Indian Journal of Health, Sexuality & Culture
Volume (6), Issue (1), June 2020
ISSN 2581-575X
https://www.iisb.org./

Review Article

Cyber law for sexual crimes

Huma Fatima[1], Jabbar Husain[2]
[1]M Phil trainee (Clinical Psychology), [2]Junior Resident, Department of Psychiatry, King George's Medical University, Lucknow, U.P., India.

Date of Submission :
8 April 2020
Date of Acceptance :
29 May 2020

Keywords: Cyber-crime, Cyber sexual crime, Cyber law, Indian penal code, IT Act, Judicial system.

Abstract

Cyber-crime is a known entity since the introduction of the internet. Cyber sexual crime is a variant of this. Sexual crimes are always present in our society but the internet changed the nature of sexual crimes. It looks like there is a rise in sexual crimes over the internet. We can attribute to this the luxury of anonymity present over the internet. Indian Penal Code, 1860 did not have any section or chapter addressing cyber law. Information Technology Act, 2000 was a milestone in the Indian Jurisdiction System. It is a help for addressing, combating, and curbing cyber-crimes. IT Act is also helpful in creating awareness among the masses.

Introduction

Cyber-crime is an amalgamation of two words i.e. cyber and crime. In common parlance, the term cyber is taken to be something relating to the Internet or the virtual world. Whereas, the term crime is an action not permitted in law and which is a civil wrong. Cyber-crime is any crime that is committed over the internet. Easily, we can say that cyber-crime is illegal acts, where, the computer system is either a device or prey or maybe both.

Corresponding Author : Miss Huma Fatima
E Mail: fatimahuma786@gmail.com
How to cite the article : Fatima, H., Husain, J., (2020). Cyber law for sexual crimes. Indian Journal of Health, Sexuality & Culture, 6(1), 22-28.
DOI : 10.5281/zenodo.3929139

Definition of cyber-crime

The Encyclopaedia Britannica defines cyber-crimes as *"Any crime that is committed through special knowledge or expert use of computer technology"*. Therefore, in cyber-crime different sorts of criminal offenses might be put together and acts with a reasonable conscience.

The Oxford Dictionary defines crime as *"An offense against an individual or the state which is punishable by Law"*.

The term 'cyber' was given by William Gibson in his 1984 fictional novel 'Neuromancer'. Cyber is used as a prefix to the worldwide field of electronic communication. (Giacomini & Zaidi, 2012).

Crime is an action that is punishable by law. The same can also be used for cybercrime.

The only aim of the cyber world is to suggest that computers are used to perpetrate an illegal act and to alert the users of protecting electronic proof, which is inherently fragile. This crime can, in short, be referred to as electronic crime. Crime is a legal wrong that may culminate in punishment. Cyber-crimes are committed against a person, society, or property. Examples of these crimes are cyberstalking, violation of privacy, pornography, defamation, e-mail spoofing, and hacking, etc.

Reasons of cyber-crime

There are various reasons for which people commit cyber-crimes. For example, in computers, data is stored in a very small space and the data or information can be easily obtained or removed by surely implanting programmed bomb or keyboard capturing devices that can steal access code, use of improved voice recorders, or retina images that can deceive biometric systems. The criminals take advantage of these loopholes and lacunas. Furthermore, negligence is also part of human conduct and criminals take advantage of this negligence. Criminals are also aware that the data are routinely destroyed and this affects the investigations of crimes (Giacomini & Zaidi, 2012). Moreover, cyber offenders prefer for this crime as it is less physical and more mental. Its nature as a white-collar crime attracts only persons qualified in this arena. Once data stored in cyberspace is breached, it ensures access to very huge and sensitive information at one single place of the virtual world. After stealing data, it is much much easier to transmit the same to the destination of choice. It also ensures hefty returns realizing the dream of getting rich overnight.

Ways of cyber sexual crime

1. Cyber bullying

The term cyberbullying also known as cyberstalking in documentations entails following a person's activities by way of the internet and sending messages (sometimes threatening in nature) to the target person or victim, unlawful entering the websites used by the victim or bombarding with messages or e-mails, etc even after his/her constant disinterest.

2. Cyber pornography

Cyber pornography includes pornographic websites, online pornographic magazines, uploading, downloading, and transmitting pornographic materials unlawfully. It also includes sharing with friends and sending them to another communication device. It also includes child pornography.

3. Defamation

Defamation is a false or fake rumor about a person. It can be committed by spoken words or in writing via communication devices like SMS, MMS, E-mail, etc. A false rumor gets viral through the internet may be counted as defamation. Defamation has been defined in Indian Penal Code (IPC), 1860 under section 499 as *"Whoever by words, either spoken or intended to be read or by sign or by visible representations makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person"* (Ranchhoddas & Thakore, 1997).

4. Criminal intimidation

It also has been defined under Indian Penal Code,1860 as *"Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with intent to cause alarm to that person or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation"* (Ranchhoddas & Thakore, 1997).

5. Obscene act in public

This involves exchanging or receiving pornographic items over the Internet, disregarding the dignity or modesty of a woman by attacking her and disregarding in public the modesty of a woman by word or deed, etc.

Present status of cyber-crime in India

According to the latest report of the National Crime Record Bureau (NCRB), total 21,796 cyber crime cases were recorded out of 50,07,044 cognoscible offenses in 2017 (Bhaskar, 2019). As per NCRB, during 2017, 56.0% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by 1,460 cases for sexual exploitation (6.7%) and 1,002 cases for causing disrepute (4.6%) (Bhaskar, 2019).

Cyber law

The IT Act (Information Technology Act), 2000 is the only federal legislation that provides legal recognition to computers and their liability issues. '*Actus reus and men's rea',* i.e. illegal act and wrongful intention, must be enforced to remedy criminal liability. Misdeeds alone are not enough for punishment because there is a mandatory limit of punishment. '*Actus non facit reum nisi mens sit rea',* i.e. if an act is done in a blameworthy manner then only it could be considered a crime. The Information and Technology Act, 2000 for the very first time brings cyber-crimes, punishment, and course of action for providing it within a legal frame. It is said that *'People are fragile so the law is important to protect them'*. And so also there must be laws to safeguard computers against cyber-crime.

Table-1. Classification of cyber-crimes

Crime Against Individual	Crime Against Economy	Crime Against Society	Crime Against Nation
◆ Carding ◆ Cyberstalking ◆ Hacking ◆ Identity theft ◆ SMS Spoofing ◆ Cyber Obscenity	◆ Computer fraud ◆ Computer forgery & counterfeiting ◆ Computer sabotage ◆ Cracking ◆ Cybersquatting ◆ Economic espionage ◆ Hacking ◆ Intellectual property rights infringement ◆ Malicious programs viz. ○ Virus ○ Worms ○ Trojan horse ○ Hoax ◆ Phreaking ◆ Salami attacks ◆ Tax evasion ◆ Theft of telecommunication services ◆ Web-jacking	◆ Cyber pornography ◆ Child pornography ◆ Racial & other hate speeches on blogs and other social networking sites	◆ Cyber terrorism ◆ Cyberwarfare ◆ Damaging critical infrastructure

Table-2. Sexual crimes covered in the Indian Penal Code (IPC)

Offense	Section
Obscene act in a public area	Section 294
Scandalizing by an assault on a woman's modesty	Section 354
Scandalization by word or expression of a woman's modesty	Section 509
Sending a threatening message by E-Mail or SMS	Section 506
Sending defamatory messages by E-Mail or SMS	Section 499

Table-3. Sexual crimes covered under the Information Technology Act (IT), 2000

Offense	Section
To pass on obscene material in electronic form	Section 67
Pornography	Section 67-A and 67-B
Sending offensive messages	Section 66-A
Violation of privacy	Section 66-E
Cheating by personation	Section 66-D

Modus operandi in cyber sexual crimes

- Violation of privacy: capturing and publishing the images, pictures, and videos of individuals often without the knowledge and thereby causing humiliation and embarrassment. Normally females are victimized in this way by the posting of pictures with a hidden attachment of an unwanted and often harmful message. It sometimes also contains phone numbers to cause disturbance to the part of the victim.
- Obscenity and pornography: Uploading and transmitting obscene and salacious materials over the internet and causing escalation and further transmission. It also includes images and videos of children of such taste. Many national and international online sharing websites have provided a nurturing

Table-4. Sexual crime and their punishment under cyber law

Section	Offense	Punishment	Fine	Cognizable or Non-Cognizable	Bailable or Non Bailable	Court of Trial	Compoundable or Non-Compoundable
66-E	Violation of privacy	Imprisonment of three years and also likely to fine	Up to one lakh rupees	Cognizable (section 77-B)	Bailable (section 77-b)	Magistrate of first-class	Compoundable (section 77-a)
67	Publishing or electronically transmitting obscene materials	**In first conviction**		Cognizable	Bailable	Magistrate of first-class	Compoundable (section-77-a)
		With imprisonment of either for a term which may extend up to five years and with fine	Which potentially extend to ten lakh rupees				
		In the second or following conviction					
		Imprisonment of either for a term which may extend up to seven years and also with fine	Which potentially extend to ten lakh rupees				
67-a	Publishing or transmitting of material containing sexually explicit act etc.	**In first conviction**		Cognizable (section 77-b)	Non-bailable	Magistrate of first-class	Non-compoundable (section 77-a)
		Imprisonment of either for a term which may extend up to five years	Potentially extend to ten lakh rupees				
		In the second or following conviction					
		Imprisonment of either for a term which may extend up to seven years	Potentially extend to ten lakh rupees				
67-b	To publish or transmit materials related to children in a pornographic manner	**In first conviction**		Cognizable conviction (section 77-b)	Non-bailable (section 77-b)	First-class magistrate	Non-compoundable
		Imprisonment of either description for a term which may extend to five years	May extend to ten lakh rupees				
		In the second or following					
		Imprisonment of either description for a term which may extend to seven years	May extend to ten lakh rupees				
72	Breach of confidentiality and privacy	Imprisonment for a term of two years	Up to one lakh rupees	Non-cognizable	Bailable	Magistrate	Compoundable

environment for creating, uploading, and transmitting such kind of materials including related to children. They make money by the propagation of such materials.

Blocking of these sites has been a challenge both in legal as well as technical means because the content can be uploaded in the different domain name or IP address and hosted in different IP addresses in different geographies. (Basha, 2010).

Jurisdiction of the court in cyber-crimes carried out outside India

There is a provision of Section 75 of Information Technology (IT) Act, 2000 which states that if an act constituting an offense involving a computer is committed by a person outside India, the court in India has jurisdiction to see the case. The computer or computer system must be located in India. In this case, the nationality of the person committing the offense is not pertinent and concerning the internet, there is no specific law regarding its jurisdiction.

Cyber laws related to sexual offenses-international glimpses

United Kingdom

- Obscene Publication Act, 1959
- Protection of Children Act, 1978
- Defamation Act, 1996
- Malicious Communication Act, 1998

USA

- Child Online Protection Act, 1998
- Protection of Children from Sexual Predators Act, 1998
- Spyware Control and Privacy Protection Act, 2000
- Children Internet Protection Act, 2000

Ireland

- Child Trafficking and Pornographic Act, 1998

How to combat and to keep a check on cyber-crime

The creation of a cybercrime investigation cell under the Central Investigation Bureau (CBI) was an important step in the right direction.

All cases of these crimes are to be decided by the court of law therefore, judges must be fully aware of the provisions of various laws regarding these crimes.

E-courts must be established in India. The IT Act should be given extensive publicity. And lastly, the police force is also must be trained for dealing with these crimes and they should be thought to be sensitive and cooperative with the general public.

Conclusion

In conclusion, it must be said that it is not easy and even possible to eradicate cyber-crime once and for all especially given the latest advanced scientific and technical developments. Nevertheless, it is always possible to combat or encounter this type of crime. To achieve that objective, the first and foremost requirement is adequate awareness among the general public about these types of crimes and also about its machinery. They must practice precautions to protect from the cyber-crimes and always be vigilant and watchful of their activities as well as others' activities over the internet.

References

Akdeniz Y. (2001). Cyber Rights, Protection, and Markets: Articles Governing Pornography and Child Pornography on the Internet. 32 University of West Los Angeles Law Review 247.

Basha K.N. Justice. Detection of Cyber-crime and Investigation, (2010). http://www.t nsja.tn.

gov.in/article/Cyber%20Crime%20by%20KNBJ.pdf

Bhaskar, U. (2019). Cyber-crime cases in India almost doubled in 2017. https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html [Last accessed on 23-05-2020]

Giacomini F, & Zaidi M.H. (2012). Electronic Evidence. Allahabad, India: Alia Law Agency.

Muralidhar S. Justice (2008). Avnish Bajaj vs State, 29 May, 2008. https:// indian kanoon.org/doc/309722/.

Pollack R.F. (1996). Creating the Standard of a Global Community: Regulating Pornography on the Internet - an International Concern. 10 Temple International and Comparative Law Journal, 467.

Ranchhoddas R, & Thakore D.K. (1997). The Indian Penal Code, New Delhi, India: Wadhwa & Company.

Ratanlal & Dhirajlal. (2008). Indian Penal Code (31st edition). Delhi, India: LexisNexis India.

Soanes C & Spooner A. (2001). Compact Oxford Dictionary Thesaurus & Wordpower Guide, Oxford University Press, Indian Edition.