
Chapter 12 deals with Miscellaneous

CYBER CRIME
Cyber crime is a combination of two terms "crime" with the root "cyber" derived from the word "cybernetic", from the Greek, "kubernan" , which means to lead or govern. The cyber environment includes all forms of digital activities, irrespective they utilize single network. Cyberspace is borderless as no Courts across the globe can claim jurisdiction. Any illegal act which involves a computer, computer system or a computer network is cybercrime.[6]

DEFINTION OF CYBER CRIMES
Using the Greek word "kubernan," which meaning "to lead or rule over" as the root of "cybercrime," we get the name "cybercrime.". "Cyber" comprises all digital operations, regardless of whether they are carried out on a single network or not. In the virtual world, no court may claim jurisdiction because there are no borders. Any criminal activity involving a computer, computer system, or computer network is considered a cybercrime.[7]

Most common types of cybercrimes are as follows:

[5] Supra note. 3
[6] Rohasnagpal , *Cyber Crime and Corporate Liability* 45 (4th edn 1997)
[7] Rohasnagpal , Cyber Crime and Corporate Liability 45 (4thedn 1997)

Cyber stalking: Women are the most frequently targeted victims of cyber stalking, which is on the rise. Using the Internet to track and harass someone is known as "cyber stalking." Instead of making physical threats, a cyber stalker monitors the victim's internet activities to acquire information and provide threats that can take many different forms of verbal harassment. Cyber stalking is more widespread than physical stalking because of the anonymity afforded by internet communication..
Morphing: It is possible to alter an image in such a way that it can be used against its author's intentions by morphing it. Morphed images of female victims are used by perpetrators on social networking, porn sites, or to register themselves as anonymously as possible on other platforms..
Cyber-pornography: This poses an extra threat to women and children since it entails the publication of pornographic materials on pornography websites through the use of computers and the internet.
E-mail spoofing: When an email is sent from one source, it is referred to as a "outbound" email. It may generate financial losses..[8]

Phishing: An attempt to get private information, such as a user name and password, is called phishing..[9]

Cyber Defamation: Libel and defamation on the internet are two forms of cyber defamation. To do this, facts regarding the victim's character or character's reputation must be posted on the internet or distributed to the victim's social circle or workplace..[10]

Cross site scripting: Malicious web users can insert code into web pages they're viewing through vulnerability known as cross-site scripting (XSS), which is most commonly discovered in web apps. HTML code and client-side scripts are examples of this type of code. The usage of an exploited cross-site scripting vulnerability allows attackers to circumvent security measures.[11]
Web jacking: Hi jacking is the ancestor of the word "Web jacking." By creating a false website, the perpetrator tricked the victim into clicking on a link that took them to a another website, where they were forced to click on another link. Clicking on a link that appears to be authentic redirects the victim to a phoney website. These forms of attacks are carried out in order to gain entry or control over another's location. The information on the victim's webpage may likewise be altered by the assailant.[12]
Hacking: Internet and e-commerce are most at risk from this sort of cybercrime, which is the most dangerous and serious. In order to hack a computer system without the owner's knowledge or approval, a hacker must break into the system and remove sensitive data.. The term "computer virus" refers to a set of instructions that can be used to carry out a variety of harmful actions. System programmes are interrupted and a few anomalies are inserted by viruses. It is possible for a computer virus to propagate through the usage of e-mail, compact discs, USB flash drives, multimedia files, and the internet.[13]
SMS Spoofing: You can change the identity or phone number from which SMS messages seem to be sent by using SMS Spoofing..[14]

Trolling: It is the goal of online bullies and criminals to arouse the emotions of their victims by the use of provocative or off-topic utterances in online communities (such as a newsgroup, forum, chat room, or blog).

PROVISIONS RELATED TO CYBER CRIME UNDER IT AMENDMENT ACT 2008
Stalkers and cyber criminals are subject to criminal charges under the Information and Technology Act of 2000, which includes many sections dealing with invasions of privacy..
Section 67 - focuses on the distribution of obscene material via the internet. Child pornography and intermediary document storage were added to an earlier Section in ITA following the ITAA 2008...

Section 66A - Email spoofing, IP spoofing, and other forms of communication service spoofing are all included in this section. A fine or up to three years in prison can be imposed for this type of conduct.

Section 66B - Dishonestly accepting stolen computer resources or communication equipment is a crime punishable by up to three years in prison and a fine of up to one million rupees.

---

[8] Classification of cyber law, available at: https://www.scribd.com/doc/316141735/Characteristic s-of-Cyber-Crime (last visited on 2nd nov. 2019)

[9] Cyber Crime mans safety , available at: http://www.sbsnagarpolice.com/Cyber_crime.htm (last visited on 12 October 2019)

[10] Ibid.

[11] Hemraj Saini, Yerra Shankar Rao, T. C. Panda, "Cyber Crimes and their Impacts: A Review" IJERA, Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209, (last visited 23rd October 2019)

[12] Ibid.

[13]Ibid

[14] Computer Crime, available at: https://www.lectlaw.com/mjl/cl025.htm (last visited on 22nd October 2018)

Section 66C - Identity theft occurs when someone steals someone else's password or e-signature.

Section 66D - A maximum of three years in prison and a fine of up to one lakh rupees are available to those who conduct fraud by impersonating another person through the use of a computer resource or a communication device.

Section 66E - Privacy infringement - Publishing or disseminating a person's private information without their permission. Some possible punishments include prison time for up to three years or a fine of up to two lakh rupees (or both).

Section 66F- It is illegal for anyone who has not been authorised to use a computer resource or who is encroaching on a computer resource in an unapproved manner to gain access.

Section 72- Penalties for violating someone's right to privacy and secrecy.

Section 72A - For revealing confidential information throughout the course of a legal transaction.

Section 441 IPC- Criminal trespass is addressed in this section.

Section 354D IPC- This section deals with stalking, which is illegal. man who stalks ladies by using digital media to follow them and try to get in contact with them.

RULES RELATED TO CYBER SECURITY UNDER THE ACT

Under the Information Technology (Indian Computer Emergency Response Team and Manner of performing Functions and Duties) Rules 2013, a central agency for collecting, analysing and disseminating information on cyber events has been established (the CERT Rules).

Among the provisions of the IT Act pertaining to cyber security are the following::

The SPDI Regulations are a set of 2011 information technology rules that outline the required procedures that must be followed to protect personal or sensitive data when it is collected and handled.; and

The Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018 apply to protection systems as specified by the IT Act (the Protected System Rules). Information on the scope and jurisdiction of protected systems can be found here.IT (Intermediaries Guidelines), 2011 (the Intermediaries Guidelines), must protect their computer resources and their data, which necessitates that intermediaries put in place suitable security measures. Aside from reporting cyber security issues, intermediaries are also expected to provide CERT-In with all relevant details of such instances..

Businesses are required by the Companies Act 2013 (the CAM Rules) to protect electronic data and security systems from unauthorised access, among other types of offences punishable by Indian Penal Code 1860 (IPC).

ROLE OF JUDICIARY IN EXPANDING CYBER CRIME JURISPRUDENCE:

The Indian judiciary has made a huge effort to recognise crimes perpetrated through the use of computers. Some of the leading cases are :

In *The Bank NSP Case,* A bank's management trainee got married. The computers at the workplace were frequently used by the pair to communicate via email. It wasn't long before they divorced and she started using bogus email addresses like "Indian bar organisations" to communicate with her ex-international husband's customers. The bank's computer was used to complete this task. Having lost a huge number of clients as a result of the bank's conduct, the boy's business took legal action. It was the bank's responsibility if emails were sent through their system.[15]

An obscene CD offered on Bazee.com's website was sold out in Delhi the same day the CEO of Bazee.com was arrested for selling it there in December 2004.. The CEO was released on bail when Delhi and Mumbai police intervened.[16]

The Gujarat High Court in the case of *Jaydeep Vrujlal Depani v State of Gujarat*, [17] to mean "crimes committed against individuals or groups of individuals with a criminal motive to harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly via modern telecommunication networks such as the Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) or mobile ".

In *Air force Bal Bharti School Case*[18] before Delhi's Juvenile Court on charges of using pornographic software. According to some legal experts, There has never been a prosecution for Indian cyber pornography in a juvenile court before to this one. An Air Force Bal Bharti School student in New Delhi was detained by the Delhi Police in April 2001.

Similarly, in a recent judgment of *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors*[19] Article 21 of India's Constitution and the country's supreme court both define the right to life and liberty, which includes the right to one's own private

[15] State by Cyber Crime Police vs. Abubakar Siddique

[16] Avnish Bajaj vs. State (N.C.T.) Of Delhi 3 Comp LJ 364 Del, 116 (2005) DLT 427, 2005 (79) DRJ 576

[17] R/SCR.A/5708/2018 Order.

[18] The Air Force bal Bharti, Delhi Cyber Pornography Case 2001

life. Indian courts have previously permitted recordings made without permission as admissible evidence despite precedents finding that private talks between individuals are covered by the "right to privacy.". A case-by-case determination of whether a recording is permissible must take place because this issue has not been resolved..

In *Shreya Singhal v. U.O.I*[20] Is A Landmark Decision in Relation to Section 66A of the Information Technology Act of 2000 This clause was initially absent from the text of the statute because of the Amendment Act of 2009, which went into effect on October 27, 2009..[21]

CONCLUSION

There has been an upsurge in cyber crimes as a result of technological advancements. Computer ethics and principles must be taught to the general populace in order for them to be used in a suitable manner. Since citizens' interests must contend with those of the law, cyber law needs to be reformed to keep up with changing times. It's not going to stay the same. This is an area where significant work has to be done, particularly in India. The safety, security, and trustworthiness of our computer systems cannot be taken for granted. Efforts should be made to modernise and equip police officers with information and skills in order to combat cybercrime. The current virtual environment, without which no human being can survive, necessitates a new cybercrime law to be drafted that specifically addresses cyber offences. As a result of this, the Act's policy has been worsening because the goal of Information Technology for which it was adopted deals with distinct difficulties..