

ISSN: 2582 - 2942



LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- V

JUNE 2020

DISCLAIMER

NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR COPIED IN ANY FORM BY ANY MEANS WITHOUT PRIOR WRITTEN PERMISSION OF EDITOR-IN-CHIEF OF LEXFORTI LEGAL JOURNAL. THE EDITORIAL TEAM OF LEXFORTI LEGAL JOURNAL HOLDS THE COPYRIGHT TO ALL ARTICLES CONTRIBUTED TO THIS PUBLICATION. THE VIEWS EXPRESSED IN THIS PUBLICATION ARE PURELY PERSONAL OPINIONS OF THE AUTHORS AND DO NOT REFLECT THE VIEWS OF THE EDITORIAL TEAM OF LEXFORTI. THOUGH ALL EFFORTS ARE MADE TO ENSURE THE ACCURACY AND CORRECTNESS OF THE INFORMATION PUBLISHED, LEXFORTI SHALL NOT BE RESPONSIBLE FOR ANY ERRORS CAUSED DUE TO OVERSIGHT OTHERWISE.

ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE
OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICFAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS
INTERNATIONAL UNIVERSITY) - MARKETING
MANAGEMENT

EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION
BUSINESS LAW)

EDITOR

DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL
AND ADMINISTRATIVE LAW)., NET (TWICE) AND
SET (MAH.)

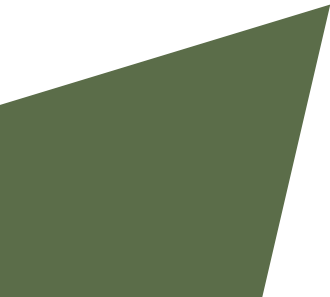
EDITOR

MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE

ABOUT US

LEXFORTI IS A FREE OPEN ACCESS PEER-REVIEWED JOURNAL, WHICH GIVES INSIGHT UPON BROAD AND DYNAMIC LEGAL ISSUES. THE VERY OBJECTIVE OF THE LEXFORTI IS TO PROVIDE OPEN AND FREE ACCESS TO KNOWLEDGE TO EVERYONE. LEXFORTI IS HIGHLY COMMITTED TO HELPING LAW STUDENTS TO GET THEIR RESEARCH ARTICLES PUBLISHED AND AN AVENUE TO THE ASPIRING STUDENTS, TEACHERS AND SCHOLARS TO MAKE A CONTRIBUTION IN THE LEGAL SPHERE. LEXFORTI REVOLVES AROUND THE FIRMAMENT OF LEGAL ISSUES; CONSISTING OF CORPORATE LAW, FAMILY LAW, CONTRACT LAW, TAXATION, ALTERNATIVE DISPUTE RESOLUTION, IP LAWS, CRIMINAL LAWS AND VARIOUS OTHER CIVIL ISSUES.



Cyber Crimes: A wrong use of Technology against the Society

Carishma Bhargava

ABSTRACT

“Cyber Security is as important as Economic Safety in these days”. Like many other crimes Cyber Crimes are also nowadays increasing. Crime committed using a computer and the internet to steal a person’s identity or illegal imports or malicious programs. Cyber Crimes is very harmful to each and every individual as it directly includes theft of their personal data which can harm their respect in the society, cybercrime have a great deal of negative impact on our society and economy and business because for our society cybercrimes could be seen in the form of bullying, identity theft, cyber stalking and cyber defamation which results creating a very awkward situation for the victims of these attacks. Different forms of Cyber Crimes affecting our society are as follows:

- *Cyber Pornography*
- *Cyber Terrorism*
- *Cyber Bullying*
- *Exploitation of Girls and Trafficking of Children*
- *Cyber Harassment*

Cyber Crimes affects Economy and Business as well as there are many cases of Data Theft and other Cyber Attacks on some big business houses recorded in the last few years. Every year Companies spend millions of Dollars in order to secure their system from any kind of Cyber Theft, misuse of their documents. Cyber Crimes not only affect any individual economically but they affect them mentally also like in case of woman’s outraging the modesty of women by sharing their pictures on internet and it also hamper the mental growth of any teenager these days as many teenagers get into this cyber trap and ending their lives by suicides and depression. In order to protect all individuals from cybercrimes there are many laws relating to prevention of cybercrimes they are as follows:

1. *Information and Technology Act 2000*
 2. *Indian Penal Code 1860*
-

INTRODUCTION

Cyber Crimes can be defined as Acts that are punishable by the Informational Technology Act, moreover the Indian Penal Code have also some provisions regarding the cyber laws. Cyber Crimes are not defined anywhere particularly in general these are does not differ from crime in te conventional sense except the method adopted for commission of crime. As there are different forms of misuse of information technology a exact definition of cybercrime is not possible, and if the misuse of information technology is finalized then the new ways can be easily drawn by the experts. Moreover, Cyber Crime is any illegal behaviour directed by means of electric operations that targets the security of computer systems and the data proceed by them.

In order to deal with Cyber Crimes Cyber Laws were Enacted which generally deals with all aspect of Electronic Communication and regulatory aspect of internet. The Cyber Law is the branch of law which handles the legal aspect while using the internet. It means that anything concerned with related to any legal activity of the internet user in the cyberspace is covered in the cyber law. The term Cyber Crime is the creation of Information Technology World and also may said to be those species of which genus is the conventional crime and the computer is either an object or subject of the conduct constituting crime it could also be said that any criminal activity that uses computer either as an instrumentality or as a means for the commencement of other crimes.

ESSENTIALS OF CYBER CRIME

As nowadays the development in technology has created new ways to commit a crime which is called Cyber Crime but it is radically different from the normal crime and its characteristics are all Together different from that of a conventional crime the most common feature of such crimes is that

- Easy to commit
- Difficult to detect
- Harder to prove

In many cases even the victim affected by cyber-crime is unaware of its occurrence, this could be due to lack of adequate skills and also the knowledge as to how to handle the computer system. Cyber Crime have been categorized as high-tech offences because they are committed by using computer network and telecommunication technology in a wrong and abusive manner and has a range to affect the socioeconomic and the legal rights of people. Like any other cybercrimes the high technology cybercrimes which are committed with the help of computer networks has the following problems

1. The perpetrators as well as victim both remain unanonymous and are difficult to be identified
2. There are many unspecified potential customers that are used which may be far away from the place of crime
3. The evidence against the crime could easily be erased thus making the victim helpless

TYPES OF CYBER CRIMES

CYBER PORNOGRAPHY-

It could be defined as an act of using cyber space to create, display, import or publish pornography or obscene material especially depicting children engaged in sexual acts with adults therefore cyber pornography is considered as a criminal offence classified as causing harm to the persons. In May 2002 one of the biggest publicized catches of Child Pornography Perpetrators was launched which was named Operation Ore as such pornography access was increasing the FBI started accessing the credit card details, e-mail address and home addresses of thousands of pornographers accessing child pornography sites and the cases were given to the British police for investigation. After the investigation the arrest of a computer consultant in taxes that led to an International Investigation that jailed Thomas Reddy with a life imprisonment for running the pornographic ring. After this the following acts were implemented : Child Obscenity and Pornography Prevention Act: The act was introduced on 30 April 2002 by US Representative Lamar Smith with the motive to stop Child Pornography and Obscenity Trafficking, the solicitation of visual depiction of children under the age of 18 involving themselves in sexually explicit conduct and the use of child pornography and obscenity to carry out crimes against children. Further under this act it was made illegal to produce, Distribute or own computer made child pornography images appearing to be same to that of the image of a real children finally through this act the government's access to e-mail was expanded without the order of the courts.

In India under the Information Technology Act 2000 Cyber Pornography is a grey area of law where it is illegal under the section 67 of the IT Act 2000 makes the following act punishable up to 3 years and fine up to 5 lakhs.

- Publication- This includes uploading on a website, whatsapp groups or any other digital portals where 3rd parties could have access to obscenity scenes

- Transmission- This includes sending obscene photos to any person via e-mail messaging or any form of digital media.

In the famous Baze.com the CEO Avinash Bajaj was arrested for an advertisement by a user to sell DPS sex scandal video it was held in this case that intermediary guidelines were passed in the year 2001 where an intermediary liability would be absolved if they exercise due diligence to ensure that such content is not displayed on their portal.

CYBER TERRORISM –

Cyber Terrorism is defined as using the internet to conduct acts which are violent in nature that results, threatens, loss of life and body injury with an aim to achieve political and ideological games through such acts. Sometimes Internet Terrorism are also considered as an act where terrorist activities which includes act of deliberate, large scale disruption of computer networks , mainly of computer networks which are connected to internet by the means of tools such as computer viruses, computer worms and other malicious software and hardware methods and various programming scripts. In regard to India the country was among top five nations which were affected by the Cyber Terrorism as well as the country is on the threshold of a digital age and the use of Aadhaar Card or any other identity is becoming Ubiquitous. The most dangerous thing is that if it becomes easier to make an identity online it could be bought and can be used wrongfully by hackers anywhere in the world. The US Department of Defense gives charge to the United States Strategic Command with the duty of combating Cyber Terrorism and this was accomplished through the Joint Task Force Global Network Corporation which is the operational component supporting. In the year 2006 the Secretary of Air Force announced the creation of Air Force's Newest MAJCOM, which is the Air Force Cyber Command and their task was to monitor and defend America from Cyber Terrorism.

CYBER BULLYING –

It is also known as Cyber Harassment and it is considered as a form of bullying with the use of electrical means, It has become increasingly common and is mainly practiced by teenagers. Cyber Bullying is done when someone tease, bully or harass other on social media sites which includes posting rumors, threats, sexual remarks victims personal information or speech containing abusive language against each other. It can take place on social media such as Facebook and Twitter it was stated that 93% of young people between age of 12 to 17 are indulging in such activities as

they spend most of their time on social media. As per 2013 Pew Research study 8 out of 10 teenagers who use social media indulge in such activities and share such information which is not meant to be shared. There are laws that address online harassment of children as well as protect adult cyber stalking victims. Currently there are 45 Cyber Stalking Laws which are enacted while there are some sites which specializes in law that protect victims belong to the age of 18 or under. The global cyber law database aims to become comprehensive and authoritative source of law for all countries, states including Florida, California and Missouri have developed state laws against Cyber Bullying.

EXPLOITATION OF GIRLS AND TRAFFICKING OF CHILDREN-

It was found out that every second one women in India becomes the victim of Cyber Crime and thus the online platform has become a latest platform where a women's dignity, privacy and security is again and again being challenged every moment. Women Exploitation includes trolling, abusing, threatening, abusing, body shaming, revenge porn and other forms through which dignity of women is harmed Everyday. In Cyber Crimes against women the effect is more psychological than Physical while the focus of the loss which are ensuring women safety is focused on more mental harm. It was also found out that National Crime Bureau Of India does not maintain any separate record of the Cyber Crimes happening against women. In Cyber Crimes the technology is used as a main resource by the perpetrators whose aim is to defame women by sending obscene messages and emails. The main reason behind increasing Cyber Crimes against women in India is that the Indian women are not able to report such crimes immediately as they are not aware as to where such crimes are to be reported or sometimes due to the society they have to face.

CYBER HARASSMENT –

Cyber Harassment is the use of Information and Communication Technology with a motive to harass, control, manipulate or habitually disparage any human being without causing him any physical harm. It is different from physical harassment as it does not involve face to face contact. It requires the use of ICT and the person is abused verbally, sexually, emotionally or socially. The main objective of Cyber Harassment is to gain power and control over the targeted victims. When in the case of Cyber Harassment the minor is involved the term is known as Cyber Bullying. When direct or implied physical harm is caused to the targeted victim the Cyber Harassment becomes Cyber Stalking.

LEGAL PROVISIONS ON ONLINE HARASSMENT

As the cases of Online Harassment was increasing day by day Section 354D of Indian Penal Code which was added by criminal law (Amendment) Act 2013 especially mentions the act of stalking as whosoever follows a person and contacts or attempts to contacts such persons with a motive to foster personal interaction repeatedly despite a clear indication of disinterest by such person is committed for the offence of stalking.

Section 354A punishes offence of sexual harassment with 3 years of imprisonment or fine or both.

Section 503 Punishes Criminal Intimidation as threats made to any person causing injury to his reputation or to make victim change course of action regarding anything victim otherwise do or not do. The offence under Section 499 and Section 503 are punishable with imprisonment which may extend to 2 years or fine or both.

CAUSES OF CYBER CRIMES

As we know that Crime is a social phenomenon and various causes behind it is studied by various criminologists and they have given different reasons as Cyber Crimes are done by use technology and the Technology makes the life of Human Beings easy thus everyone is attracted to this technology without having sufficient knowledge so following are the main reasons behind commission of Cyber Crimes:-

•NEGLIGENCE OF NETWORK USERS-

As Negligence is closely related to human acts so it is probable that while protecting the computer system there might be negligence on part of the Owner so thus user which may provide an opportunity to Cyber Criminal for gaining unauthorized and illegal access over the computer.

•NON-AVAILABILITY OR LOSS OF EVIDENCE-

In the cases of Cyber Crime the main issue which comes before the law enforcement and investigating agencies is how to procure or preserve the evidences unlike many other offences it is very difficult to collect sufficient evidence of Cyber Crime which could be used to establish the guilt of the Cyber Accused in front of the Court. Thus, this encourages them to indulge in criminal activities without

•THINKING OF THE SOCIETY-

It is very wrong to say that the thinking of today's generation is changing but they are still thinking like old people and this could be proven with an example that whenever any girl post any picture of her on her profile then some of her followers write abusive comments with an intention to troll

her or make her mentally weak and judging her character on the Picture she posted thus becoming a big cause behind Cyber Crimes.

•UNAUTHORIZED USE OF INTERNET-

As nowadays The Social Media has become a big platform for the teenagers to gain popularity and with the motive of this they do abusive comments and write indecent language on the posts of celebrities and they take it as adventure or fun without having any knowledge of the future consequences of their wrongful acts.

EFFECTS OF CYBER CRIME

1. The Psychological Effects could mainly be seen in teenagers as they try to conduct acts like adults by making abusive comments on someone else profile this affects them mentally
2. Sometimes Cyber Crimes also affect individuals mentally and it results into depression, anxiety, stress and sometimes due to the fear of image in public some individuals commit suicides.
3. As the Wrongdoer could easily escape from small Cyber Crimes this boost their Self Confidence and they commit big Cyber Crimes as they know that they could not be easily identified.
4. Sometimes a particular religion is blamed for a wrongful act happened in the society and by making the social media a platform such religion is humiliated or trolled by posting immoral posters so by act of any individual it is wrong that people of particular religion would be humiliated and this it results they feel that they are discriminated by the society.

CONCLUSION

At the End we would like to conclude it by asking few questions that for what purpose the Social Media is and for what purpose it is being used by the youth? Can't it be used for bringing a positive change in the society, the answer of these questions is hidden in the acts done by youngsters as we have again and again mentioned the use of Social Media is only done for getting popularity or to take revenge by various means. It is very important that today's youth must be made aware regarding the future consequences and this was done not only by various Organizations but also by some Youth Channels such as MTV by introducing serials like MTV WEBBED and Troll Police which could be seen as a perfect example to make youth aware that how their wrongful acts create negative impact on the society as a whole as they showcase the cases in which the Trollers are called upon on the show and made guilty for their wrongful acts as the main aim of the show is to make them realize by making them meet the person they trolled on social media. One of the

main causes or reasons of increasing suicides is also Cyber Crime as it is used as a mean for taking revenge by posting the victim's images or obscene videos and this revenge gives negative impact on victim's sentiments or feeling. It is not always the boys that use social media to harass but sometimes even girls try to harass boys by posting the screenshots on their profile to gain sympathy and for damaging reputation of Boys in front of her friends and the whole society. Now as we earlier mentioned some reasons of cybercrime and the main reason which came is that the accused could easily escape due to lack of evidence and somewhat inefficiency of investigating agencies. Even sometimes if the crime is committed against the women and with the fear to face the society and fear of being embarrassed they do not file suit against the wrongdoer and not filing the cases boost self-confidence of Cyber Criminals to Continue their wrongful acts. So in order to put light on suggestions we would like to say that there should be a special tribunal for handling Cyber Crime cases by keeping the personal information of the victim confidential. And even the Investigation Agencies should recruit more Specialized Experts that could easily deal or locate and find suitable evidences against the person so that a fair trial could be done against the wrongdoer. At the end we can use social media for stopping such crimes by using high level security for maintaining privacy of the person and the account must be fully verified to stop Troller from trolling anyone. As the society could not prevent such crimes but their small steps by creating awareness or giving knowledge to their upcoming generations for the right use of social media could make a big difference and take our society to bright and sage future and to use the social media in the positive manner rather than trolling anyone.

REFERENCES

1. <https://www.yourdictionary.com/cyberpornography>
2. <https://en.wikipedia.org/wiki/Cyberterrorism>
3. <https://www.healthychildren.org/English/family-life/media/Pages/Cyberbullying.aspx>
4. www.legalseriveindia.com/articles/tech_wo.html
5. <https://www.ipredator.co/cyber-harassment/>
6. <http://krazytech.com/technical-papers/cyber-crimes>