Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
July to September 2025, E-Journal, Vol. I, Issue LI (51), ISO 9001:2015 - E2024049304 (QMS)

Impact of Cyber Crime

Sandeep Kumar Dixit*

***Research Scholar (Legal Studies & Research) Barkatullah University, Bhopal (M.P.) INDIA**

Abstract-Cyber crimes cause more harm to society than traditional crimes. In Present time crime in computer generated super high way is a new Phenomenon in contemporary social scenario. Under cyber crime hacking, spamming, cyber theft, cyber fraud, cyber-terrorism, unauthorized access to computer and computer system etc are to be recognized as more grievous than any ordinary crimes world-wide.
Keywords- Cyber theft, Cyber fraud, Internet Criminals, Computer Networks, Computer Stalking, Cyber Space, Computer Trespassing.

Introduction: Traditional crimes hacking crimes as hacking. We have to undertake intensive study to find out how to prevent and control cyber hacking. Hackers usually represent themselves information; their activities are within legal boundaries; they are not always law breakers sometimes protectors when they act as ethical hackers. Most of the times they believe that victims are hardly interested in loading complaint against them and most of times victims are unable to identify their activities due to unspecified and undefined jurisdiction in cyber world. When hacker view on webpage and by deep linking get very confidential information without the consent of the person who holds it and download it with dishonest intention; it is a complete case of theft. Section 378 of the Indian Penal Code provides that when any person with the intention dishonestly transfers any movable properly from one place to another place method the consent of the possessor them it is called theft.

What is Cyber Crime: The Person who get wrongful ownership of computer or stop other computer to working or disturb to work computer or harmful to the software or collected materials of other person this process is called Man Computer Crimes. This is called cyber crime to cheating the other person or harmful to other computer inject virus or disturb the computer network is called cyber crime.

Jurisdiction: Under section 1(2) of the Information Technology Act applies all over India including the State of Jammu & Kashmir. It also applies to any offence or contravention committed by any person outside the territory of India.

The Main object of section 75 which apply for offences and contravention committed outside India are:-

1. The provisions of the Information Technology Act, 2000 also apply to any offence or contravention committed outside India irrespective of the fact whether the accused is a national of India or not.
2. The act will apply only if the act or conduct constituting the offence or contravention involves computer, computer system or computer network located in India.

The Act gives territorial as well as extra territorial jurisdiction to the law enforcement agencies. This the Act also applies to any offence or contravention committed outside India by any person irrespective to his nationality. If the act or conduct constituting the offence or contravention involves computer, Computer system or Computer Network located in India.

Under Civil Procedure Code, 1968 the plaintiff may sue the defendant at a place where the defendant actually or voluntarily resides or carries on business or personally works for gain (at the time of commencement of suit) or at place where the cause of action, wholly or in part has arisen this traditional concept of jurisdiction, however, cannot be applied to the cyber space.[1]

Liability: The following are essentials to make a person criminally liable under section 71 of I.T. Act,

1. The person should have made any misrepresent to or suppressed any material fact from the controller or the certifying authority.
2. Such misrepresentation or suppression of material fact shall be in connection with obtaining of any license or digital signature certificate.

Starting of incorrect and false fact can be called as misrepresentation where as non disclosure of required fact can be termed as suppression.

This section 73 to make a person's criminally liable are:-

1. A person should have published or otherwise would have made available digital signature certificate to any

other person.

2. He should have published or would have made it available to any person with the prior knowledge of the fact that the certifying authority listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

An exception, however, has been restored to this i.e. if the publication of digital signature certificate is for the purpose of verifying a digital signature created prior to such suspension or revocation, them it does not constitute an offence under the act.

The following amounts to an offence under section 74 for publication for fraudulent purpose:-

1. Creation, publication or otherwise making available a digital signature certificate.
2. Such creation, publication etc. Shall be for any fraudulent or unlawful purpose.
3. The person creating publishing or making available digital signature certificate shall do so knowingly :-

This knowingly creating, publishing or making available a digital signature certificate for any fraudulent or unlawful purpose is an offence under section 74 punishable with imprisonment up two years or find up to one lakh rupees or both.

Impact of Cyber Crime : Cyber crimes include hacking into a computer network, creation of viruses and forcibly taking over a Computer Network main crimes like fraud, sabotage, pornography, copyrights piracy etc, have been redefined to include the aspects of internet.

Cyber crimes can be basically divided into 3 major categories being cyber crimes against persons, property and government.

1. Cyber crimes against Person: The first category cyber crimes committed against person include various crimes such as harassing any one with the use of a computer that could be via e-mail, cyber stalking and transmission of child-pornography. One of the most important cyber crimes known today includes dissemination of absence material including pornography, trafficking, distribution, posting and indecent exposure, and child pornography.

Cyber harassment is distinct upper crime various kinds of harassment can and does occur is cyber space or through the use of cyber space. Another cyber crime against person is that of cyber stalking. The interest is a wonderful place to work, play and no less than a mirror of the real world and that means it also contain electronic versions of real life problems, stalking and harassments are problems that many also occur on the internet, in that has become known as “Cyber Stalking” or “On line harassment”

2. Cyber crimes against property : The second category of Cyber Crimes is that of Cyber Crimes against all forms of property. These crimes include unauthorized Computer Trespassing through cyber space, Computer Vandalism, transmission of harmful programs and unauthorized possession of Computerized information it is a dreadful felling to know that some one has broken into your Computer System without your knowledge and consent and has tempered with precious confidential date and information. Coupled with this the actuality is that no computer system in the world is hacking proof. It is unanimously agreed that any and every system is the world can be hacked.

3. Cyber crimes against Government : The third category of Cyber Crimes related to Cyber Crimes against government cyber terrorist is one distinct kind of crime in this category. The growth of internet has shown that the medium of cyber space is being used by individuals and groups to threaten the international governments and also to terrorize the citizens of the country. This crime manifests itself in to terrorism when an individual ‘cracks’ into a government or military maintained website.

The Indian Courts realizing the importances of domain names have responded strongly against cyber squatting and legal principles have been formulates in regard there to probably the first Indian case yahoo.

Inc Vs. Akash Arora [2] where in the defendants were restrained from dealing in service or goods on the internet of otherwise under the domain name “yahoo India.com” as being deceptively similar to the plaintiffs trademark “Yahoo” it was said that through yahoo is a dictionary word, get it has acquired uniqueness and distinctiveness and are associated with the business of the concerned company and such words have come to receive maximum degree of protection by courts.

Another case legal protection of domain names came 2004 is Satyam Infosys Ltd Vs Sifynet Solution Pvt. Ltd[3] In this case the Supreme Court approved that the domain names are entitled to legal protections equal to that of a trade marks. The Supreme Court further observed as under. The Delhi High Court in Acqua Minerals Limited Vs Pramod Borse[4] observed that “If any person get the domain name registered with the registering authority which happens to be tade name of some other person. The registering authority has no mechanism to inquire into it do decide whether the domain name sought to be registered in it is prior existence and belongs to another person’s”

It is the data and not the Computer person that is the target of Cyber Crimes. Theft of a Computer printout may be construed as Cyber Crimes. The planting of Computer Virus causes destruction of date, not the compute itself. Thus the Computer system is the means, not the end. New approaches should be forged to battle growing Cyber Crimes but no solution is being formed to the problem. The world-wide date network jump over all borders and so internet criminals do not stop at our national boundaries.

Cyber experts say hackers are constantly attacking both government and private sector Computer System, sometimes with specific aim to cannot crimes, but often as a sort of intellectual test. Software that enables hackers to

break into private networks is widely available over the internet itself.

Conclusion: While concluding the above discussion it may be said the Cyber Crime in burning topic in whole world. Various countries have made laws to prevent Cyber Crimes. Country system can also be used to sort out claims of cyber squatting but Jurisdiction is often a problem as different court have ruled that the proper location for a trial is that of the plaintiff the defendant or the location of the server through which the name is registered some countries have legislated specific laws against cyber squatting beyond the normal rules of trade marks law. Awareness regarding cyber crimes and cyber laws must also be created among general masses private and non-governmental organizations can play a predominant role in these issues.

The cyber criminal should not be shown any leniency with regard to punishment, for, they are not the victims of gross injustice done by social structure of the society, but are sophisticated and educated members of the real wired. Lastly, the laws relating to cyber crime in our country must be on consonance with the international standards so as to combat with faceless nameless criminals in the virtual world.

References:-

1. Section 20 of the Coe of Civil Procedure, 1908
2. 1999 PTC (19)201
3. (2004) 6 SCC 145
4. 2001 PTC 619

****