DIGITAL SHADOWS: UNRAVELLING CYBER CRIME AGAINST SOCIETY IN INDIA

Nikita Begum Talukdar, Assistant Professor, Senior Scale, SOL, UPES, Dehradun, Uttarakhand.

ABSTRACT

Over the last ten or so years, cybercrime has gained more and more attention from people in a variety of backgrounds. Because society depends more and more on computer networks, we are more susceptible to the malfunctions and abuses of those systems. For those who study crime and deviance, such as criminologists and sociologists, the rise of cybercrime raises challenging issues. These academic fields have developed theories and explanations of crime based on presumptions (about who, what, where, and other factors) derived from crimes committed on land.

In this paper we will discuss the various cyber crimes which is against the society like cyber pornography, online gambling, cyber terrorism and the laws relating to it. We will also discuss the relevant case laws relating to the subject and the ways to report and prevent cyber crimes in the society.

Keywords: Online gambling, Cyber Crime, Cyber pornography, Child pornography.

1. Introduction

In the modern era there is abundance of knowledge in every sphere of life. The world has become very small and has come to be known as a *global village*. The means of communication has become very fast and any kind of information from any corner of the world can be obtained within minutes with the help of Internet wherein websites have been created in every field of knowledge to be available to people anywhere in the world. Gone are the days when a country's sovereignty was the sole determinant of the political economy of the political systems. Now, countries are interdependent and the market forces in the business are setting commercial and business trend in the world. E-commerece is the trend today and many business transactions are going online. Information and communication is under a revolutionary change which has brought about unprecedented changes, compelling the business world and the political government to follow the modern system of governance through computer and internet [1].

2. Nature and Definition of Cyber Crimes

Encyclopaedia Britannica defines cybercrime as, *"any use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing, identity or violating the piracy."*[2]

Cyber crime is not defined in the Information Technology Act, 2000 (hereinafter Be called as IT ACT) or in the Information Technology Amendment Act,2008 (hereinafter be called as ITAA) nor in any other legislation in India. The oxford Reference Online defines cybercrime as a crime committed over the internet. Generally speaking, cyber-crime can be referred to an unlawful act wherein the computer is used either as a tool or as a target or both. There can be different motives which may lead one to commit the crime. It may be greed, desire for power, publicity, revenge or adventure. It may also be the desire to access forbidden information or to somehow sell all the new security services. Though cyber crime is not defined but *Cyber Security* is defined under *Section (2)(b) of the IT Act* as *protecting information, equipment, devices computer, computer resource, communication device, and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.*

[1] Harish Chander, *Cyber Laws & IT Protection,* 3 (PHI Learning Private ltd., Delhi, 2016).
[2] Muragendra Tubake, "Cyber Crimes: An Overview", *3 JOIIR*, 130 (2013).

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crime related to computer networks, Cybercrime was broken into two categories and thus defined thus[3]***:***

a. **Cybercrime in a narrow sense (computer crime) :** any illegal behaviour directed by means of electronic operations that targets the security of computer systems and data processed by them.
b. **Cybercrime in a broader sense (computer related crime) :** any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or disturbing information by means of computer system or network.

Cyber crime is a narrow sense therefore targets the machine and its data, while the broader cybercrime targets not just the machine, its data but also anything related to it. Another working definition was provided by the OECD Recommendations of 1986 as computer-related crime is considered as any illegal , unethical or unauthorised behaviour relating to the automatic processing and the transmission of data.[4]

3. Cyber Crime against The Society and the Legal Framework

Cybercrimes also impact society as a whole. The sale of illicit goods, pornographic websites, and unlawful online auctions are all factors in the deterioration of social values. Cyberterrorism refers to the use of computers or computer networks for terrorist actions. Cyberspace is also being used by criminals to manufacture counterfeit revenue stamps and banknotes, which has an impact on society as a whole. The impact of cybercrimes on society is briefly discussed in this paper. Or focus on this paper will be the following three:

1. Online gambling;
2. Cyber pornography and child pornography;
3. Cyber terrorism.

The following can be described as the cyber crime against the society-

[3] *Supra, Note* 3 at 8.
[4] *Ibid.*

3.1 ONLINE GAMBLING-

"Gambling" as per most Gambling Legislations is understood to mean "the act of wagering or betting" for money or money's worth. Gambling under the Gambling Legislations however does typically "not include (i) wagering or betting upon a horse-race/dog-race, when such wagering or betting takes place in certain circumstances, (ii) games of "mere skill" and (iii) lotteries (which is covered under Lottery Laws)."

There are thousands of websites that offer online gambling. The issue that makes regulation of gambling more difficult is the fact that it is legalised in several countries. This makes the owners of these websites, safe in their home countries. The legal issues arise when a person residing in a foreign country like India (where such websites are illegal) gambles on such a website. The law related to gambling is also applicable to online gambling. All gambling contracts are considered to be wagering contracts and it is not possible to enforce such contracts. Since ancient times, the most popular types of gambling in India have been card games such as poker, rummy, bridge, and teen patti, which is similar to a flush, as well as sports betting. Since the advent of technology, many games have successfully expanded their audience and level of popularity online. The most well-liked online gambling platforms in India are card game websites that include poker and rummy competitions..

Legal framework

The only state in India with legislation allowing internet gaming and sports betting is the State of Sikkim. Enacted on June 28, 2008, the "Sikkim Online Gaming (Regulation) Act, 2008" aims to regulate and govern online gambling in both electronic and non-electronic modes, as well as levy a tax on such games inside the State of Sikkim. On March 4, 2009, the Sikkim Online Gaming (Regulation) Rules, 2009 were subsequently passed (and have since undergone periodic amendments; see "Sikkim Online Gaming Laws"). Goa and other states are considering passing legislation along these lines. The Indian casinos are governed by the Gambling Legislations. The gambling laws in Goa, Daman & Diu, and Sikkim permit a certain amount of gaming in five-star hotels with a licence.[5] The law in Goa permits casinos to be located on an offshore vessel. The state governments are in charge of authorising and running lotteries as well as enacting legislation

[5] Sikkim Casinos (Control and Tax) Act, 2002 read with Sikkim Casino Games Commencement (Control and Tax) Rules, 2007 and Sikkim Casino Games (Control and Tax) Amendment Rules, 2011.

pertaining to betting and gambling, while the union government is authorised by the seventh schedule of the constitution to enact regulations governing the conduct of lotteries.[6]

The law related to gambling is also applicable to online gambling.

- **"The Public Gambling Act, 1867",** provides details for the punishment of public gambling. The Lotteries (Regulations) Act, 1998, lays down guidelines and restrictions in conducting lotteries.
- **Section 294-A of the Indian Penal Code 1860**, lays down punishment "for keeping a lottery office without the authorisation of the state govt. which may extend to six months, or with fine, or with both. And whoever publishes any proposal to pay any sum, or to delivery any goods, or to do or forbear doing anything for the benefit of any person, on any event or contingency relative or applicable to the drawing of any ticket, lot, number or figure in any such lottery, shall be punished with fine which may extend to one thousand rupees."
- **Section 30 of the Indian Contract Act, 1872**, "prohibits anyone from filing a lawsuit to recover any winnings from a wager; this guarantees that no court case can be filed to recover any winnings from lotteries, gambling, or betting."
- **The Lotteries(Regulation) Act 1998,** provides a framework for "organizing lotteries in the country. Under this act the state governments have been authorised to promote as well as prohibit lotteries within their territorial jurisdiction. This act also provides for the manner in which the lotteries are to be conducted and prescribes punishment in case of breach of its provision. Lotteries not authorised by the state have been made an offence under the IPC."

As a result, although purchasing a lottery ticket may be entirely lawful in India, the winner of such a ticket will not be able to sue the lottery organisation should it decline to pay the winnings. The Information Technology Act of 2011 covers gambling websites and requires Internet service providers to prohibit offshore betting sites in an effort to put a stop to online gambling.[7]

[6] *Supra Note 3* at 83.
[7] *Supra, Note 3* at 84.

3.2 Cyber Pornography

Cyber pornography is believed to be one of the largest business on the Internet today. The millions of pornographic websites that flourish on the internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most nations today.

The word pornography originally referred to any work of art or literature dealing with sex and sexual themes[8]. The word pornography is difficult to define because what is provided in the dictionaries is quite different than what is defined under the law. Pornography has been defined as:

> *The sexual explicit depiction of persons, in words, in words or images, created with the primary, proximate aim and reasonable hope, of eliciting significant sexual arousal on the part of the consumer of such material*[9].

There is no uniform and single definition of law of the word pornography applicable all over the globe. The word pornography and the pornographic material is dependent on the vision and understanding in different cultures and countries in this world. And therefore, what may be considered pornography in India may not be considered as pornography in the western countries and the US. Pornography corrupts one's moral senses and instigates them to participate in various sexual offences. Pornography is nothing but marketing of women's sex. Women are shown as 'objects' to those who long to get involved into sexual acts[10].

Thus the graphics, sexually explicit subordination of woman through pictures and/or words refers to pornography. It is verbal or pictorial material which represents or describes sexual behaviour that is degrading or abusive to one or more of the participants in such a ways as to endorse the degradation.

From a legal standpoint, the terms "pornography" and "obscenity" are distinct and should not be used interchangeably. There are variations in the global standard for defining obscenity in relation to criminality among various regions, societies, and nations. Even the criteria for what

[8] Pornography, Microsoft Encarta online encyclopaedia 2007; *available at* http;//Encarta.msn.com.
[9] R.K Chaubey, *An Introduction To Cyber Crimes And Cyber Law*, p.381 (Karnal Law House, Kolkata, 2009).
[10] Id. at 382.

constitutes obscenity as a crime is subject to periodic revision. Because of the internet and cyberspace, which have no national boundaries and have made the globe a smaller place, things that were deemed objectionable in the 19th century might not be so in the present. Nowadays pornographic material is available in different formats on the internet. With the help of the latest technology and techniques the pornographic industry is flourishing in formats like, images files, video files, text audio formats and so on.

Legal framework

The term "pornography" is not used in any Indian legislation. Not even US or UK lawmakers have attempted to give this term "pornography" legal significance. And because there is no universal norm for morality or ethics, there can be no universal standard for law in the various cultures and nations of the world, making it impossible to find a definition of this term in the multi-national and multi-cultural environment of the Internet. There is no limit to how broadly one might interpret the terms obscenity and pornography.

For the first time, the test of obscenity was held to have the tendency "to deprave and corrupt those minds are open to such immoral influences and into whose hands a publication of this sort may fall"[11]. It was agreed upon that this criteria would only be applicable to discrete sections of a work. A US superior court ruled that "whether publication taken as a whole has a libidinous effect" rather than the content of a single, obscene section was the threshold for obscenity."[12].

Section 67 of the IT Act, 2000, provides for punishment for publishing or transmitting obscene material in an electronic form. It provides for both imprisonment up to three years as well as fine which may extend to five lakh rupees. And for subsequent offence of obscenity under the above section the punishment is increased up to five years imprisonment and with a fine which may extend to ten lakh rupees.

Generally there is a salutary principle in criminal law that no person shall be held liable for an offence unless the offender also has *mens rea* which means that for the commission of an offence

[11] *Regina v. Hicklin* (1868) 3 QB 360.
[12] *United States v. One book entitled ' ulysses*', 72 NY 705 (1934).

apart from the act or omission there shall also be *mens rea* in order to punish an offender for crime. This means that there shall be either intention, or knowledge or negligence on the part of an affender in order to commit a crime. And the relevant definition of *offence* provides for any mental state required as necessary for the commission of an offence. However, section 67 of the IT Act,2000 does not provide for intention or knowledge for the commission of the offence of publishing or transmitting or causing to be published in the electric form. Therefore section 67 of the IT Act does not require *mens rea or* guilty mind on the part of the offender to commit the offence. Section 67 of the IT Act is analogous to **section 292 of the IPC** which does not require either intention or knowledge in order to punish an offender for offence of obscenity. S.292 of IPC does not make knowledge of obscenity an ingredient of the offence.

Section 67A of the IT ACT provides for the punishment of publishing or transmitting of material containing sexually explicit act, etc. in electronic form and says that "whoever.

- Publishes or
- Transmits or
- Causes to be published or transmitted

in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees. If the act if repeated then, in the event of second or subsequent conviction the imprisonment may extend to seven years and also with fine which may extend to ten lakh rupees."

Section 67A of the IT Act provides for ***exceptions*** and says that both section 67 and 67A of the IT Act "do not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form:

- If the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or
- which is kept or used bona fide for religious purposes."

Along with section 67A of the IT Act, Sections 292,293,294, 500, 506 and 509 of the Indian penal code are also applicable which must be rea thoroughly.

3.3 Child Pornography

Child pornography is a menace and the way it is growing using information technology & communication tools, one may even come to a conclusion that no child is safe. Every child has the right to protection from all forms of exploitation.

Child pornography refers to images or films (also known as child abuse images) and in some cases writings depicting sexually explicit activities involving a child: as such, child pornography is a record of child sexual abuse. A child means a person who has not completed the age of 18 years. The interest is being highly used by its abusers to reach and abuse children sexually, worldwide. The explosion of internet has made the children a viable victim to the cybercrime. The easy access to pornographic content, readily and freely over the internet, lowers the inhibitions of the children. Paedophiles lure the children by distributing pornographic material, and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions.[13]

Legal Framework

Section 67B of the IT Act provides for child pornography and says that "any person who does the following would be guilty of the same:

a. publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
b. creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
c. cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
d. facilitates abusing children online or

[13] *Supra, Note 3* at 80.

e. records in any electronic form own abuse or that of others pertaining to sexually explicit act with children."

The punishment under the section is as follows:

- "on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees
- in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

provided that this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes."

As per section 67B Of the IT Act,2000, the above offence shall be cognizable and non-bailable, while, if sections 292/293/294 of the IPC are applied it will be cognizable, bailable and non-compoundable and triable by any magistrate. Sections 292/293/294, 500, 506 and 509 of the IPC which are also applicable and the victim can file a criminal complaint in the nearest police station.

3.4 Cyber Terrorism

The general meaning of Terrorism involves the use or threat of violence and seeks to create fear, not just within the direct victims but among a wide audience. Federal Bureau of Investigation (US) describes terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance

of political or social objectives."[14]

The term cyber terrorism was coined in 1996 by combining the terms cyberspace and terrorism. The beginning of cyber terrorism can be traced right from early 1990s when the increase in the growth of internet and cyberspace was visible to the world. A report generated in 1998 by the Center for Strategic and International Studies was entitled Cybercrime, Cyber terrorism, Cyber warfare, averting an Electronic Waterloo. In this report, the probabilities of such activities affecting a nation were discussed, followed by a discussion of the potential outcomes of such attacks and methods to limit the likelihood of such events. We will use the term cyber terrorism as:

"Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant target."[15]

Cyber terrorist use various tools and methods to unleash their terrorism. Some of the major tools and methodologies are hacking, virus/Trojan/worm attacks, email related crimes, DOS etc.[16]

Legal Framework

The Information Technology Act 2008 covers all actions in this domain. The IT Act provides following provisions:

- **Section 66F** says about cyber terrorism. It prescribes the punishment for cyber terrorism. It says Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life. This section has defined conventional cyber-attacks like, unauthorised access, denial of service attacks, etc.
- **Section69**, Power to issue directions for interception or monitoring decryption of any information through any computer source.
- **Section 69A,** Power to issue directions for public access of any information through any computer resource.

[14] *Supra, Note 3* at 84.
[15] Lech J. Janczewski and Andrew M. Colarik, Cyber Warfare and Cyber Terrorism, Information Science Reference, New York 2008.
[16] *Supra.*

- **4.Section 69B,** Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
- **section 70A**, Appointment of National Nodal Agency.
- **Section70B** Indian Computer Emergency Response Team to serve as National agency for incidental response.

4. Prevention of Cyber Crimes

Cybercrimes are on the rise, as was previously mentioned. There is a wealth of information about such frauds in newspapers. Bot infections have increased by 280 percent in India, and they are still spreading to more and more developing Indian towns. India has the greatest daily outflow of spam, or junk mail, globally, with an estimated 280 million messages sent out every day. Home computer owners in India are the group most frequently the victim of cyberattacks. The top two cities for cybercrime are starting to emerge as being Mumbai and Delhi.

In these circumstances, it becomes important to keep our computers and other electronic devices safe. There are various steps once can be taken to keep themselves safe from being a victim of such crimes:[17]

- it is suggested by most of the cyber law and technology experts that keeping the operating systems of computers and anti-virus updated and on, is one of the foremost ways to avoid cyber-attack. Updated computers means upgraded software, which would make it difficult for a hacker to immediately attack.
- Security software like firewalls which control who and what can communicate with the online system should be installed on the computers.
- Those mails which ask for personal information should not be responded to, and it should be remembered that when visiting a website type the URL directly into the web browser rather than follow a link within the email or instant message.
- Today most of the places, public wireless networks or wifi is available and even when at home these wireless networks are vulnerable to intrusion if they are not properly secured. Thus they should be key-protected.

[17] Refer E-Security Tips provided by cyber police station, CID, Bangalore *available at* http://www.cyberpolicebangalore.nic.in/E.security.html. (accessed on 3 May, 2014).

- Finally, one should immediately, call the cyber crime cells and police authorities, in case a computer crime is suspected.

5. Conclusion

Cyber crime has high potential and thus creates high impact when it is done. It is easy to commit without any physical existence required as it is global in nature due to this it has become a challenge and risk to the crime fighter and vice versa. The human mind's capacity is incomprehensible. It is impossible to completely eradicate cybercrime from the internet. You can check them with ease. History attests to the fact that no piece of legislation has been able to completely eradicate crime worldwide. Making individuals aware of their rights and responsibilities—such as reporting crimes as a group obligation to society—as well as tightening up the application of the law are the only ways to effectively combat crime. In the realm of cyberspace, the Act is unquestionably a historic step.

References:

1. Indian Penal Code 1860.
2. The Information Technology Act, 2000.
3. Information Technology (Amendment) Act, 2008.
4. The Protection Of Children From Sexual Offences Act, 2012 [No. 32 Of 2012]
5. The Sikkim Online Gaming (Regulation) Act, 2008.
6. The Lotteries(Regulation) act 1998.
7. The Public Gambling act, 1867.
8. Harish Chander, *Cyber laws and IT protection*, PHI Learning Private Ltd. Delhi, 2016.
9. Garima Tiwari*, Understanding Laws cyber laws and cyber crimes*, Lexis Nexis publications, Gurgaon, 2014.
10. Vakul Sharma, *Information Technology Law And Practice,* Universal Law Publishing House, New Delhi, Reprint, 2012.
11. Dr. Pramod Kr. Singh, *Laws on Cyber Crimes (Along with IT Act and Relevant Rules),* Book Enclave, Jaipur, 2007.
12. Kamath Nandan. *Law relating to Computers, Internet and E-commerce*, p.22 Universal Law Publication, Delhi,2009.
13. Gaur K. D. , A *Textbook on the Indian Penal Code*, Oxford and IBH Publication, New Delhi, 1992.
14. R.K Chaubey, *An Introduction To Cyber Crimes And Cyber Law*, (Karnal Law House, Kolkata, 2009).
15. Muragendra Tubake, "Cyber Crimes: An Overview" 3 OIIRJ (2013).
16. Govil, J., "Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology", *IEEE*. 2007 p. 610-615: Chicago.
17. Roshan, N., "What is cyber Crime. Asian School of Cyber Law", 2008: *Access at* - http://www.http://www.asclonline.com/index.php?titl e=Rohas Nagpal.
18. Dr. Ajeet Singh Pooni, "Cyber Crime: Challenges and its Classification" *ISSN 2278-6856*, *available at* www.ijettcs.org.
19. Lech J. Janczewski and Andrew M. Colarik, Cyber Warfare and Cyber Terrorism, Information Science Reference, New York 2008.