VOLUME 1 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CRITICAL ANALYSIS ON CYBERCRIME

- Deep Kathin[1]

ABSTRACT

In today's world, the strongest Cybernetic Medium is known as Social media. We can simply post something on the internet and it becomes easily viral in minutes. We cannot contradict the fact that the internet is one of our elementary requirements. We dependupon the internet for everything and social media is one of the major social networking. Social media is a podium where we can not only like and comment on any post but also share any photo, video and share any information or data using the internet. Cybercrime is a terrible kind of crime having its beginning in the growing dependency on computers in the modern lifecycle. Computers and informatics have certainly carried in extraordinary transformation at all stages. The world, as we observetoday, is not the similar world that it was earlier the arrival of the Internet and afterwardthe World Wide Web. It changed and developed more popularly as a cyber world. This cyber world is bounded by the number of things in which crime is anextremely serious threat. This article is an attempt to deliver a glimpse of cyber-crime in India. India has now been developed into a digital world, on the part where digital functioning has assisted the people to digitalize their working but on the other part, it gave aninnovativeaspect to crime which implements different conducts to commit the crime in the worldwide. Cybercrime is one of the most threatening weapons to attempt crime on the internet. It hinders the person's identity as well as highlights them on the internet which takes the position as the form of defamation. International governments, police departments, and intelligence entities have started to counter. Advantages to control cross border cyber threats are taking effect.This article is an attempt to provide a preview of cybercrime in humanity and how it can be prohibited.

INTRODUCTION

[1] Student at Mumbai University

Defamation means the action of destructing or damaging the respectable reputation of some other individual. In simple words, defamation means defaming anindividual's reputation in oral or written form. Libel is in the written method of defamation and Slander is an oral methodof defamation. Cyber Defamation means an act done purposefully which can be beyondimpertinentor offending anindividual or a group through a virtual medium. Cyber Defamation can be similarly oral and written. Any planned false statement, either printed or verbal, that damages a person's reputation,lessens the respect, esteem, or confidence in which a person is detained; or encouragesdisapproving, intimidating, or unpleasant opinions or thoughts against anindividual is known as defamation.[2] This system of the cyber world operates on websites, internet facilities,and the internet domain. Such a system is coordinated by the internet providers or by the company itself through its computer programmer, including having requirementsor necessities of constraints on certain websites or a certain procedure.[3]

Defamation can also be recognized as the intended infringement of another person's right to his good name. It is the unlawful and intentional publication of arguments or behaviour concerning another individual, which has the outcome of injuring that person's status, moral name, or reputation in society. Libel is a written form of defamation and slander is an oral form of defamation. The fundamental difference is that in libel, damages are recognized, whereas in slander activities unless the slander falls into a certain classification, called slander per se, the plaintiff must verify actual or evidenced damages.[4]Anindividual'smoral name can only be damaged if defaming or criticizing statements are made to somebody other than that individual, by which, the defamatory statement must be revealed to a third individual, thereby significantlyisa requirement of publication. Whileregulating, whether defamation has or has not taken place, the only question to consider is whether anindividual of ordinary intelligence in society would trust that the words would certainly injure the person's reputation.

Hence, the law of defamation places a substantialload on the defendant. Completely, that a plaintiff has to verify, in a defamation argument, the publication of defamatory count. In a cyber world, the right to an undamagedstatus and the right to freedom of expression

[2] Loftus E. Becker, Jr., The Liability of Computer Bulletin Board Operators for Defamation
[3] John D. Faucher, Comment, Let the Chips Fall Where They May: Choice of Law in Computer Bulletin Board Defamation
[4] Clare Dyer, Scientist Wins Out of Court Damages for Internet Libel

isprogressively significant benefits. Safekeeping of reputation is doubtful, even more,significant in anextremely technological society, since one might not even encounter an individual or society other than concluding the standard of the internet.Cyber lawincludescybercrimes, electronic trade, freedom of expression, intellectual property rights, jurisdiction matters and optimal of law, and privacy rights. Cybercrimes comprise events like credit card fraud, unofficially access to computer systems, child pornography, computer software piracy, and cyber nuisance. Freedom of expression comprises defamation, offensiveness issues, and censorship. Jurisdiction mattersemphases on who makes and imposes the rules leadingto cyber space.The description of what institutes a crime in cyberspace is still being established.[5]Previously, the states and central government defined cybercrime actions to comprise the destruction or theft of computer information and programs. More recently the meaning has extended to compriseactions such as forgery, illegal betting, cyber stalking, cyber defamation, etc.There are several areas on the internet where there is anactual risk of responsibility for defamation. The fact that anoperator is unaccompanied with his computer and separated from other operators creates anintellect of understanding. There is no verbal or telephonic conversation or verbalizedcommunication that would generallyinculcate some attention. In addition, the concept that the internet is brawl cyberspace where there are no restrictions or boundaries consequences in anoperator'sintellect of social norms and modesty generally distorted.[6]

The Web network outcomes in an immediate international publication of information at a very low price. Information, which would not generally have been openpreceding the origin of the internet, can now be extracted by practically everyone. Intranets are envisioned to be entirely used by a company. Though, information from an intranet can be straightforwardly downloaded and forwarded by electronic mail or otherwise to tertiary parties. Information forwarded to a statement or bulletin board can be retrieved by anyone. This means that anybody can place derogatoryaccusations on the statement or the bulletin board. Electronic-mail operators generally manage to pleasure their communication as a kind of conversation or discussionslightly than written communication. Operators forget that electronicmails are collected and can be recovered as hard copies and that their matters cannot be uncertain.[7]A

[5]Resnick, supra note 20
[6] Ethan Katsh, Law in a Digital World: Computer Networks and Cyberspace
[7] Verity & Hof, supra note 6

single message can be spread to accurately hundreds of individuals. As a derogatoryaccusation needs only to be released to a single person for publication to be verified, every time electronicmail is forwarded to another person, it is published again and a supplementary source of action for offense arises.The scope of every law firm having a cyber-occurrence to restrain defamation is universal. Internet sites can be retrieved in most nations throughout the world; vast amounts of data can be communicated simultaneously to numerous different destinations,and electronicmail can be forwarded to an unlimited number of recipients without the original author having any direction over the communication.[8]

REASONS FOR CYBERCRIME

The Perception of Law has said that human beings are helpless so rule of law is required to defend them. Concerning this to the Internet, we may say that computers are helpless, so rule of law is mandatory to protect and safeguard them against cybercrime. The reasons for the helplessness of computers may be said to be:

1. Room to store information in reasonably small space: The computer has an exceptional characteristic of storing information in anexceptionally small space. This allows to remove or acquire information either through substantial or virtual medium makes it much comfortable.
2. Comfortable to access: The problem confronted in safeguarding a computer system from unlawful access is that there is every opportunity of violation, not due to human error but due to the complicated technology. By cautiouslyrootedjudgementfail, crucial loggers that can steal access codes, innovative voice stereos; retina imagers, etc. that can dupe biometric systems and sidestep firewalls can be applied to get manyprior security systems.
3. Complicated: The computers work on functional systems and these functioning systems in turn are comprised of millions of codes. The human mind is imperfect and there might be aninterval at any point. The cyber offenders take benefit of these omissions and infiltrate into the computer system.
4. Negligence: Negligence is very thoroughlyassociated with human manner. It is therefore very possible that while safeguarding the computer system there might be any negligence,

[8] Henry H. Perritt, Jr., President Clinton's National Information Infrastructure Initiative

which in turn specifies a cyber offender to gain admittance and control over the computer system.[9]

5. Shortage of evidence: Shortage of evidence is a very mutual&understandable problem as all the informationishabitually destroyed. A further collection of information outside the regional extent also incapacitates this system of crime investigation.

Cyber offenders are organized into various groups and categories. This partition may be warrantedbased on the entity that they have in their attention. The following are the classification of cyber offenders-

1. Children and youngsters between the age group of 6 to18 years: The modest reason for this type of offending behaviour pattern in children and youngstersare seen frequently due to the curiosity to know and discover the happenings. Another similar reason may be to demonstrate themselves to be unresolvedamong other children in their group. Further, the reasons may be even emotional. For example, the Bal Bharati case in Delhi was the consequence of harassment of wrong done by his friends.
2. Organized hackers: These categories of hackers are habitually organized together to achievea certain objective. The reason may be to accomplish their political partiality, fundamentalism, etc. The hackers from Pakistan are supposed to be some of the finestsuperiority hackers in the world. They mostly target the websites of Indian governments with the persistence to accomplish their political objectives. Further, the National Aeronautics and Space Administration (NASA) as well as the Microsoft and many more internationally verifiedwebsites are always under attack by hackers.
3. Professional hackers and crackers: Their work is organized by the influence of money. These types of hackers are mostly employed to hack the website of competitors or rivals and get reliable, consistent, and valuable information. Further, they are partiality employed to crack the system of the company basically as a measure to make it safer by sensing the ambiguities. [10]
4. Dissatisfied employees: This group comprises those individuals who have been either dismissedor sacked by their company or are disappointed with their employer. To retaliate, they usually hack the system of their employee.

[9]Grayson Kemper,SEO and emerging technologies researcher
[10] By Akhilsharma870, geeks for geeks

METHODS AND MEANS OF COMMITTING CYBERCRIME

Illegal access to computer systems or networks / Hacking: This variety of offence is generallymentioned as hacking in the general sense. Though, the framers of the Information Technology Act, 2000 have notmentioned this term, so to evade any confusion that we would not correspondently use the word hacking for 'unofficial access' as the latter has an extensiveimplication.[11]

1. Theft of information enclosed in electronic form: This contains information stored in computer hard disks or disk drives, removable storage, media, etc. Theft may be either by seizing the information physically or by interferingor tampering with it through the virtual medium.
2. Information exploiting: This kind of occurrence involves varying rare information just before a computer processes it and then shifting it back after the processing is finished. The energy board faced the comparable problem of information exploiting, while the department of the company was being computerized.
3. Email intimidation: This kind of pursuit refers to sending huge numbers of emails to the target or receiver, which may be an individual or a company, or even mail attendants thereby eventually resulting in intimidation.
4. Salami attacks: This type of crime is usually predominant in financial organizations or institutes to commit financial crimes. A significant feature of this kind of offence is that the modification is so small that it would generally go unobserved. For example- the Ziegler case, where a logic bomb was initiated in the bank's system, which abstracted ten pennies from every account and deposited it in a precise account.[12]
5. Informationexploiting: This kind of occurrence involves varyingrareinformation just before a computer processes it and then shifting it back after the processing is finished. The energy board faced a comparable problem of informationexploiting, while the department of the company was being computerized. [13]
6. Disowning of Service attack: The computer of the sufferer is flooded with additional requests than it can manage what was the cause to crash. CirculatedDenial of Service

[11]Hacking articles, Raj Chandel's blog
[12] Ajay Maurya, how to identify the Salami attack?
[13] Kunsoo Han, Robert Kauffman, Journal of Management information systems

attack is also a type of denial of services attack, in which the offenders are varied in number and prevalent. For example- Amazon, Yahoo.

7. Logic bombs: These are happening conditional programs. This indicates that these programs are formed to do something only when a confident event also known as a prompt event arises. For example- even some viruses may be named logic bombs because they lay inactive all through the year and become vigorous only on a specific date just like the Chernobyl virus.[14]
8. Virus or worm attacks: Viruses are programs that affix themselves to a computer or a file and then socialize themselves to add files and to other computers on a network. They frequently affect the information on a computer, either by changing or deleting it. Worms, dissimilar to viruses, do not need the host to assign themselves to. They simply make efficient copies of themselves and do this frequently till they plague up all the available and remaining space on a computer's memory. For example-the "ILOVEYOU" virus, which affected at least 5 % of the computers of the world. The sufferers were accounted to be 10 million dollars. The world's most eminent worm was the Internet worm which was let loose on the Internet by Robert Morris in 1988. Almost gave expansion of the Internet to a broad halt.[15]
9. Web jacking: This term is consequent from the term hi-jacking. In these types of crimes, the hacker advances access and control over the website of another. He may even harm or modify the information on the site. This may be done for satisfying political purposes or for extracting money. For example- recently the site of MIT (Ministry of Information Technology) was hacked by international hackers doubtful from Pakistan and some offensive matter was committed therein. Additionally, the website of the Bombay crime branch was also web jacked. An alternative case of web jacking is that of the 'gold fish' case. In this case, the website was hacked and the information relating to goldfish was altered. Further,the payment of US million dollars was demanded as ransom. Thus, web jacking is a procedure whereby power over the website of another is made supported by some consideration for it.
10. Trojan attacks: This term has its derivation in the word 'Trojan horse'. In software subject, this means an unofficial program, which inactively gains control over another's

[14] http://www.techopedia.com/definition/4010/logi c-bomb
[15]D. Nicol, M. Liljenstam, J. Liu, Multiscale modeling and simulation of worm effects on the internet routing infrastructure.

system by representing itself as an official programme. The most mutual form of connecting a Trojan is through electronicmail. For example- a Trojan was connectedto the computer of a female film director in the United States while conversation. The cyber offender through the web camera installed in the computer obtained her naked photographs. He additionally harassed this lady for a long time.[16]

11. Internet time thefts: Usually in these types of thefts, the Internet browsing hours of the sufferer are used up by another individual. This is done by gaining an approach to the login ID and the password. For example- in the Colonel Bajwa case- the Internet hours were used up by any other individual. This was possibly due to one of the first testified cases connected to cybercrime in India. Though, this case made the police notorious as to their lack of perceptive to the nature of cyber-crimes.

CATEGORIES OF CYBERCRIME

The function of computers in cybercrime can be categorized in a restricted or extensive sense, where the computer can be used as a purpose, a tool, or computer as the situation or framework. The cybercrimes can be generally classified as follows:

1. Cybercrime contrary to individuals: In such cybercrimes, individual people are affected. The main objective is to misuse manipulate human weakness like greediness and innocence. The potential damage of such a crime to humankind is harsh. A few of the generalcybercrimes against individualscomprise ofporn especially childpornography, desecration of privacy, the annoyance of a person through electronic-mail tricking, hacking, cracking, cyber nuisance, defamation, cheating, fraud, electronic-mail hoaxing, password sobbing, credit card rackets, gambling, etc.
2. Cybercrime contrary to property: The second type of cybercrimes is against the property. Intellectual Property Crimes, cyber bending, cyber impairment on the property, broadcast of malware that dislocatepurposes of the system or clean out information or create non-functional of the involved devices, cyber intruding, Internet time thefts are insufficient of the most generalcybercrimes against the property.
3. Cybercrime contrary to government/organizations/society: One of the different cybercrimes contrary to government and connected organizations is cyber intimidation.

[16]Alkabani Y, Koushanfar F (2009) Consistency-based characterization for hardware Trojan detection.

The individuals and groups use electronic media and the Internet to hoverover the international governments and the inhabitants of the country. This crime establishes itself into terrorism when an administration or military websites are hacked and vigorous information is regained. Cybercrime against society and humanity mainly includes unofficial access toa computer, password sobbing, disowning of service attacks, malware attacks, crimes originating from non-centralized computer network groups, industrial snooping, or spying, network interruptions, counterfeiting, web-jacking, etc.

Though a legal conflict based on defamation is frequentlyexpected at ending defamatory accusations, the damage in most cases has previously been done. Therefore, the most significant relief declared in a defamatory action is damages. The number of damages approved will be contingent on the nature of the defamation required and the extent of publication. Additionally, a defamation accusation can be instituted in any dominion in which anorigin of action arises.Every time a tertiary party accesses a defamatory posting on the Internet, the publication is already done.[17]

Freedom of Speech and Expression, as delivered by the Constitution under Article 19 (1) (a), provides that all inhabitants shall have the right to freedom of speech and expression. Though, such freedom is studied to a rational restraint. The protection of the reputation of another individual falls inside the domain of rational restraint and any observation or remark which hinders the reputation of another individual, except the statement is true, would summon responsibility under the law of defamation.

WHERE AND WHEN TO FILE A COMPLAINT?

Any individualdistressed of cyber defamation can file a grievance to the National Cyber Crime Reporting Portal. Nevertheless, it is appropriate to note that filing a cyber-defamationgrievancecontrary to anindividual is one of the most significantdecisions, subsequently, the act of filing a complaint also brings the reputation of the offender in the line of ignition. Additionally, the responsibility of proving that the offender has been defamed deceitscompletely with the complainant and if he or she is incapable to do so, the offender shall have the right to litigate for defamation, false and inconsequential complain, and damages thereto.

[17]David Wall, "Cybercrimes and Internet", Crime and the Internet

CONCLUSION

Information Technologies not only assist individuals, organizations, and governments; but also expands the possibility of criminal activities. Currently, the credit card robberies and online money-laundering cases of cyber crimes are on the upsurge. Agitation and defamation done through social media are also a matter of apprehension to individuals. Cyber intimidation is the most conspicuous characteristic of cybercrime across nations. It is the absence of cybercrime knowledge that leads to cybercrimes. There are a lot of benefits and drawbacksto social media. It is just in what way we choose to operate it and we have to be equipped for the denials as well. Social media is now a mode of the lifecycle, where we can freely write, comment, and post everything. In circumstance, schools must also start spreading cognizance among children before they get grabbed into the world of social media and parents should advise their children about the advantages and disadvantages of using social media. It is also necessary to re-examine the existing legislative provisions to certify that the network atmosphere is sufficiently protected contrary to criminal activities.

VOLUME 1 | ISSUE 3 APRIL 2021 ISSN: 2582-7340

For general queries or to submit your research for publication, kindly email us at editorial@ijalr.in

https://www.ijalr.in/