RISE OF CYBERCRIMES AND MASS SURVELLIANCE AS A THREAT TO CIVILIZATION: AN ANALYSIS

Written by ***Dr. Jharasri Paikaray***

Faulty of Law, P.G. Dept. of Law, Utkal University, Odisha

ABSTRACT:

The introduction of internet, people have come up with ways to pervade it. As the information and communication sector develops, the cyber criminals are also developing ways of keeping the pace with the new security measures. Since the internet is soon becoming one of the many necessity a person can't stay without the criminals advancing the sector also to keep up with ever changing technology. The criminals will find every loop hole to sneak to your private information that has been stored in our PC or even in cloud storage as long the storage is connected to the internet. Cyber crime is defined as the act of creating, distributing, altering, stealing, misusing or destroying of information through the computer without the use of physical force and against the will of the victim. In this paper the author focused on different causes of cybercrime and different forms of cybercrime committed by criminals. It is very difficult to caught the cyber criminals in this 21st Century. The establishment of IT Act, 2000/2008 some how gives protection to the people like a piece of bread on the hand of a hungry man. So the author stressed for enacting a detailed legislation for reducing cybercrimes from our society.

Key words: Internet, cybercrimes, cyber flashing, technology, websites, motivated.

INTRODUCTION:

The internet has developed so rapidly since the 1990's that we have now entered an age where we require laws to regulate and govern it. Essentially, the internet relies upon voluntary adherence and theoretically is a network of people passing along pockets of information so that where the time comes you pass along packets for them. Tim Berness Lee, the inventor of world

ISSN 2581 6551
VOLUME 7 – 2022

wide web, conceived it with the idea that the internet was meant to be decentralized and an absence of choke point should make it impossible for one person to control. However, this utopian internet now seems to be threatened by governments and business corporations world wide who are seeking regulation, control and accountability to make profits. The central idea behind the conception of the internet was to enable and increase the exchange of information and this fundamental exchange has since the commencement increase human interactions and its openness is coming under threat by business. [1]The 'generative technology' has since 2006-07 started experiencing security issues due to several leaks, hacks and attacks. As a result of the security issues, surveillance has become a key area for research in this field and the privacy of individuals has come under scrutiny. It is not an uncart fact that privacy is an inherent human right and therefore any threat to privacy be it physical or digital results in activism. The need for governance right from sexual orientation to privacy is resulting in the creation of cyber war between the citizens on one front and government and business on the other. A Cyber-attack has capability of paralyzing the critical infrastructure of a country and damage could range from simple shut down to complex paralysis of significant portion of infrastructure of entire country like meltdown of nuclear reactors, disabling power plants, causing war planers to crash, cut off military command to control and malfunction civilian and military networks by controlling and choking the cyberspace from one end of the spectrum.

CAUSES OF CYBERCRIME:

1) Economically motivated cybercrime: - As the case with many crimes committed outside the internet money is a major motivator for many cybercriminals. Especially because the dangers of criminality are less apparent when the person is hiding behind a network, the perception of low risk and very high financial reward prompts many cyber criminals to engage in malware, phishing, identity theft and fraudulent money request attacks. Business week estimates that cyber crimes targeting online banking accounts alone, for example Pull in nearly 700 million dollars per year globally.[2]

[1] . Govil,J.2007, "Ramifications of cybercrime and suggestive preventive measures",2007 IEEE International,17-20 May, Chicago, USA, pp.610-615
[2] Combating cybercrime, Department of Homeland security. 19th June, 2012. Retrieved 1 November 2019.

ISSN 2581 6551
VOLUME 7 – 2022

2) Ideologically motivated cybercrime:- After financial companies like Visa, Master card and Paypal refused to let account and card holders make contribution to the controversial non- profit wikileaks, the hacktivist group anonymous coordinated a series of boat attacks on the companies servers rendering them unreachable to internet used. These kinds of attacks are conducted for perceived ethical ideological or moral reasons damaging or disabling compute equipment and networks to express grievances against individuals, corporations, organizations or even national governments.
3) Personally motivated cybercrime: - Cyber criminals are still human beings and what they including their crimes are often the cause of personal emotions and vendettas from the disgranted employee installing a virus on office computers to a jealous boyfriend hacking into a girl friend's social media accounts or a teenager taking down a school websites just to prove that he could do it, many cybercrimes are essentially of passion committed over the internet. Many of these crimes however can still have very serious impacts and cause considerable property damage.[3]
4) Potential economic impact:- As today's consumer has become increasingly dependent on computers, networks and the information these are used to store and preserve, the risk of being subjected to cybercrime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies surveyed acknowledged financial losses due to computer breaches. As the company or economy increases its reliance on the internet it is exposed to all the threats posed by cyber criminals. Stocks are traded via internet, bank transaction are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.
5) Possession of unauthorized information: - It is very easy to access any information by the terrorist with the aid of internet and to possess that information for political, religious, social, ideological objectives. New categories of cybercrimes from email hacking to software privacy from cyber stalking to cyber terrorism are taking place with qualified world of information and communication.

[3] "ASEAN Declaration to Prevent and Combat Cybercrime", ASEAN,14th November 2017. Archived from the original on 3 July 2021. Retrieved 5 June 2022.

ISSN 2581 6551
VOLUME 7 – 2022

NATIONAL PLAN TO COMBAT CYBERCRIME:

It is suggested that alike the developed countries, Indian Government should also initiate a National Plan to combat cybercrime. This national plan should intent to work on the following objectives and key priorities:

i) Educating the community to protect themselves.
ii) Partnering with industry to tackle the shares problem of cybercrime.
iii) Fostering intelligence led approach and sharing information.
iv) Improving the capacity and capability of agencies to address cybercrime.
v) Ensuring effective criminal justice system.
vi) Improving international cooperation on cybercrime.

THE INFORMATION TECHNOLOGY ACT:

Recurrent cyber offences, particularly due to the introduction of the Aadhar Scheme by the Unique Identification Authority of India (UIDAI) have made conspicuous the loopholes in the Information Technology Act, 2000. Having said that what is landable is the acknowledgement of the flaws by the legislature and its willingness to make amendments to the legislation. "Crime is crime because it consists in wrongdoing which directly and in serious degree threatens the security or wellbeing of society and because it is not safe to leave it redressable only by compensation of the party injured." Upon a perusal of the lines, one could understand the severity of an act that constitutes crime: wrongdoing which directly threatens the society of equal relevance is the observation that it is something that cannot be redressed by compensation alone. However, there is something more significant then the act of wrongdoing itself which this definition fails to address i.e. the mensrea of the accused. Intentional criminal jurisprudence acknowledges that these can be no crime, large or small without an evil mind as the essence of a crime is its wrongful intent without which it cannot exist. Consequently to punish conduct without reference to the state of mind of an actor is both inefficacious and unjust.[4]

[4] Joseph, Aghatise E. (28 June 2006). "Cybercrime definition".

ISSN 2581 6551
VOLUME 7 – 2022

Section 66 of the IT Act which is a criminal provision punishes acts falling under section 43 of the IT Act when done "fraudulently or dishonestly". The first ingredient of Section 43 of the IT Act, in its relevant part, covers the act of accessing a computer, downloading, copying or entrancing any data or information from such a computer. The analysis undertaken, however has little to do with the first ingredient. For our purposes, it is the required intention which is pertinent to highest. Briefly the two degrees of intention mentioned in the provision could be understood as follows;

Fraudulently- An act is done fraudulently when done with an intention to defraud. Where there is a benefit or advantage or even the likelihood of advantage to the deceiver as a result of the deceit, he is said to have an intention to defraud.[5]

Dishonestly- An intention gain wrongfully by getting what one does not have amounts to a dishonest intention. To gain wrongfully simply indicates towards gaining unlawfully.

Applying the legal maxim, let us determine whether the actions of the individuals who attempted to access the Aadhar database by opening the link satisfy the requisite intention. Neither does their act deceive anyone nor does it involve an advantage or even its likelihood for the matter. Accordingly, it does not amount to a fraudulent act. Similarly, in the absence of an intention to gain wrongfully, their act is so dishonest. Therefore the actions of the people though not satisfying the ingredients of the less serious offence punishable under Section 66 of the IT Act clearly satisfy the essential under the more serious offence punishable under Section 70 of the IT Act. Hence, the addition of either of the two degrees of intention appearing in the former provision to the letter as an essential requirement would restrict the ambit of the provision and would thereby solve the problem to a great extent. This elucidates how certain criminal provisions of the IT Act drafted in all embracing manner require a stricter wording to exclude ethical hackers. This exigency demands that other degree of mensrea be incorporated in the provisions of Sections 66& 70 of IT Act.

"CYBER FLASHING"- A NEW AGE FORM OF CYBER SEXUAL HARASSMENT:

[5] "Cybercrime threat response". www.interpol.int. Retrieved 17 May 2021

Intentionally sending unsolicited media which may be considered obscene is referred to as cyber-flashing. This may include pictures of pornography or other such items which may evoke feelings of repulsiveness in the minds of the receiver. Though reported cases are rare in India and these has not been much legal development in this sphere, it is quite likely that you or someone you know has encountered such an incident at least once if not more. It should be understood without a doubt that cyber flashing amounts to cyber sexual harassment.[6] The rising menace of cyber flashing has forced countries such as Singapore and Scotland and the State of Texas, USA to come up with specific laws to deal with this digital form of sexual harassment. The United Kingdom too is working on a legal framework for its prevention. It is high time that India follows suit as well.

The coronavirus lockdown situation has seen many of us increasingly finding ourselves on online platforms for various purposes such as work, leisure, communication, academia etc. In the lack of a proper legal framework meant for dealing with this issue, incidents of cyber flashing are already on the rise and are likely to be on an upword trend from here on online class being attended by children held via zoom having already been cyber flashed.

THE INTERNET RISKS OF CYBER-FLASHING:

India is rife with sexual abuse and harassment. For many, the online world is a safe space from the sexual harassment faced daily in the physical world. Thus, facing harassment even online in the form of cyber flashing leaves many, with no safe space be it physical or virtual. Cyber-flashing can be especially traumatizing for victims of sexual abuse or assault. Moreover, cyber flashing by friends or other known people under the garb of pranks ends up wrongly, trivializing an act of sexual harassment as a mere joke or something to be laughed off rather than being taken seriously. In a patriarchal and conservative society like ours if such an incident of cyber flashing occurs in front of family members a woman may end up losing access to her phone or computer for literally no fault of losing access to the online world as well.[7]

[6] Prof. Dr. Gercke, M.(Sept.2012). Understanding Cybercrime; Phenomena, challenges and legal response.
[7] Forensic Examination of Digital Evidence: A Guide for Law Enforcement NCJ 199408, Spril 2004, Special Report, National Institute of Justice.

ISSN 2581 6551
VOLUME 7 – 2022

The threat posed by cyber flashing is the greatest for children. They may not understand that they have been cyber flashed. Due to their lack of understanding of the matter or because of fear or the shame involved they may find it extremely hard to convey it to their parents or guardians that they have been cyber flashed. [8]As has been pointed our reporting of cases of cyber-flashing is rare. This is because of multifactor, primarily among there being having to deal with the police and the lack of proper legal training.

NEED OF LEGAL FRAMEWORK:

Due to lack of a proper legal framework to deal with this specific kind of act, most incidents of cyber flashing in India are as of new booked under various existing sections of the IPC and IT Act, 2000. On a very wide and subjective application of the provisions originally meant to deal with other kinds of offences and thereby having their own short comings. The IT laws in India have no separate provisions to report an unwanted sexually explicit picture or video. This combined with the general difficulty of dealing with and reporting of sexual harassment due to the stigma that it still attached to it and the undeniable fact that there is hardly any legal awareness regarding cyber flashing and cyber sexual harassment in general contributes significantly to the problem. All these factors mixed in with the slow and cumbersome legal processes results in the victims reluctance to report such incidents considering that the penal code of Singapore is basically a derivative of the Indian Penal Code,1860 and both having a lot of commonalities a section based on the Section 377 BF(2) of the Penal Code of Singapore sans the causing could possibly be inserted directly into the IPC without being inconsonant with other sections of the legislation. India could possibly come up with similar legislation focusing explicitly. On sexual offences under which all the required provisions to deal with cyber-flashing.

WHATSAPP CHATS AND CRIMINAL INVESTIGATIONS:

[8] http://www.usdoj.gov/criminal/cybercrime.

ISSN 2581 6551
VOLUME 7 – 2022

Today smartphones are not merely part of our life they are our life. They contains the combined foot print of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes were sexually in the owner's life (United States vs. Adamou Djibo).

Recently, there has been a great deal of controversy surrounding the use of whatsapp chats in criminal investigations considering the extent of private information that is contained in these chats. The Indiana Supreme Court in the United States was recently faced with this significant constitutional question in the case of (Seo vs. State,2020) in order to ascertain when police authorities access the locked phone of an accused can it compete the accused to unlock it or provide the password? The petitioner, Seo was accused of harassing. DS who had first contacted with a number associated with her iphone. Subsequently, DS started receiving multiple calls and text messages from various unassigned numbers and the police authorities believed that Seo was placing those calls by concealing her phone number through a mobile app. The police arrested Seo and obtained a warrant that ordered her to unlock her iphone so that police could search it. However, Seo refused to unlock her iphone and she was held in contempt by the trial court. She subsequently appealed against the contempt order and the Indiana Supreme court reversed the same, observing that forcing Seo to unlock her iphone would violate her right against self-incrimination. The decision in Seo raises an interesting question in Indian context also. Article 20(3) of the Indian Constitution mandates that "no person accused of the offence shall be compelled to be a witness against himself".

CRIMINAL LAW IN CYBER SPACE:

India does not have a separate legislation concerning cybercrime and abuse against women and children. The Information Technology Act, 2000 (IT Act) coupled with the Indian Penal Code, 1860 provides punishment in the form of imprisonment ranging from two years to life imprisonment and fine depending on the nature of cybercrime.

THE INFORMATION TECHNOLOGY ACT,2000:

The Information Technology Act primarily aims at providing a legal infrastructure to promote e-commerce in India. It has little to do with individual and personal citizen's rights, it is

ISSN 2581 6551
VOLUME 7 – 2022

inadequate to deal with cyber rights and individual protection under the law. The IT Act initially covered cybercrime with a broad brush and it was only in 2008 amended and provisions were made to take certain cybercrimes within its field. Sections 67, 67(A) and 67(B) are primarily provisions dealing with acts which are obscene, sexually explicit and transmission material depicting children in sexually explicit acts, respectively. These provisions of the IT Act are too broad and they fail to address crimes such as morphing, phishing and cyber bullying. The piece meal approach adopted by the legislature is highly in effective and there is a need for enacting a detailed legislation governing cybercrimes.[9]

MEASURES TAKEN BY THE JUDICIARY:

The increasing instances of cybercrimes against women and children have also drawn the attention of the judiciary. The case of Suhas Katti v. State of Tamil Nadu is notable in this regard where in the conviction was achieved in few months form when the FIR was filed. The case revolved around the posting of obscene and defamatory messages against a woman on a Yahoo messenger group. This case is touted as the first caswe of conviction under Section 67 of the IT Act. Various courts have also passed similar judgments holding perpetrators accountable for cybercrimes. For instance in the case of Yodesh Prabhu vs. State of Maharashtra the accused was convicted under Section 509 of the Indian Penal Code along with Section 66E of the IT Act for stalking and sending obscene images to collegues. This is one of the first case of conviction for cyber stalking in India.[10] The judiciary has shown its stern stance against cybercrimes by awarding the maximum punishment under law for such offences, in most cases. The law enforcement agencies should be sensitized about the various facets of cybercrimes against women and children and the entire redress mechanism should be fast tracked.

CONCLUSION:

[9] Mehan, J.(2014). Cyber War, Cyber Terror, cyber Crime and Cyber- Activism: an in depth guide to the role of standards, in the cybersecurity environment. IT Governance Publishing.
[10] www.haltabuse.org. Retrieved 4 December 2019. "Federal Cyberstalking Bill info".

ISSN 2581 6551
VOLUME 7 – 2022

Cybercrime is a dangerous crime involving the use of internet and computers. It is becoming harder to stop as new technologies emerge, its impacts widespread and overwhelming financially. Through this the illegal transfer of data and information is made which is confidential value to an individual or a group. It is the most prevailing crime in the present scenario done through the internet. Through increased awareness, detailed legislation which can target cybercrime and by utilizing biometrics greatly enhance security. Apart from that the vigilant behavior and following the safety protocols are only helping aids which can reduce the occurance of cybercrime. Cybercrime is only going to get worse overtime unless preventive measures are taken to stop it. One thing must be accepted as 'Prevention is better than Cure', especially when the cure is not available.

ISSN 2581 6551
VOLUME 7 – 2022