International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 15-05-2022, Accepted: 30-05-2022, Published: 17-06-2022
Volume 8, Issue 3, 2022, Page No. 150-153

Cyber crimes and social media

Ravi
Research Scholar, Department of Law, Shri JJT University Jhunjhunu, Rajasthan, India

Abstract
Cybercrime is a crime that involves a computer and network .The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may harm someone security and financial health. Like, cybercrimes hacking, identity theft cyber stalking, steal photos form social media etc. An important of cybercrimes is its non-local character action can occur in jurisdiction separated by vast distances This poses severe problems for law enforcement since previously local or even national crime now require international cooperation. The term cybercrime may be judicially interpreted in some judgments passed by courts in India It is not defined in any act or statute passed by the India Legislature. Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life .Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience.It is a medium which is infinite and immeasurable. Social media is a weapon that is capable of construction as well as destruction. The real power of the prevailing social media platforms becomes evident by witnessing the influence created by these platforms on a large scale. It plays a significant role in everyday life.The rising popularity due to its ability to make people attached with kith and kin have paved the way for the world to share photos, feelings, videos, which bears a high-security concern.

Keywords: cybercrime, social media, hacking, cyber stalking

Introduction

In today era all the work being done through internet .Even the toughest tasks are being done very easily with the internet .nowadays people are completely dependent on internet. Everyone is aware of internet but not everyone known about what is cybercrime .Crime is different in the whole world, out of which cybercrime is also one which is done through internet in phone, computer and laptop .Today people are spending more and more time on social media platforms like Facebook, whatsapp and twitter etc. There is no doubt that this platforms is a criminal activity which is done through computer and internet .Such crime on these platforms include a wide range of activities including extortion, identity theft, credit card fraud, hacking personal data, phishing, illegal downloading, cyber stalking, virus propagation .On an average, lakhs of complaints reach the police every month due to cyber crime, the police take the help of cyber cell to settle these complaints. It is stated that millions of these cyberattacks could be proliferated onto cyberspace whose analysis would turn up complicated .This posts severe necessity to stay alert on such attackers' prevalence and protect oneself or network against such activities where such an awareness alone does not hold any good an implementation point of view. cyber defamation refers to publication of defamatory content in electronic form In order to determine cyber defamation, the court has taken into consideration factors like time of occurrence, mode of publication and jurisdiction. Cyber security poses bigger threat than any other spectrum of technology. Cyber criminals have already all -ready started abusing technology controlled devices for propelling cyber -crimes such as frauds and thefts. With technology protocols, still being developed and evolving at a gradual pace, it is very difficult to avoid such cyber -attacks.Lot plays a dramatic role in shaping the future of technology in India. with loT now becoming backbone of various ventures, firms, organization and even basic ways of living, it is worrying that India has no dedicated law for loT and some kind of guidance can be referred from the Information Act, 2000. The Digital India Initiative is driving our country towards a digitized life where the existence will highly depend on elements like cloud computing, 5G in telecom, e-commerce etc. It is imperative to keep a check on loose ends.

Definition of Cyber Crime: Cyber Crime be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime.

Crime Against Property: Some online crime occur against property, such as a computer of server. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement, and IPR violation.

Crime Against Government: When a cybercrime is committed against the government, it is considered an attack on that nation sovereignty. Cyber- crime against the government include hacking, accessing confidential information, cyber warfare, cyber terrorism, and pirated software

Misuse of social media

So many people are using social networking site in access through their mobile phones, laptops or by any other gadgets. And people feel happy to show their expertise on uploading new videos and photos or by writing some text or comment. These sites are making the life of individuals so easy that on one finger movement they can connect with their friend but still most of the people are not aware with the drawback of using these sites in access basically we are sharing our all information with these sites and that can be misused anyway. Face book, whatsApp and Instagram are the place where one can easily fetch your information regarding your location and your personal profile. However the maximum part of users is covered by teenagers in India Gangopdhyay and Dhar have posted a document in which they have got noted that social websites attract young adults and permit them opportunities to get along with regarded and unknown human.

Government has taken several steps to prevent and mitigate cyber security include. These include-

- Established of National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country.
- All Organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
- Cyber Swachhta Kendre (Botnet Cleaning and Malware Analysis centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.
- Issue of alert and advisories regarding cyber threats and counter -measures by CERT-In Provisions for audit of the government websites and application prior to their hosting, and thereafter at regular intervals.
- Empanelment of security auditing organisations to support and implementation of information security best practices.
- Formulation of crisis Management plan for countering attacks and cyber terrorism.
- Conducting regular training programmes for network/ system administration and chief Information Security Officers (CISOs) of Government and critical sector Organisation regarding securing the IT infrastructure and mitigating cyber -attacks.
- Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

Penal Provisions under Information Technology Act, 2000 for Cyber crimes

The following penal provisions under discuss below

Sec.65 Tampering with computer source documents – Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer,computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force,shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees or with both.

Sec. 66 Computer related offences: If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

S**ec. 66A. Punishment for sending offensive messages through communication service, etc.:** Any person who sends, by means of a computer resource or a communication device, -

Any information that is grossly offensive or has menacing character.

Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, dander, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will persistently by making use of such computer resource or a communication device.

Any electronic mail or electronic massage for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or about the origin of such messages.

Shreya Singhal v/s Union of India (2015) 5 SCC 1 -In this case supreme court held that in its landmark judgment struck down section 66A of the information Technology Act,2000 which provided provisions for the arrest of those who posted allegedly offensive content on the internet upholding freedom of expression. Section 66A defines the punishment for sending "offensive"messages through computer or any other communication device like a mobile phone or tablet and a conviction of it can fetch a maximum three years of jail and a fine. Over the last couple of years there has been many cases in which police has arrested the broadcasting of any information through a computer resource or a communication device, which was "grossly offensive" or "menacing" in character, or which, among other things as much as cause" annoyance." "inconvenience," obstruction." In a judgment authored by Justice R.F. Nariman, on behalf of a bench comprising himself and Justice J. Chelameswar, the Court has now declared that section 66A is not only vague and arbitrary, but that it also "disproportionately invades the right of free speech. In quashing section 66A, in Shreya Singhal, the Supreme court has not only given afresh lease of life to free speech in India, but has also performed its role as a constitutional court for Indians. The Court has provided the jurisprudence of free speech with an enhanced and

rare clarity. Various provisions of IPC and section 66B and 67C of the IT Act are good enough to deal with all these crimes and it is incorrect to say that section 66A has given rise to new forms of crime.

Sec 66B. Punishment for dishonestly receiving stolen computer resource or communication device: whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment or either description for a term which may extend to three years or with fine which may extend to rupees one lakh.

Sec 66C. Punishment for identity theft: Whoever fraudulently or dishonestly make use of the electronic signature or any password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Sec.66D punishment for cheating by personation by using computer resource: Whoever by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Sec.66E Punishment for violation of privacy: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Crimes through social media against women in Indian Penal Code, 1860

- Sexual Harassment -sec 354A of IPC
- Stalking -sec 354D of IPC
- Defamation -Sec 499 of IPC
- Criminal Intimidation -Sec 503 of IPC
- Word, gesture, or act intended to insult the modesty of a woman (Even-teasing) Sec 509 of IPC

The list of provisions of IPC listed above can happen to be applicable in a far-fetched manner in the case of that woman. Also because of the absence of a specific law regarding such offenses online, the provisions of IPC are subjected to the interpretation that they also govern cybercrimes but in the bare provisions there is no mention of committing any act online. This is nothing but a shock to the wide diversity of India and its innumerable legislation for almost everything but the absence of a specific law for such grave misconducts/crimes happening daily online.We may observe that by the actions done by a person mentioned in the first paragraph of this subheading, he has tried to outrage the modesty of a woman but the IPC provision concerning the same i.e.section 354 of IPC could not be enforced specifically against the person as the provision doesn't mention doing such an act online .

Conclusion

Cyber Crime are a new class of crimes to India rapidly expanding due to extensive use of internet.Dishonest and greedy people take advantage of easy and free access to internet and perform any acts to satisfy their needs.The need could be physiological or psychological in nature.Online shopping and wide use of social media are root cause of cybercrimes .Much awareness created for cybercrimes and users were educated.But still people do not complain it to authorities. Even somebody do it then also police or crime branch unable to clear such complains in reasonable time period. Delay in justice will lead to NO registration of complain. This is not healthy situation in free democratic India. The law IT (Information Technology) Act 2000and several sections of the IPC are in place but in large population country like China and India, it is very difficult to control crime caused by cyber world. Cyber Crime is a crime which is difficult to detect and stop once occurred leave a long term effect on victims. Cyber Crime is increasing day by day due to over use of social media, online shopping, and internet banking which need sensitive financial and personal data. The development in emerging internet technology and its wide spread knowledge leads to security issues, cybercrime, internet hackers and intruders.The charm of internet enhances the network structure that construct vast online theft,fraud are called as cyber-attacks in cybercrime.

There are different types of cybercrimes which makes the cyber world vulnerable to various threats. Some of the commonly used methods to hook people are Cyber -Stalking, Cyber Assassination, Bluffing and more. There is need to have idea about these crimes to as to safely navigate in the cyber world. Cyber crime is on peak as we all are using internet and social media but we are still lacking behind the drawbacks of using that in access. So many people are still not aware that what is happening behind the thing. Crime data is an insightful domain where effective awareness plays a vital role in crime analysis. In this paper specification of social media user and their awareness towards cybercrime is analyzed by using some data from internet.

References

1. The Information Technology Act,2000
2. https://main.sci.gov.in
3. https://www.covergenceindia.org/blog/cyber-security-challenges-solutions.aspx https://www.britannica.com
4. https://www.swierlaw.com/faqs/what-are-the-three-types-off-cyber-crimes-cfm
5. https://www.researchgate.netAnalysis of Cybercrime on Social Media Platform and its Challenges
6. https://www.britannica.com
7. https://www.livelaw.in/law-firms/law-firm-article-/section-66a-information -technology-act-2000-shreya-singhal-case-183816
8. http://ww.legalservicesindia.com/article/2473/shreya-singhal-v-U.O.I.HTMI
9. American Journal of Computer Science and Engineering Survey.ISSN 2349-7238 .AjCSES,2016:4(2):029-032. TOPIC - Study of online cyber crimes in India -Subhash Desai
10. BSSS Journal of computer :ISSN(PRINT)-0975-7228,E-ISSN -2582-4880,2020:XI(I):1-7. Cyber Crime analysis on social media -Swati Sharma, Vikash kumar Sharma
11. International Journal of law Management &Humanities (ISSN 2581-5369) VOL-3,Issue 6, Influence of Social Media and Growth of Cyber Crime -A Study -Ms. Neha Gupta