Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0014

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

An Analysis of Cybercrime among Indian Youth

Mr.Hemant G.Warghane
Assistant Professor,
Athawale College of Work,Chimur,
Chandrapur-442903
*Corresponding Author Email:hemantwarghane68@gmail.com
Contact:9423419325

Abstract: "Many silent victims will continue to suffer unless and until our society acknowledges cyberbullying for what it is." It is well acknowledged that cybercrime is a crime perpetrated by professional criminals. The philosophy driving cybercrimes has grown as a result of the internet, despite the fact that technology has made life easier and less violent. Furthermore, developments in the wireless era have fueled an obsession with illicit activity among Indian youth. Most people agree that cybercrime is a crime that is perpetrated online. At the same time, cybercrime is growing in popularity all around the world. The primary objective of the paper is to understand the level of focus among children, how children are affected and victimized by e-crime, and how their personal identification is disrupted and stolen. The gift paper is primarily based entirely on primary information, as well as secondary information and other information. In this cyber world, we virtual citizens, all of us, have instrumented the information available about our location and happenings to the point where privacy appears to vanish.Technologically demanding situations are inextricably linked to security-demanding situations. In a conceptual manner, this paper offers the effect and volume of Cyber Crime among children at a macro stage.

Keywords: Cyber Offences ; New generation ; Internet Security Awareness ;

I INTRODUCTION

In this day and age, email, websites, and online applications are the primary means of communication for everyone. It aids in data circulation as well as the exchange of images and other materials. It is, without a doubt, useful information, but it also exchanges undesirable information. It all starts with inventions in information technology, which raise opportunities after difficulties to our safety, security, and privacy prospects.These days, everyone is connected to one another through various means of communication, such as facebook, instagram, whatsapp, and many other social sites. Despite , every coin has two sides, and while the internet is assisting many people with communication and other means, cybercrime is also gradually increasing, and the world is currently facing critical security problems as a result of cybercrime. Cybercrime is not a new type of crime in the world. It is defined as any illegal activity that occurs on or through the medium of techniques, on any internet sites, or on any other technology recognised by the Information Technology Act. Cybercrime is the most prevalent crime, and it plays a critical role in modernised India. Criminals cause enormous losses to society and the government, but they are also capable of concealing their true identity to a large extent .The majority of crime in India is committed by illiterate criminals, but cybercrime is committed by highly skilled professionals with extensive knowledge of the technical world. In a broader sense, cybercrime includes any illegal activity in which a computer or the internet is used as a tool, a target, or both Cyber crime

is most of the times judicially interpreted in some Indian court judgements, but it is not mentioned in any act or statute passed by the Indian Legislature. Cybercrime is evolving into a difficult-tomanage evil, with its roots in the misuse of modern society's growing reliance on computers. The use of the internet and other technological means has grown in our daily lives and has become a trend among the youth .Furthermore, it is shocking to see that people aged 15 to 24 years are the ones who are most involved in cyber crime as well as victims of cyber crime because India has a young population of almost 27.23% and they are also the ones who are highly active on social media platforms as a result of which they sometimes become victims as well as offenders of cyber crime. This research report will demonstrate the various aspects of cybercrime as well as how cybercrime affects India's youth.

II Literature Review:

The cyber offenders are taking speedy internet and the convenience provided by her statements , she also concluded that it is the responsibility of every internet users to stay aware of cybercrimes and the laws related to cybercrimes . She also stated that citizens must also be aware of different kind of cybercrimes , so that they can not become victims of cybercrime . 1. The authors Parma and Patel in 2016 concluded after the survey that mostly the citizens regardless of the IT field were unable to actively maintain themselves to keep updated with the new information regarded to cyber law and computer safety. They realize that the condition could get ever crucial among the people who are not from the IT background . They suggested that fixing basics manners among individual , while spreading awareness on cyber crime in India . A same kind of report is eventually seen among the B.Ed. pupils of perambulardistrict ,Tamilnadu (Singaravelu and pillai) realized that the situation could become uncontrollable without the complete awareness of cybercrimes and they also can not become a successful teacher without the proper awareness . 2. Mehta and Singh(2013) made a similar statement in order to study the awareness of cyber laws in Indian society, and they discovered that there is a distinct difference in awareness between male and female users . They stated that in comparison with the female users , male users are more aware about the cyber crimes . However ,hasan et al ; concluded on cybercrimes in Malaysia that female users are the one who are aware more than male users . 3. Moreover Letizia Paoli , Jonas Visschers Cedric Verstraete and Elke van Hellemont concluded that , there is no accurate definition of cyber crime neither in the academic sense or in the legal sense and there no specific document in the legal world as well as in the academic world related to cybercrime definition . As stated in a 2013 review of the UN Office on Drugs and Crime (UNODC, 2013), many of these statements do not even have the definition of cybercrime per se, however there are relevant laws that constitute cybercrime . Clough on September 2015 concluded that “there are many terms to define cybercrime as there are many cybercrimes taking place . Van der Hulst&Neve (2008, in Domenie, Leukfeldt, van Wilsem, Jansen &Stol, 2013: 2) concluded that , For researchers, the deficiency of a accurate definition could be problematic. A exchanged definition would not only help describe the scope of the issue under examination, but also ease discussions among professors and provide a basis for comparing their research evidences (ENISA, 2016a: 82; Gordon & Ford, 2006: 13) 4. "When staying interior have become a mandate, overworked dad and mom assumed that retaining the youngsters and the young people busy on clever gadgets in

the 4 partitions is retaining them safe. But, the immoderate intake of the net and clean accessibility to smartphones has placed them at excessive threat of cybercrime vulnerabilities," says India's pinnacle moral hacker and cyber protection expert, Mr.FalgunRathod. Puja Marwaha, CEO, CRY-Child Rights and You, stated even as spending greater time on net for gaining access to schooling and different verbal exchange purposes , children have also become more vulnerable to a number of risks, particularly in the contexts of online sexual abuse, grooming or sexual solicitation, sexting, exposure to pornography, production and distribution of infant sexual abuse material, cyber-bullying, online harassment and cyber-victimization, and numerous other privacy-related risk .

III Research Methodology

Methodology is a set of rules and procedures that govern how studies are conducted and how claims for understanding are evaluated. Methodology encompasses all study techniques. The technique region of selection, populace and pattern selection, facts series strategies and techniques, and facts evaluation techniques are all discussed in methodology. 1. Cyber offences is now a global problem, and no country is immune. In 1820, the first Cyber Crime was committed in India, Japan, and China. Pornography is a major issue; under Section 67 of the Information Technology (IT) Act of 2000, creating, transmitting, and distributing cyber pornography is a crime. Surfing and viewing online pornography, on the other hand, is not always punishable. Making, dispensing, or even surfing Online Child Pornography is a crime under cyber laws. There are nearly 100,000 websites that may be providing illegal Child Pornography .Cybercrime is a type of crime in which an internet connection or a computer is used as an instrument to commit the crime. Some of the factors that influence the decision to commit a cyber crime include the quantity of data stored in a small space, ease of access, complexity of work, negligence, and loss of evidence. In Bhopal, a young person was arrested for being a member of a Whatsapp organisation that shared toddler pornography films. The crime division discovered many messages sent in "code word" annoying toddler pornography content material from the accused.

Some types of Cyber Crimes are noted below:

• Crackers are the people who create viruses. Only hackers investigate other people's computer devices for educational purposes. Pranksters are people who play tricks on others. Criminals who make a living from crime are considered career criminals. Harassment is cyberbullying that occurs over the internet.

• Computer spam refers to unsolicited industrial commercials distributed online via e-mail that may contain viruses and other programmes that harm computers. Restriction of cybercrime is dependent on correct evaluation of their behaviour and acceptance of their influence over various tiers of society. As a result, knowledge of Cyber Crimes in the modern era and their consequences on society, as well as future Cyber Crime trends, are explained.

• Phishing is a more serious type of cybercrime. It is simply one of the many internet scams. Phishing is a type of electronic fraud in which people are duped into disclosing non-public financial information to unauthorised parties. A phishing attack can be handled via voice email, landline, or cell phone. In Kolkata, the death of a younger 17-year-old student as a result of

cyberbullying is most likely an extreme case, but cybercrime is on the rise in this city that, according to a recent TCS survey, is addicted to Facebook - an excess of 85% of young adults have an account there.

1. Mens Rea and Actus Reus Doctrine in Cyber Crime As far as traditional crime is concerned, Mens Rea and Actus Reus are the two most important factors. Actus Reus is Latin for "such a result of human behaviour that the regulation seeks to prevent.". A fee or omission is required to represent a crime. As far as mensrea is concerned, it means "A responsible nation of thoughts." . The intellectual detail documentation the opposing critical aspect of crime.The act remains the same even as the state of mind renders it'reus' and thus illegal. Almost all crimes require evidence of some kind of intellectual detail. thirteen As far as cybercrime is concerned, determining mensrea is exceedingly difficult. In cybercrime, one must examine the hacker's state of mind and whether or not the hacker was aware that the access became Unauthorized. Thus, a "Specific Computer" no longer needs to be meant by the hacker; it's far sufficient if the unauthorised access turns into to "any computer".

2. According to the most recent NCRB statistics, there was a 400% increase in cybercrime instances committed against children in 2020 in comparison to 2019, with the majority of them involving the publishing or transmission of materials depicting children in sexually explicit act. Top 5 states reporting cybercrimes in opposition to youngsters are: Uttar Pradesh (170), Karnataka (144), Maharashtra (137), Kerala (107) and Odisha (71), the National Crimes Record Bureau records stated. As the NCRB 2020 facts reveals, there's a pointy upward push (over four hundred consistent with cent) in cyber crimes (registered beneathneath the Information Technology Act) dedicated towards kids in evaluation to the remaining year. In 2019, 164 instances of cyber crimes towards kids had been said at the same time as in 2018, 117 instances of cyber crimes had been dedicated towards kids and seventy nine such instances had been registered in 2017. Even aleven though the quantity of cyber crime instances dedicated towards kids in 2020 continue to be small, its upward push from 2019 is alarming.

Few cases to understand the impact of cybercrime in India and on Indian youth

The Sony case India had its first cybercrime conviction. This is the case where Sony India Private Limited filed a complaint about a website called www.sony-sambandh.com that caters to NRIs. The website enables NRIs to ship Sony products to their friends and family members in India after making an online payment. The company promises to deliver the goods to the concerned recipients. In May 2002, someone logged onto the internet web site online beneath the name Barbara Campa and ordered a Sony colour television set and a cordless phone.She requested that the product be delivered to ArifAzim in Noida and provided the number of her credit card for payment. As a result, the charge was cleared through the credit score card company and the transaction processed. Following the associated due diligence and checking procedures, the objects were introduced to ArifAzim via the corporation. When the product was first introduced, the company took virtual photographs to represent the transport being established by ArifAzim. The transaction ended there, but after one and a half months, the credit card company informed the company that it had been an unauthorised transaction because the actual proprietor denied making the purchase. The corporation had filed a complaint with the

CBI for online deception, and the CBI had registered a case under Sections 418, 419, and 420 of the IPC (Indian Penal Code). ArifAzim was arrested after the problem became investigated. Investigations revealed that ArifAzim, while working at a call centre in Noida, benefited gain access to the range of an American countrywide credit score card, which he misused at the company's website.The CBI recovered the shaded television as well as the cordless phone. The CBI had evidence to support their case in this case, so the accused admitted his guilt. The courtroom docket convicted ArifAzim under Sections 418, 419, and 420 of the IPC, making this the first time a cybercrime has been convicted .The courtroom docket felt that because the defendant was a 24-year-old boy and a first-time convict, a compassionate approach was required. As a result, the defendant was discharged from probation for a year by the courtroom docket. Sections 67 and 70 of the IT Act are also used in some cases. In this case, hackers hack one's website and replace the homepage with pornographic or defamatory content.

The Bank NSP Case

One of the most notable cybercrime cases is the Bank NSP case, which is the only one in which a financial institution's control trainee became engaged to be married. The couple exchanged numerous emails regarding the use of the organization's computers. After a while, the two split up, and the female created bogus email addresses like "Indianbarassociations" and sent emails to the boy's overseas customers. She did this on the financial institution's computer. The boy's company lost a large number of customers and went to court against the bank. The financial institution was held liable for the emails sent using the financial institution's system.

Kinds of cybercrime :

According to the research , in this report we can say there are ample number of cybercrimes present in this world . As population is increasing rapidly many different kins of technologies are coming and with this the rate of cybercrime is elevating day by day . some of different kind of cybercrime are as follows ; 1. Data manipulation Data manipulation is a kind of fraudulent activity where one person fraudulantely and maliciously alter the data or information of a material for some type of gain or profit . In this activity the fraudulent person will alter and modify the valuable document instead of originally stealing it .

2. Data theft The term data theft is used in different aspects sometimes data theft can be define as ,when a fraud person maliciously stole the data or document of a company or stole any research work of any individual or when a person fraudulently take out bank information using different technical tools illegally , for an instance , stoling of account number , pin number etc. 3. Social interference or Network interference crime Nowadays everyone is uses social media apps and specially the youth are the one whos mostly involved in social media or networking sites .some social media thefts takes out personal information using illegal technical tools and then start blackmailing the victim . Sometime the fraud person takes out the password of a person`s social media app an then hack there account .

Law regarding cybercrime in India :

India is a diverse country and there are various types of laws for different aspects including cyber law . Some of them are mentioned as follows :

In India, Information Technology Act , 2000 is the act in which laws regarding cyber crime is mentioned which has been enforced on October 17, 2000. The major concern of the Act is to provide legal exemption to electronic commerce and to ease filing of electronic records with the Government.

IV Conclusion:

Even if no longer everyone is a victim of cybercrime, they are still at risk. Crimes committed by way of computer vary, and they don't always originate in the back of the computer, but they are completed by way of computer. The identity of the hacker ranges from 12 years old to 67 years old. The hacker ought to stay 3 continents away from its victim, and that they wouldn't even recognise they were being hacked. Crimes committed behind a computer screen are a problem in the twenty-first century. With the advancement of technology, criminals should not rob banks, nor should they be outside to commit any crime. They have everything they desire on their lap. Their guns are no longer weapons; they now attack with mouse cursors and passwords. Individuals should avoid disclosing any information about themselves in order to protect themselves from cyber stalking. This is the same as revealing your identity to strangers in public. Avoid sending any photographs online, particularly to strangers and chat buddies, as there have been incidents of image misuse. To defend against virus attacks, always use cutting-edge and up-to-date anti-virus software. Always keep backup volumes so that data loss is no longer experienced in the event of virus corruption.Never send your credit card information to any website online or to a stranger; this isn't always secure to defend against fraud. Always keep an eye on the websites your children visit in order to avoid any type of child harassment. It is far better to use a security programme that allows you to manipulate the cookies and send all of the data back to the website online, as leaving the cookies unprotected can be fatal. Website owners should keep an eye on the traffic and their patterns on their websites.It is critical to discuss and calculate the outcomes of various other data security consciousness transport methods used in improving end users' data security consciousness and behavior.

V References:

1. https://www.legalserviceindia.com/legal/article-4901-cyber-crime-among-the-youths.html
2. https://www.outlookindia.com/website/story/outlook-spotlight-sextortion-impostingpornography-tops-the-cyber-crime-list-against-indian-youth-in-2021-says-indias-top-ethical- /405056
3. https://economictimes.indiatimes.com/news/india/over-400-rise-in-cyber-crime-casescommitted-against-children-in-2020-ncrb-data/articleshow/87696995.cms?from=mdr
4. https://www.cyberralegalservices.com/detail-casestudies.php
5. https://indiankanoon.org/search/?formInput=cyber+crime+cases