IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER CRIME AND PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

Pranjali Saxena

LLM Student

Amity University, Noida, India

ABSTRACT

Cyber crime has grown with the internet as an apparatus to unlawful ends like frauding, trafficking in child predator and belonging, burglary or violating privacy. Internet is became the habit of everyone in today's life. Internet has everything that you want in day to day life. Computer has very much become the central to commerce, entertainment and government. First Worldwide adoption of computers is United States and early most of victims and offenders of cybercrime were Americans. The foremost of the cyber crime is associate in nursing attack on information concerning people, companies and government. Cyber crime ranges from a broad spectrum of activities. At one aspect crime that involve basic breaches of private or company privacy . Another side are crime that involves individual with corporations or government bureaucracies for profit or political objectives. Cybercrime also ranges from spam, hacking and threats against specific sites to act of cyber terrorism. To prevent from all type of cyber crime the branch name cyber security is made to protect all the network and system from the cyber attack. India does not have a separate dedicated cyber law, it comes under the criminal law of India. In a Democratic country like India everybody has their right to freedom in some way all the citizens has the correct to web or liberty to attach. Right to internet is directly associated with the Human Rights. International human rights makes balance between the crime management and respect for rights of human. The expanding realm of cybercrimes involves offences like cyberstalking, fraud,cyberbullying, phishing or spamming but also extends to the violation of intellectual property rights (IPR). These infringements involve online theft of copyright material, trademarks, trade secrets , audios, videos and service marks through illicit methods such as hyperlinking, framing, meta-tagging.

KEYWORDS : *Trafficking, Company privacy, Cyber Terrorism, Hacking, Human Rights, Intellectual Property Rights*

INTRODUCTION

Cyber crime referred to as PC crime, in which computer act as an instrument for any prohibited ends, like committing theft , deal with child predator and property, stealing identities or violating privacy.

Cyber crime started with the hacking within which hackers attempt to hack into computer networks in 1970. The some hackers did it in thrill of accessing high level security networks and some did to gain sensitive classified material subsequently the criminals started to infect computer system with computer viruses and which led to collapse of personal and business computers.

table no. 1. the dateline of cyber crime from 1800 to 2013 [1]

1834	French Telegraph System	A combine of thieves hack the French Telegraph system and steal monetary market information, effectively conducting the world's initial cyber attack.
1870	Switchboard hack	A teenager employed as a manipulator is ready to disconnect and direct calls and use the road for private usage.
1878	Early Telephone Calls	Two years when Alexander Grahmen Bell invents the phone, the bell telephone service kicks a bunch of adolescent boys of the phone system in New York repeatedly and intentionally misdirecting and disconnecting client calls.
1940	First Ethical Hacker	Rene Carmille a member of the Resistance in Nazi captured the France and a using the punch card information, finds out that the Nazis are using punch card machines to process and track down the information against jews.
1955	Phone Hacker	David Condon Whistles his"Davy Crockett cat''and"Canary bird flute' into his phone, Testing a theory on how communication system works. The system acknowledge the key code, assumes he's an worker and connect thus a protracted distance operator. She connects him to any number request without charge.
1969	Rabbit Virus	An anonymous person in installs a program on a laptop at the University of Washington computer center. The invisible program a makes copy of itself breeding sort of a rabbit until the pc overloads and stops operating. It is find to know first computer virus.
1984	US Secret Service	The North American nation comprehensive Crime Management Act provide US Secret Service jurisdictions over computer fraud.
1999	The Melissa Virus	A virus infects Microsoft Word mechanically distributive itself as an attachment via email. It mails resolute the primary 50 names listed in an infected computers outlook email address box. The creator David Smith says he didn't intend for the virus that value $ 80 million in damages to damage, computers can stop. he is arrested and sentence to twenty months in prison.
2005	Phone Buster	Phone Buster reports 11K+ identity theft complaints in Canada and total losses of $8.5M making this the fastest growing form of consumer fraud in North America.
2011	Sony Pictures	A hack of sony's knowledge storage exposes the records of over 100 million customers utilizing their Playstations online services. Hackers will gain access to all Or any mastercards information of users. The breach prices Sony over than $171 million.
2013 – 2015	Global Bank Hack	A group of Russian primarily based hackers gains access to secure data from over 100 establishments around the world. The hackers use the malware to infiltrate banks computer systems and gather personal knowledge stealing euro650 million from world banks.
2015	Locker Pin	Locker pin resets the pin code on Android Phones and demands $500 from victims to unlock the device.

Source: www.herjavegroup.com

[1] Robert Herjavec (cybersecurityceo.com)uuuh

In the digital age, the protection of Intellectual Property (IPR0 has become increasingly crucial as cybercriminals exploit online platforms for illegal activities. Intellectual Property Rights refer to legal rights that protect creations of the mind or intellect, providing exclusive rights to creators or owners for a certain period. These rights include patents, copyrights, trademarks, trade secrets and industrial designs. It aim to encourage innovation and creativity by granting creators control over their inventions, artistic works, brands., and confidential information allowing them to benefit financially and maintain a competitive advantage in the marketplace.

BACKGROUND OF THE PAPER

The background of the paper is about how knowledge of cybercrime is important in India. All the information adhere here is collected through different books, articles and law websites. The central topic of research paper is how cybercrime started in India , in what extent it is spread around the country and how cybersecurity and IT ACT 2000 has been introduced to stop the crimes. All the information in the paper is relevant and upto the mark as all the information is searched from the trusted source. This paper will contribute to the public policy because in this internet world where all activities and transcations go through network, people have to aware of all the crimes. If they know about all laws they will be free from frauds.

RESEARCH METHODOLOGY

The topic of this research is such that which requires a lot of reading and collecting data which includes both qualitative and quantitative knowledge. Qualitative data includes the analysis based on language, images and observations. In this research we have studied the different articles and news on the cybercrime and observed that how investigation happens.Quantitative data includes the analysis based on numbers. We have also mentioned the timeline on the history of the cybercrime which comes under the quantative data.

ANALYSIS

CYBERCRIME AND CYBERSECURITY

All new and upcoming technologies create the new criminal oppurtunities. Cyber crime is different from the old criminal activity and one difference is the use of digital computer. But technology alone is insuff[i]icient to commit any crime. As criminals do not need any kind of technology or a computer to commit fraud, traffic in child predator and holding property, violate someone's privacy. All these activities existed also before **cyber** prefix become ubiquitous. Crime especially involving the internet, represents an criminal behavior alongside some novel banned activities.[2] Most of the crime attacks is on individual firms or government. These attacks do not take on surface of physical bodies however do take place on personal or company virtual body, that is set of informational attributes that outline individuals on the web. In different words in this digital age our virtual identities are essential parts of everyday, all the information is bunded in multiple computer databases closely held by Government or Firms. This could be clear from the recent CAA in that government has all the list of the citizens or the non citizens during which government has prepare the list of Muslims citizens in Assam which don't have the documents to prove their citizenship national wide. [3]

The main facet of cyber crime is that it's non native character: actions will occur in jurisdiction separated by large distances. Investigation are usually not very easy as comparatively the police investigate are, they are more international and global. What is Cyber space? It is a richer version of space where telephone conversations take place at a large scale. Telephone conversations means the connections all over the world because of Internet. Cyber security is practice of defending computers, servers, mobile devices, electronic system, networks and data from malicious attacks. Cyber security is a vital for safeguarding all the sensitive information, in personal Diagnosable data(PII), protected health and personal data.These are common types of cyber security:

1.Network security : it protects network from dominant incoming and outgoing activities to forestall threats from getting into and spreading on network

2.Data Loss Prevention (DLP) : protects information by classification and observing of data.

[2] Cyber crime – BRITANNICA

[3] Citizenship Amendment Act 2019

3.Antivirus/ anti-malware: it scans computer from the threats. Even the current solutions are able to discover the threats from its behavior.

CYBER SECURITY: LAWS AND POLICIES

Cyber law is that part of the system that deals with the all cyber problems, web and cyber space. Freedom of expression, access to web and online privacy are subtopics of cyber law. In easy words cyber law is directed to the law of the Internet.

Any activities of the citizens which are associated to cyberspace come within the jurisdiction of cyber law. Cyber law consists of statutory and constitutional provision which affect the computers and networks.

On 17 October 2000 the IT act came into the force that are applicable to whole of India and its provisions additionally apply to any offense and resistance committed outside the territorial jurisdiction of Republic Of India , by any person regardless of his nationality. The provisions of this act say that any offence or contravention ought to involve a system or network located in India. Some of the highlights of act are listed below:[4]

Chapter II: of the act specifies that any subscriber will correct their electronic record by affixing his digital signature.

Chapter IV: of the act gives a option for regulation of certifying authorities. The act gives a controller of certifying authorities who perform the duty to look over the activities of certifying authorities and also set the limits and conditions governing the certifying authorities and it also specify the forms of Digital Signature Certificates.

Chapter VII: of the act tells regarding the theme of things about to Digital Signature Certificates.

Chapter IX: of the act tells regarding the penalties for numerous offences. The penalties for injury to computer or computer systems are mounted not exceeding of Rs 10000000 to affected persons.

Chapter X: of the act regarding the institution to cyber rules appellate tribunal, where individuals can appeals on the order given by the officers.

Chapter XI: of the act tellsa bout the offences that are investigated by a Police Officer not below the rank of Deputy Superintendent of police. These offences consists of hacking which is obscene in electronic type, tampering with computer source documents, publication of data.

TYPES OF INTERNET/ CYBER CRIME

This is the time where all digital devices including computers and smartphones are interconnected to the web.

Hacking : Hacking is an associate degree act that is committed by trespasser or intruder who access other persons computer without their knowledge. Hackers are the computer programmers who are expert in the knowledge of PC and they misuse their knowledge. They have expert level skills in a particular software or language. Hackers sometime in greed break the systems to steal the personal banking information or financial data. And on one side some develop interest in computer hacking out of intellectual curiosity. Many companies hire these hackers to find the flaws in the security system and fix it .[5]

Phishing : Confidential informations can be withdrawn by using the phishing scam by making the email look bona fide, with a forged sender address. Tapping it can be wrong move as malware get installed.

Cyber Stalking : Cyber Stalking is the new way of crime nowadays in which person is followed online. A cyber stalker does not follow person physically but he does by following online activity to get the information or harass them or make threats. This is the way to invade ones online privacy. Cyber stalkers harass their victims via email ,chatrooms or blogs. It has now spread to all social media platforms such as facebook, twitter, flickr and youtube, your profile, photos and status updates are up for the world to see. The cyber stalking crimes happens mostly with the women.

Identity Theft : Identity Theft is once somebody steals your identity and acts to be you to access your resources like credit cards, bank accounts and take advantages in your name. Mastercard fraud is the most simplest form of fraud during which criminal uses your credit card to fund his transcations.

[4] The Information Act 2000

[5] Farukhan chand Shaikh vs State by Cyber Crime Police on 8 Janurary,2013

RIGHT TO NET AND FUNDAMENTAL RIGHTS

Fundamental Rights are the rights which are given to the citizens of India. This is the basic rights which all citizens practice and if anyone violate the others right there are many laws against them. Similarly the right to net is the major topic whether it is fundamental right or not? The apex Supreme Court of India declared access to internet is a fundamental right. The Supreme Court has extended Article 19 (The Right to freedom and Expression) in many occasions. This ruling is in connection with the United Nations directions that every country should make use Internet a Fundamental Right.[6]

This law came after hearing a plea in connection with internet usage of Jammu and Kashmir since August 5 when Article 370 revoke in Indian Union Territory. Internet is the primary source of information which is spread to millions to Indian Citizens. Right to speech and expression comes under Article 19(1)(a) and this time it expanded with the innovation of technology. KERALA is the first state in 2007 to declare access to internet – a basic human right.

From a recent case, the right to internet use was known as a fundamental right which form part of the right to privacy and the right to education under article 21 of the constitution.[7] As now the internet has became the important part of life it is necessary to be the fundamental right as it is written in the constitution and no one is deprived of it.

RIGHT TO PRIVACY AND RIGHT TO INTERNET

Right to privacy is the right given to all the citizens in which no one shall be interfere with his privacy, family, home or non one can harm the reputation.[8]The Kerala High Court held that the right to net is part of the fundamental right as well as right to privacy under article 21. Article 21 states the right to life and personal liberty. Internet helps by facilitating of all kind of primary necessities in terms of social benefits. Internet can also achieve the target of Sustainable Development Goal. These involve poverty, hunger, education, maternal care and link between government and service. Internet helps in the education system as we can see that the in this huge pandemic covid 19, online classes are taking place in all the institutions and education is in continuous process.

LEGISLAGTIONS ENACTED TO PROTECT IPR

In 1999, the government enacted significant legislation inspired by global standards to protect intellectual property rights. These measures include:

- The introduction of the Patents (Amendment) Act,1999, which facilitated the establishment of the mailbox system for patent fillings and granted exclusive marketing rights for a duration of five years.
- The enactment of the Trademarks Bill 1999.
- Amendments to the Copyright Act through the Copyright (Amendment) Act, 1999.
- The introduction of the Geographical Indications of Goods (Registration and Protection) Bill, 1999
- The replacement of the Designs Act,1911, with the Industrial Designs Bill,1999
- Further amendments to the Patents Act of 1970 were proposed through the Patents (Second Amendment) Bill,1999 to ensure compliance with the TRIPD Agreement.

INDIAN LAWS ON IPR

Section 51 of the Copyright Act, 1957, unequivocally states that the exclusive rights are vested in the copyright owner and any contrary action constitutes copyright infringement. However, the absence of explicit legislation to determine the liability of Internet service providers (ISPs) leaves room for interpretation. Section 51 could be construed to encompass the provision of service facilities by ISPs for storing user data at their business premises, which is then monetized through service charges and advertisements. Nevertheless for such interpretation to hold, certain conditions must be met cumulatively including the criteria of ‘knowledge’ and ‘new diligence’ to establish ISPs liability for abetting copyright infringement.

The Information technology (Intermediaries Guidelines) Rules 2021, along with section 79 of the IT Act 2000 offer conditional protection against liability for online intermediaries. However, these provisions remain subject to interpretation under other civil or criminal acts. Section 79 of the IT Act, 2000 shields intermediaries

[6] News Channel – India Today Network

[7] Faheema Shirin v. State of Kerala

[8] Right to privacy

from liability from third party content hosted on their platforms. The 2021 guidelines emphasises the adoption of diligent approach by intermediaries to qualify for production or exemption under section 79 of the IT Act 2000. Consequently, judicial interpretation becomed paramount, tailored to the specific circumstances of each case.

INTERNATIONAL CYBER CRIME

Cyber crime were first taken place in the US because the US is the first company to adopt the computers which spread the crime faster. In 1996 the Council Of Europe with other government representatives country from the United States, Canada and Japan drafted a international treaty for computer crimes. In the world, civil libertarian groups protested against provisions in the treaty requiring internet service providers to store information on their customers transcations. On November 23 2001, 30 counties signed European convention on cybercrime and came into effect in 2004. Another national laws such as USA PATRIOT ACT of 2001 have enforcement power to monitor and protect computer networks.

INTERNATIONAL LAWS FOR PROTECTION OF IP IN CYBER WORLD

The array of international conventions, treaties and agreements aimed at safeguarding intellectual property in the digital realm including the following:

The Berne Convention (1886) safeguards intellectual property rights pertaining to literary and artistic works with specialised provision catering to developing and countries

The Rome convention (1961) addresses creative works of authors and the owners of tangible indicators of intellectual property. It allows for implementation at the domestic level by member countries with disputes falling under the jurisdiction of the international Court of Justice unless resolved through arbitration.

The TRIPS Agreement (1994) is a multilateral agreement on Intellectual property with broad broad coverage, encomposing copyright and related rights.

The Uniform Domain Name Dispute Resolution Policy (UDRP) (1999) facilitates the resolution of disputes concerning the registration and usage of Internet domain names.

CONCLUSION

Change is the law of nature. With evolution many new technologies invented as computer came first then the internet .The internet is now became the most important part of everybody life. And if any new technology or any resource come, it come with both advantages and drawbacks. The one of the drawback of computer and internet is cyber crime. With other more crimes such as murder or rape , cyber crime is also emerge as a threat to the country, to the world and most importantly to the citizens of the entire world. Some or the other many people face cyberbully. Not only common people but the very successful people also faces cyberbully in form of abusive language or murder threats or sometimes rape threats on social networking sites.

There are some precautions which are taken to prevent from the cybercrime are: use the full service internet security means to protect against the viruses, to make and use of strong passwords which no one can hack or keep yourself updated on the laws and the cases against the cyber crime. Manage your social networking sites as major cybercrime is happen on social sites platform as identity theft.

Right to internet has became the fundamental right and kerala is the first state to declare this right as part of the Article 19 and 21. The IT act 2000 was passed against the cybercrime. In case anybody get victim of cybercrime they can report their issue in cyber cell. Government also issue certain rights regarding the right to internet and justice shall be provided by the honorable courts.

BIBLOGRAPHY

1. www.cybersecurityceo.com
2. Britannica.com
3. The information Technology Act 2000
4. www.mamupatra.com
5. www.indiankanoon.org

---

1. Dennis Michael (2018) www.britannica.com (Cyber crime- Definition; https://www.britannica.com)
2. Dutta Prabhas (2020) www.indiatoday.in (Internet access as a fundamental right, Supreme Court makes it official; https://www.indiatoday.in)
3. Keshavanarayana K.N. (2013) www.indiankanoon.org
4. www.gktoday.in (India and Cyber security; https://www.gktoday.in)
5. Erikson, John (2008) *Hacking: the art of Exploitation.* 2nd edn.: United States: No Starch Press
6. Sharma, Vakul (2019) *Information Technology law and practice. 6th edn.*: Delhi : Universal law publication
7. Mehta, D. S, (2014) *Mass Communication and Journalism In India* (14th edn.). New Delhi: Allied Publisher