VOLUME 8 ISSN 2456-9704

CYBER CRIME: A NEW SPECIES OF CRIME

By *Dhanesh Desai & Naireen Khan*
From *Amity Law School, Noida*

I. INTRODUCTION: CONCEPT OF CYBER CRIMES

"This is just the beginning; the beginning of understanding that cyberspace has no limits, no boundaries."

-Nicholas Negroponte

With the coming of 21st Century, there has been tremendous increase in technological innovations and advancements which in turn has led to a rise in threats related to cyberspace. The crime has been computerized and financially sophisticated. Sutherland described such crimes as White Collar Crimes and nowadays they are known as Social and Economic offences in India.[1] Computer and Internet is a technological innovation which has proved to be an intoxicating threat to the society because it may offer a blanket to the criminal to get away with legal proceedings as the Internet provides an opportunity to act in secrecy. The enormity and anonymity of internet and lack of legal control over internet have led to the emergence of concept of Cyber crimes.

As per expert recommendations by UNO, Cyber crimes cover any crime committed by using computer systems or networks, within their frameworks or against them. Theoretically, it embraces any crime that can be committed in the electronic environment. In other words, crimes committed by using e-computers against information processed and applied in the internet can be referred to cyber crimes.[2]

Pavan Duggal in his book "Cyberlaw- The Indian Perspective" defines Cyber crime as,
"All the activities done with criminal intent in cyberspace or using the medium of internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium. Any activity, which basically offends human sensibilities, can be included in the ambit of cyber crimes."[3]

Thus, we can describe Cyber crimes as, the crimes which are committed by mishandling of computers. However, instead of using the expression computer crime, the current trend leads to call them as computer-related crimes. Cyber crime involves activities where computer technology is used as an instrument to access sensitive information of people, revealing business trade secrets and using internet for malevolent purposes.

The anonymity of internet makes it easier for cybercriminals to attack various computers present in different parts of the world. That's why cyber crimes usually go concealed and unreported, rendering the jurisdiction unstipulated. Thus, Cyber crimes are found to be discreet and universal in nature and that they do not leave any physical evidence behind.

II. FORMS OF CYBER CRIMES

Cataloguing of cyber crime is an intricate task because it is new manifestation of crime

[1] Dr AMITA VERMA, CYBER CRIMES & LAW 43 (1st ed. 2012) .

[2] Dr AMITA VERMA, CYBER CRIMES & LAW 43 (1st ed. 2012) .

[3] PAVAN DUGGAL, CYBERLAW-THE INDIAN PERSPECTIVE 256 (2002) .

which is increasing at a great pace with each passing day and producing new and different species of cyber crime. Some of the cyber crimes committed with malicious intentions such as gaining wealth in a short period of time, for vengeance or harassment, are described as under:

*A. **CRIME AGAINST INDIVIDUAL***

i. **Cyber Stalking/Cyber Harassment-** Cyber stalking, which is simply an extension of the physical form of stalking, is where the electronic mediums such as the internet are used to pursue, harass or contact another in an unsolicited fashion.[4] The term is used to refer to the use of the internet, e-mail, or other electronic communication devices to stalk another person. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.[5] Internet has become a basic need of the individuals and they are connected through various social networking sites, making it easier for cyber stalkers to collect the private information about the victim. There is a misconception that cyber-stalking is concentrated because there is no physical contact involved and as such no physical harm. However, it's important to note that easy access to private information can cause greater harm by way of cyber-stalking/harassment.

ii.

iii.

iv.

v.

vi.

vii.

Cyber Pornography- Cyber pornography refers to activities where sexual or illicit or obscene content is published or displayed over the internet. Pornographic contents become easily accessible to adults and children as well. Cyber pornography is banned in many countries and legalized in some. In India, under the Information Technology Act, 2000, this is a grey area of the law, where it is not prohibited but not legalized either[6]. Child pornography is another issue which is on rise and is a type of Child abuse where paedophiles obdurate their victims. Bombay High Court Committee gave recommendations to Hon'ble Chief Justice of Bombay High Court in its report, complaining about proliferation of pornographic sites on the Internet.[7]

Cyber Defamation- Defamation of an individual over internet or pertaining to cyberspace refers to Cyber Defamation. It will leave that individual's disposition vulnerable and open to abhorrence or mockery. Cyber defamation is covered under Section 499 of the Indian Penal Code.[8]

E-mail Spoofing- A spoofed e-mail is one which appears to be sent from a particular source but is actually sent from some other source. For example, a person sends an e-mail to another person by using his friend's

[4] Wayne Petherick, *Cyber-stalking: Obsessional Pursuit and the Digital Criminal*, (Sept. 27, 2018, 4:30 PM) http://www.angelfire.com/journal2/bewareoftrolls/stalking.html .

[5] *Report on Stalking: A New Challenge for Law Enforcement and Industry*- A Report from the Attorney General to the Vice President, Aug. 1999, USA.

[6] Advocate Puneet Bhasin, *Cyber Pornography Law in India*, (Sept. 27, 2018, 7:00 PM) https://blog.ipleaders.in/cyber-pornography-law-india/ .

[7] *Protecting Children from Online Pornography*- A report from Bombay High Court to Hon'ble Chief Justice of Bombay High Court, Jan. 30, 2002, India.

[8] The Indian Penal Code Act, 1860, No. 45, Acts of Parliament, 1860 .

e-mail address, thus the receiver of spoofed mail would trust such e-mail, presuming it to be sent by his friend. Spoofing is done to gain access to private information by camouflaging a computer as some other computer.

viii. **E-mail Spamming-** Spam is a type of trash e-mail which is sent by the companies for the advertising purposes. The messages sent through e-mail may be same or different and can be received by the receiver on regular basis. These junk e-mails can be bothersome and wastes a lot of time of the receiver.

ix. **Phishing-** Phishing can be said to be similar to e-mail spoofing wherein vital information may be obtained falsely through e-communication. The users generally fill up their vital information on a fake website or counter, believing it to be an authenticated one. In Wombat Security's latest report, 76% of information security professionals revealed that their organization experienced phishing attacks in 2017.[9]

B. CRIME AGAINST STATE OR SOCIETY

i. **Hacking-** When any person gains illegal access to others computer, computer database or network or tampering with the data or any computer programme, by breaking into the security system, amounts to crime. Hacking is a wide term and one of the primitive and perfidious cyber crimes. The techniques used for gaining illegal access may vary from stealing passwords by peeking at someone's information at work or by luring to log in on spoofed sites. As far as legal aspect is concerned, Section 66 of The Information Technology Act, 2000, defines hacking and states that whoever commits hacking shall be punished or penalised with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or both.[10]

ii.

iii. **Cyber Fraud-** In the present scenario, financial institutions carry out all their activities and money transactions through computers by way of Electronic Fund Transfer, increasing the chances of cyber fraud. Any act done with an aim to deceive a person by unjust means without the knowledge of that person is commonly known as fraud. Frauds which are practiced through computer network or internet and such related exchanges are known as cyber fraud. Most of the cybercrimes across India are related to online banking. There were about 2,095 cases of online banking fraud reported in 2017[11]. Some common ways through which cyber frauds are committed include credit card frauds, e-retail fraud, embezzlement of funds, deceptive get-rich schemes provided online and job fraud.

iv.

v. **Cyber Terrorism-** Cyber terrorism does not involve violent acts expressly and that one does not witness immediate consequences. These groups fulfil their agenda by way of spreading threat and violence through computer network. Extremist groups or preachers with ideologies different from those of reasonable ideas, use technology as

[9] The Barkly Team, *Must-know Phishing Statistics 2018*, (Sept. 29, 2018, 5:00 PM) https://blog.barkly.com/phishing-statistics-2018

[10] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

[11] Shreyas Suryanarayana, *Online Banking Fraud Tops Cyber Crime List in India*, (Sept. 27, 2018, 5:30 PM), https://www.statista.com/chart/14532/online-banking-fraud-tops-cyber-crime-list-in-india/ .

a weapon to spread those ideologies. Therefore, cyber terrorism may be defined as an act where computer set-up are used to create terror among the population at large and very often against the Government. It leads to a great threat to peace and national security.

vi. **Cyber-Squatting-** Cyber-Squatting is a form of speculation where a domain name is registered with the intention of selling off the same.[12] It refers to the activity whereby a person registers an established domain name of other's business as his own to sell it later in exchange of relevant consideration.

III. GROWTH OF CYBER LAW IN INDIA

With the evolution of the digital world, new technologies were discovered, leading to excess use of computer systems, software and networks for the processing and distribution of data. It further led to rise in legal issues and complications, which the existing laws in India were not able to deal with. With the emerging needs, it became a necessity to frame relevant and enhanced laws.

It has been observed that there is continuous addition and alteration to the already existing crimes. Cyber crimes too have shown modifications which could have been plausibly prevented with an appropriate legal infrastructure. These challenges led to the enactment of Cyber Laws in India.

The Union Cabinet approved the Information Technology bill on May 13, 2000 and on May 17, 2000; both the houses of the Indian Parliament passed the Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.[13]

Some of the objectives of IT Act, 2000 are:

- It provided legality to the e-transactions.
- It reduced the number of cyber crimes and protected the privacy of users of the Internet.
- Electronic records and other relevant activities received legal sanction.
- Book-keeping of accounts by bankers and other institutions also received legal sanction.

In 2008, changes were made to the IT Act, 2000 and came to be known as Information Technology (Amendment) Act, 2008. Amendments were made to introduce new types of cyber crimes and ways to prevent them. Some of the new provisions in order to cover those crimes are:

- Sections 66A to 66F has been inserted to Section 66 providing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.[14] However, in 2015 in a landmark case, Section 66A was struck down in entirety by the Supreme Court of India as it falls outside the scope of Article 19(2) which is associated to Freedom of Speech.[15]

[12] Dr AMITA VERMA, CYBER CRIMES & LAW 270 (1st ed. 2012) .

[13] *History of Cyber Law in India*, (Oct. 2, 2018, 12:30 PM) http://www.indiancybersecurity.com/cyber_law/8_history_of_cyber_law_in_india.html .

[14] The Information Technology (Amendment) Act, 2008, Acts of Parliament, 2008 (India).

[15] Shreya Singhal v. Union of India, A.I.R. 2015 S.C. 1523

- Section 67 of IT Act, 2000 has been amended by reducing period of detention for publishing obscene content from 5 years to 3 years and increasing the fine from Rs 1 lakh to Rs 5 lakh. Section 67A to 67C has been added wherein 67A covers materials containing obscene acts, 67B covers child pornography and 67C covers obligation of an intermediary to safeguard and keep certain records as arranged by the Central Government.[16]

The Information Technology (Amendment) Act, 2008 has brought some striking changes to the IT Act, 2000 on several issues.

IV. DIFFICULTIES TO CYBER LAW IN INDIA

The difficulties faced by Cyber Law in India are fundamental and one of the principal difficulties to the law is to keep rhythm with the escalating technology. The laws are framed keeping in view the current trends in the technology, but the laws soon become obsolete with the rapid growth in technology. Cyber laws in India are in itself a big challenge as they are not legally adequate and are not appropriately enforced.

Another major issue faced by Cyber law is the surreptitious and gigantic nature of the Internet which helps the cyber criminals to perform unlawful activities on Internet without being caught or identified. Cyber crimes leave the jurisdiction unstipulated because any individual sitting in any part of the world can corrupt other individual's network. Furthermore, cyber crimes in India are not reported by the people because of its unawareness and that it is still a growing issue. As many as 5,752 people were arrested for cyber crimes in 2014 and only 95 persons were convicted and 276 acquitted for cyber crimes in 2014.[17]

V. JUDICIAL RESPONSE

A variety of laws have been passed by the Legislature and implemented by the Executive and other controls to prevent Cyber crimes but ultimately it's the Judiciary which is in charge of administration of Justice. Judiciary takes help of precedents for deciding the cases of similar kinds but as far as Cyber crimes are concerned, there are not many precedents to be found. Thus, judiciary needs to be a step ahead while interpreting the laws on the matters pertaining to Cyber crime.

The effective response of the judiciary to settle Cyber contention is contemplated through various case-laws.

In the case of **Shreya Singhal v. Union of India**[18], the apex court had been called upon to examine the constitutional validity of Section 66A of the Information Technology Act, 2000 and its various parameters from the perspective of the various principles enshrined in the Indian Constitution. In an unprecedented judgement it declared that the said section was unconstitutional, marking the day as a time of jubilation for free speech activists. However, the said judgment was also a landmark as it upheld the power of interception under Section 69A

[16] The Information Technology (Amendment) Act, 2008, Acts of Parliament, 2008 (India).

[17] Chaitanya Mallapur, *As Internet Use Spreads, Cyber Crimes up 19 Times Over 10 Years: Report,* (Oct. 3, 2018, 3:25 PM), https://www.youthkiawaaz.com/2016/06/cyber-crime-rate-in-india/ .

[18] Shreya Singhal v. Union of India, A.I.R. 2015 S.C. 1523

of the Information Technology Act, 2000 as enshrined under the law. The Supreme Court also upheld Section 79 of the Act, pertaining to intermediary liability, but with a caveat: intermediaries in India will have to act only on court order or on order of governmental agency. The said judgment once again reiterated the principle that any provision of law, concerning the real as well as virtual world, will have to ensure compliance with the Indian Constitution.[19]

In **Satyam Infoway Ltd v. Sifynet Solutions Pvt. Ltd**[20], the Supreme Court of India decided on the issue of domain name protection for the first time in its history. This was the case wherein the apex court declared that the Indian Trade Marks Act, 1999 was applicable to the regulation of domain names as well. It held that though there was no law in India which explicitly deals with the domain names; it falls within the ambit of the Trade Marks Act. It further observed that a domain name enjoyed all features of a trademark. Accordingly, it ruled that if the respondent was allowed to further continue using the domain names it would in all likelihood create confusion in the minds of the general public. A user could be diverted to the website containing the unauthorized domain name. And upon his arrival at the website, if he does not find the goods or services associated with the mark, he might think that the legitimate owner was misrepresenting the claims. This would result in the loss for the legitimate owner, thereby affecting his goodwill and brand name. Thus, the apex court granted an injunction in favor of the appellants, thereby restraining the respondents from further using the domain names in their business transactions.[21]

In the case of **National Association of Software and Service Companies v. Ajay Sood and Ors**[22], the plaintiff in this case was India's premier software association. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognized the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for

[19] Pavan Duggal, *Why 2015 Was a Landmark Year for Indian Cyberlaw* (Oct. 4, 2018, 12:43 PM), https://www.huffingtonpost.in/pavan-duggal-/2015-a-landmark-year-for-_b_8898122.html .

[20] Satyam Infoway Ltd v. Sifynet Solutions Pvt. Ltd, A.I.R. 2004 S.C. 3540

[21] Law Wire Team, *Satyam Infoway Ltd v. Sifynet Solutions Pvt. Ltd, Supreme Court of India AIR 2004 SC 3450*,(Oct. 4, 2018, 1:36 PM), http://www.lawinfowire.com/articleinfo/satyam-infoway-ltd-v-sifynet-solutions-pvt-supreme-court-india-air-2004-sc-3540 .

[22] National Association of Software and Service Companies v. Ajay Sood and Ors., 2005 (30) PTC 437 Del

violation of the plaintiff's trademark rights.[23]

Although, it is going to be challenging for the judiciary to overcome the hurdles with changing times but, the above cited landmark cases acted as eye-openers and helped to interpret the laws in a different way.

VI. AUTHOR'S VIEWPOINTS

As authors, we have made an attempt to present these new species of crime in a precise manner for the better understanding of the readers. The research regarding the subject matter made us realise about its complexities and vastness and the challenges arising out of it. The viewpoints which we present are concerning the cyber security.

To prevent cyber crimes, the statutory provisions should be adequate enough and be fully complied with. Besides that, the relevant authorities must be fully aware and well equipped with, in order to face the operational challenges such as convictions. The Judiciary needs to be conscious and responsive towards cyber crimes so that the convictions can become prominent.

For better prevention, co-operation between the Indian Agencies and Foreign Authorities should be made possible, so that Cyber security is achieved. It is not possible to achieve security and prevention in entirety but new initiatives must be taken and it's all that counts.

VII. CONCLUSION

Technology has made the world a global circle by bringing the people living in different dimensions of the world together with just few clicks and clacks. Internet helped reduce the time and distance constrictions. However, every great innovation does not come alone and brings hazards along with it such is the nature of Cyberspace. With every new invention comes bigger responsibility and with such opinion many countries including India have adopted the UNCITRAL Model Law for enacting the laws regarding the computer network and the Internet. The United Nations Commission on International Trade Law (UNCITRAL) framed the 'Model Law on Electronic Commerce' which makes it compulsory for the member nations to follow while structuring the Cyber laws.

This new species of crime has grown immensely in the last few decades and though the laws to avert them did not come up in the due time but the Information Technology Act, 2000 opened up new gateways and it is sincerely hoped that it establishes better Cyber security.

*****

[23] Ankit Mathur, *Case study cyber law - Nasscom vs. Ajay Sood & Others*, (Oct. 4, 2018, 3:50 PM) , http://cyber-law-web.blogspot.com/2009/07/case-study-cyber-law-nasscom-vs-ajay.html .