NATIONAL LAW SCHOOL OF INDIA UNIVERSITY, BENGALURU

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF
LL.M. (HUMAN RIGHTS) DEGREE PROGRAMME
FOR ACADEMIC SESSION 2019-20

"CYBER DELINQUENCY: ITS FACTORS AND LEGAL FRAMEWORK"

Under the supervision and guidance of:
DR. A. NAGARATHNA,
ASSOCIATE PROFESSOR OF LAW.

Submitted by:
NAME: KETHOVELU RESU
Roll no: LLM/886/2019

CERTIFICATE

This is to certify that, this Dissertation titled “Cyber Delinquency: its factors and legal framework” submitted by Kethovelu Resu (ID No. - 886) in partial fulfilment of the requirements for award of degree LL.M. (Human Rights), is a product of the candidate’s own work carried out by her under my guidance and supervision.

The matter embodied in this dissertation is original and has not been submitted for the award of any other degree in any other University.

Date: 27/05/2020 Dr. Nagarathna A

Place: NLSIU, Bangalore Associate Professor of Law

National Law School of India University

DECLARATION

I, Kethovelu Resu, do hereby declare that this Dissertation titled "Cyber Delinquency: its factors and legal framework" is a result of the research undertaken by me in the course of my LL.M. (Human Rights) programme at the National Law School of India University (NLSIU), Bangalore, under the guidance and supervision of Dr. Nagarathna A.

This work is my own work and that it has not been submitted anywhere for any award. Where other sources of information have been used, they have been acknowledged.

Date: 27/05/2020	Kethovelu Resu
Place: NLSIU, Bangalore.	ID No. – 886

ACKNOWLEDGEMENT

I take this opportunity to express my deepest gratitude towards my guide Dr. Nagarathna A for her guidance and wisdom in this dissertation. She has imparted her valuable wisdom and knowledge in this research and her encouragement has aided in the completion of this paper. I also thank the facilities that were made available by the college through the remote access library which have been of great convenience and necessity.

I also thank my friends and family for the constant encouragement in these trying times of the Covid-19 pandemic as their support has immensely enabled me to write this dissertation to the best of my abilities. I thank God almighty for his grace and strength in this endeavour.

Sincerely,
Kethovelu Resu
LLM 886

LIST OF ABBREVIATION

AI Artificial Intelligence

PC Personal Computer

IT Act Information technology Act

Sec Section

Ads advertisements

PTSD Post Traumatic Stress Disorder

NCMEC National Centre for Missing and Exploited Children

Govt Government

POCSO Protection of Children from Sexual Offences

NGOs Non-Governmental Organisation

ICT Information and Communication Technology

UNESCO United Nations Educational, Scientific and Cultural Organization

UNCRC United Nation Convention on the Rights of the Child

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

The power of the cyber world cannot be denied nor underestimated. It has greatly aided development in all spheres of life with easy accessibility and its vast plethora of information. The world as we know it would not be the same without the internet, in fact it would be gravely lacking and the opportunities would be very limited. But while the internet has much to offer, its darker features is also a force to be reckoned with. The youth especially is fascinated with the idea of infinite possibilities of the cyber space. Since April 2020, there are 4.57 billion internet users all over the world with China, Unites States and India topping the list. As of 2019, 32% of the Indian population of the internet users are between the age of 12 and 19 and 35% consists of person of age ranging from 20-29. The youth have always been the most active participants of the internet. The world has become a global village with the help of the internet and globalisation is a phenomenon accelerated by the world wide web. As much as the internet allows us to progress, its depravity also corrupts. It provides anonymity in various harmful websites and grey areas like the dark web. The youth are also influenced by the negativity and in turn influences negativity around them online. The social media boom is another factor that hold weight when it comes to the youth influence, good and bad. Children are not victims but perpetrators here with online bullying, hacking, revenge porn, etc. The media has played a role in desensitising and normalising violence and suffering to many youths that watch or come across such kind of content. The increase in interaction in the internet has made the youths more susceptible to all kind of dangers.

The rise of AI is a wonder which was, at one point of time only dreamt of but now AI like Siri and Alexa have caught the attention of the younger population and have actively engaged with it. However, one must wonder, has it replaced familial love and communication or is it just harmless entertainment? The breakdown and separation of families have driven young people to seek comfort from the online world, in search for bonds that that they think will replace the family they are longing for. However, their vulnerability is what attracts the wrong kind of attention. They are soon influenced by the dangerous social groups and take part in different kinds of illegal activities. They do not realise that the real-world concept of family is different in the cyber world.

Although there is a legal framework to tackle issues related to cyber- crime, it is often vague and insufficient due to the of the fast growing pace of the cyber world and also because the possibilities is infinite with the internet even the problems that arise from it are often unique and do not fall within of the existing traditional provisions of law. This gap in law have often crippled the law enforcers and administration in dealing with such problems. There is a need for reformation in order to properly tackle cyber crimes with respects to youth. Awareness on safe practice and precaution must be disseminated in all education institutions. cyber delinquents should also be provided with the right mentors so that they may amend their ways and also use their talents and skills for the good of society. Major steps must be taken if the younger person are to be protected from the online world and also in order to prevent them from engaging in cyber vagrancy. It is time to face the severity of the situation and recognise cyber delinquency as a growing threat to society.

1.2 AIMS AND OBJECTIVES

The aim of this research is to examine youths as victims as well as perpetrators of cyber-crimes. It looks into the various aspects cyber crimes related to youth crimes. Its objective is also to evaluate the factors that greatly impact the commission of these crimes and the impact of social media and different kinds of online communities in the real world must not be underestimated. It also looks at how the existing laws and policies tackle at such problems and examine whether they are sufficient to address and remedy an ever-growing problem. This study also make recommendations on the existing laws

1.3 STATEMENT OF PROBLEM

As we already know cyber delinquency and victimization is a growing problem in society, with more youths turning to online world for entertainment and help. The issues faced in this is manifold but this paper examines the difficulties faced in online safety and cyber security. In this regard, social media plays a vital role as young adolescents and youth affected by it in their daily lives. Another related problem that the research looks into are the existing legal framework for minor cyber criminals and the need for its reformation by specifically addressing and recognising them and then criminalizing them

1.4 HYPOTHESIS

The exposure of children and youth to the Virtual world has made them susceptible to online dangers and well as encouraged them to indulge in deviant conduct online and the present laws are insufficient to address this problem

1.5 RESEARCH METHODOLOGY

The research methodology adopted by the researcher is entirely analytical and descriptive in nature, deriving her views from primary and secondary sources. T

1.6 MODE OF CITATION

The mode of citation adopted in this paper is the Bluebook 19th edition.

1.7 SIGNIFICANCE OF STUDY

This research is significant as it looks at the problem of the cyber crimes with respect to the youth from a broader perspective. It takes into account the factors that influences the young individual to take part in such activities and also examines how an individual becomes a victim of such crimes, that includes socio-economic factors, the environment of the child, peer influence, the attraction of the idea of anonymity, etc. This study also looks at the influence of social media and technological boom Another facet of this research is exploring the question of whether the legislative framework provided in dealing with this kind of crime have been able to adequately handle such crimes. The answer of course is a resounding no but it examines on how and why it has not been able to do so. Therefore, this research is important as it dives deeper into cyber world in order to assess how the youths that are operating in this virtual space are affected.

1.8 LIMITATION

This study is limited to the doctrinal study, hence no empirical study has been undertaken by the researcher. This study is of the views and opinions of the researcher only. And cannot therefore cannot be taken as a legitimate source of law.

1.9 RESEARCH QUESTIONS

1. What is understood by the term “Cyber Delinquency”?
2. Whether youth as both victims and perpetrators of cyber crime have resulted in the endless cycle of online harm?
3. Whether the factors influencing the youths to commit cyber crimes or become victims of the same are justifiable?
4. Whether social media has served as a tool in taking advantage of the vulnerability of youths online?
5. Whether the current legal framework have been sufficient and efficient in dealing with cyber-crime with respect to youth.

1.10 CHAPTERISATION

Chapter 1 introduces the research, and also discusses the Aims and objectives, Hypothesis, Statement of problem, Research methodology, Mode of citation, Significance of study, limitations and chapterisation.

Chapter 2 talks about Cyber delinquency, i.e, the commission of cybercrimes by minors and young adults and define the various kinds of cyber crimes often committed by children and youth. It looks at the nature of these crimes and how they being committed and against whom

Chapter 3 discusses the factors that contributes to the commission of crimes by young cyber criminals. The researcher attempts to understand the individual’s inherent disposition and external influences that play a role in their delinquent behaviour online and how they are an obstacle in their development

Chapter 4 looks at children and youth as both perpetrators and victims of cybercrimes in specific crimes like revenge porn, hacking and pornography and well as their participation in the dark web. Children are easy prey because of their lack of awareness and also unpredictable perpetrators because of their lack of motivation for committing such crime and their ignorance of the legal consequences.

Chapter 5 delves into the effect that social media is home to various cyber threats and affects the young user negatively. The dangers that they are exposed to hampers their psychology and they by developing various kinds of mental illness. It also speaks on the impact of online gaming and Artificial Intelligence. Theses are areas that children are youth have most interest in but these also as where they most vulnerable. This chapter also briefly speaks on the trend of quitting social media by people that are against the control it has over their lives and thus it is an act to be more attentive to their surroundings and the real world.

Chapter 6 addresses the gaps in the present legal systems and analyses how it has failed to provide online protection and also in specifically recognising cyber delinquent.. The chapter also examines whether cyber crimes in general are associated with age and maturity or immaturity of the child or youth inclination their inclination towards cyber victimization or delinquency.

Chapter 7 recommends the steps that can be taken or laws that can be improved in the national and international scenario and the importance of education and awareness in stopping such crimes. There is also a need for mentors in guiding young cyber criminals to redirect their skills in helping society and looking at the factors on why they turned to cybercrimes in the first places.

1.11 LITERATURE REVIEW

- Claudia Megele & Peter Buzzi, Safeguarding children and young people online: A guide for practitioners

This book aims to help social workers in dealing with young children that have suffered from modern digital abuse through the platform of social media. Virtual offences like sexting, revenge porn or the selfie obsession are new to traditional social workers or organisation concern for the welfare of the child therefore the author wish to equip the social worker so that problem faces by children in these matter can be dealt with efficiently and appropriately. It defines and recognises the various threats that are there online and it also lays down important safety practices that can be imparted to the child.

- Nana Yaa A. Nyarko et. al, Juvenile Delinquency: Its Causes and Effects

This article studies juvenile delinquency in general and looks at the circumstances that pushes a child to behave contrary to the law and social norms. It also examines various factors involved in the child's life that shape them, like friends, family, school and home environment. The author also looks at the state of the mind of the child that is likely to indulge in illegal activities, and the effects of abusive parents and interrupting in education.

- Astha Srivastava & Shivangi Sinha, Cyber Delinquency: Issues And Challenges Under Indian Legal System

This article briefly lays down the cyber crimes scenario in the context of India. It is a basic reading on the challenges it faces while handling cyber delinquents. It also recognises the prevalent dangers in the online world like pornography and suicide. The article mentions various legislations that are already in place and encapsulates the holes in the legal system and suggests new way to improve upon it. Its findings are short by effective in delivering the need of the hour, it stressed on building awareness among the common people and educating them about the harm that exist online.

- Majid Yar, Computer Hacking: Just Another Case of Juvenile Delinquency?

The author here talks about the growing phenomenon of hacking and examines the factors as to why there is an increasing no of young juveniles joining the ranks of cyber criminals. This article also speaks on how a child's environment and social groups can influence them to take up such activities online. The motivation for a child is different form that of an adult hacker, where the child is more likely to hack just for fun. The article also sheds light on the relationship between drug abuse and cyber crime. according to the author, the gender also determines the role of the cyber criminal with girls less likely to indulge in hacking. Cyber crimes is associated as a youth problem.

- UNICEF, Child online protection in India (2016)

This report by UNICEF lays down a comprehensive groundwork on the present scenario on the online protection of children, that are in place in India. It defines various cyber crimes and brings them in the context of the children in India. It brings out various statistics and show the need for amendments and changes in the existing laws. This report also recognises role the civil society and NGOs in spreading awareness to educational institutions, children, parents etc on practicing online safety. It also addresses the danger of social media exposure and ICTs.

- Elena Sharratt, Intimate image abuse in adults and under 18s

This research delves deeply in the crime of revenge porn and studies the cause and effect of the said crime. There are surveys that have been conducted on the basis of gender, abuse, police response, case type, etc, which only goes to show that this crime is becoming more commonplace than one would think. The research have found that most of the victims are women and also that there is a lacunae in the laws. No matter how much one can pursue for the appropriate legislations to be enacted , there is nothing like prevention where young women especially are sensitized on the dangers of sharing intimate pictures with anyone online.

- Mary Aiken et al., Youth pathways to cybercrime

This research looks into the online behaviours linking criminal and antisocial activities among the youth. It explores the various gateways and trajectories that lead to cyber crimes by weighing the psychological and criminal factors and its relation to computer science. It looks into the various reasons as to why certain teenagers choose to become cyber criminals, from curiously talented youth, to cyber delinquency to organised cybercrimes.

CHAPTER 2: CYBER DELINQUENCY

2.1. WHAT IS CYBER DELINQUENCY?

Cyber Delinquency means the commission of crimes through the cyber world or internet by persons under eighteen years of age. Here, it would mean any deviant online activity or illegal online conduct committed by an adolescent or young adult. Modern technology has allowed youth today to interact freely with one another and often without adult supervision and approval. Children have also proven to adapt faster to the advancement of technology than their older counterpart. Indulging in illegal cyber activity and causing harm to others have also led the diversion from the positive help of the internet. Cyber delinquency can be various kinds like bullying, fraud, revenge porn, hacking, etc, the dark web is also a popular place among youths where anonymity is guaranteed and its contents are highly inappropriate and illegal. Although cyber delinquency occurs in the virtual world, its outcome and effect on the victims are as harmful as crimes committed in the real world. Mental suffering and trauma is a common characteristic of the victims of cyber delinquency.

Cyber-bullying is the most common kind of Cyber Delinquency and it is again most common in the platform of social media where the culprits write mean and vulgar comments or posts inappropriate content regarding that person with an intention to humiliate or bully them. Cyber delinquency has far-reaching consequences in real life as the victim is affected deeply and can go into depression, such negative feelings can accumulate and boil over in the form of harmful cyber conduct, hence the victim becomes then becomes the bully. This is a ruthless cycle that must be broken. The General strain theory also supports this theory. This theory was propounded by Robert Agnew and is a modification of the previous Strain Theory by Robert King Merton. In the latter, only financial restraints were mentioned but the former includes a more general view stating that any negative experience can induce stress to the victim. Such stress seldom find a healthy outlet and therefore it accumulates over time and compels the victim to also inflict the same harm that he/she endured onto others. It also increases the chance of the victim in engaging in activities like physical fights, carrying of weapons, being absent in school, etc.[1]

There are various online communities that promote and encourage self-harm and surprisingly has a large community of youths that advocate this. These kinds of communities include promoting suicide, self-harm like cutting oneself, pro-ana (anorexia) and are usually in a forum setting where anyone can post messages in the common board. The interactions among these peers always appear to be toxic and harmful to the mental and physical health of the individual. Persons with existing depression or eating disorders or suicidal tendencies have a strange sense of belonging in such websites where their disorders are celebrated and encouraged instead of dealing with the fact that such disorders are life threatening.

Another kind of harmful sites/communities are those that encourage persons to inflict harm on others and this results to real life commission of such crimes by persons that are members and party to such sites. These harmful websites usually draw in young audiences that are easily influenced or pressured. The administrators of such webs are usually teenagers themselves.

Hacking and cyber fraud have gained popularity among the cyber delinquents today. This is because the internet provides them a certain amount of anonymity and a vast ocean of information about others. What must have started as a harmless prank is now an insidious activity growing at an alarming rate.

2.2. CYBER CRIMES AS CYBER DELINQUENCY

A juvenile is someone who is under the 18 years of age and has been termed as Juveniles in conflict with the law. Therefore, when such a juvenile commits a crime it is called a juvenile crime and not a crime. Cyber Delinquency therefore means a minor behaving in away that is contrary to the law online. The law is not comprehensive in dealing with cyber delinquency which poses a problem because there is a growing number of children committing cyber crimes. This has caused young criminal to be dealt with inefficiently by the law and authorities are confused

[1] Ian D Greenwood., *CYBER-VICTIMIZATION AND DELINQUENCY: A GENERAL STRAIN PERSPECTIVE*, Graduate Student Theses, Dissertations, & Professional Papers. 10715. (2016)

as to how to deal with such apparent loopholes in the law. The most common kinds of cyber-crimes committed by juveniles today are cyber bullying, harassment, defamation, drug trafficking and hacking into stored data bases. Juvenile delinquency in general is an uprising topic today in the context of criminal law in the country. It is most likely to result in commission of more crimes when the child becomes an adult since it is a fact that criminals activity commences in childhood.[2] Additionally, when this delinquency is coupled with the cyber world, it becomes a lethal combination.

2.3. KINDS OF CYBER DELINQUENCY

The internet is a double-edged sword, while it has tremendously enabled the youth to learn and advance it has also equally allowed delinquency is the spheres of the cyber world. It is true that children are often victims illegal online activities namely child pornography, harassment, grooming, etc but we must acknowledge the growing trend of the children and youth becoming perpetrators of such crimes online. One of the most recurring cybercrime is cyberbullying which involves harass and at time defaming their victims. Cybercrimes can be broadly categories into two kinds:

- Firstly, crimes where the network or P.C is the target for example crimes like hacking, production of malware
- Secondly, cyber crimes where the internet or computer is used as a tool to commit the crime, for instance, child pornography, cyber bullying, harassment, etc.

2.3.1 Computer as the target of cyber crimes

Hacking is the unauthorised access and use of other people's computer systems. It can be said to be a break-in in the cyber world. It is usually not motivated by financial gain but instead, gaining recognition and respect from peers or to prove their worth to themselves by doing something that is considered *'cool'* by their peers. There are also several movies that celebrates such criminal activity which only cements the idea of hackers being teenage miscreants. The term 'hacker' first appeared in the 1960s to

[2] R Kalaivani & Muthu Kumar, *Juvenile delinquency in cyber crime*, 2 Int. j. acad res & dev, 624-626 (2017)

positively denote people that could solve and develop creative problems related to computer programming. They believed in an ethic where there was freedom to access and exchange information and the potential of science and technology to advance the lives of individuals. It can be said that it is not entirely fair to associate hacking with criminal activity but there is a tendency to stress on the negative impact of hacking, completely putting aside the genesis of the term. What must be considered here is the motive and intention of the hacker. Hacking can be a gateway to much bigger problems. What started as something as innocent as showing off their hacking skills to their peers can turn into a serious addiction over-taken by greed. It can also turn a teenager to other illegal activities as it emboldens them to move on to more dangerous activities.

In Sec 66 of the it Act, 2000 non-ethical hacking is a punishable with imprisonment up to 3 years and fine up to two lakhs rupees or with both imprisonment and fine. Section 43 also prescribes penalty for destroying the computer or its system, which is common whenever a PC and its system are hacked. Section 65 also states that tampering with the Computer Source Document is an offence. Ethical hacking can be encouraged among young hackers in order to redirect their skills.

Malware is a malicious software and is designed for various reasons:

- To take gain unwanted access and control of the computer;
- To gather, modify and tear down information in the computer.
- To spy on the activities of the victim and secretly insert and run new application.

Remote Access Trojan or RAT are malware that are designed to take control of a computer. This is usually carried out through the entry of an infected document which takes over the system as soon as the document is opened by the unsuspecting victim. Delivery of RAT via e-mail is also a common attack method.

2.3.2 Computer as a means to commit cyber crimes

Cyber Bullying is growing at a rapid rate practiced by both school children and college students. Bullying is no longer limited to the schoolyard or college campuses as children and youth have to also deal with it online. It is a cruel act of harassment against the helpless and it is used as a means of shaming someone or spreading vicious rumours or even as an act of revenge. It may occur in various ways like hurtful messages or abusive emails and messages, images and videos, which contains imitating someone or including or excluding a person, humiliating others and spreading online gossip in chats. It is an abuse of technology and must be stopped and youths must be made aware of its impact on their peers. According to a 2018 study done by Ipsos[3], parents were polled in from twenty-eight countries to ascertain cyberbullying and India was rated as the country with most parents confirming instances of cyberbullying where 37% of parents said that their children were bullied online and 14% stated that online bullying occurred on a daily basis. Cyber bullying is dangerous because its consequences can be deadly, there have been several cases where victims have resorted to suicide. For example, *United States v Lori Drew*[4], the perpetrator, Lori Drew, was charged for causing the suicide 13-year-old Megan Meier, who was a victim of cyber bullying. The most dangerous aspect of cyber-bullying is that with the use of technology the perpetrator can dispense any harmful content against the victim at nay time of the day. Such content spreads like wild fire.

Social media has become the biggest platform for cyber bullying as well. For example, there have been a large number of bullying in Instagram where embarrassing pictures are posted along with insulting hashtags or creating fake account with the purpose of defaming and insulting a particular person. Another channel of bullying would be confession pages, where anyone can post anything anonymously. The administrators, who are usually young individuals themselves, receives messages which they then post for everybody to read. Person who have ‘liked’ these pages stay connected and receive notification whenever there are new posts in the confession pages. These pages are at times used to expose secret information of the victim and this anonymity encourages people to say anything they want.

Other than suicides that have been induced by bullying, there is a rise in cyber-suicides all over the world and is a more recent phenomenon among the youths. It is

[3] Ipsos is a global survey-based market research company, owned and managed by research professionals.

[4] 259 F.R.D. 449 (C.D. Cal. 2009)

where a person commits suicide abetted by technology and there have been instances where such suicides have take place live using the internet.

Cyber Stalking is another dangerous online activity. It is stalking or harassing or intimidating someone through the means of the internet or other electronic means. Here the victim is stubbornly pursued online by sending them emails or through other ICT with the aim to control and intimidate the victim. In 2001, India had its first cyber stalking case in the *Ritu Kohli case*[5] where the victim Ritu complained of being stalked online. It was discovered that a person names Manish Kathuria had stolen her identity and had been using it to chat with strangers and send obscene messages on the website named www.mirc.com. He then further distributed her personal information on the site which led to her receiving calls and messages by unknown number at all hours of the day. This resulted in an estimated 40 calls from both national and international numbers within the span of three days. This case was registered under sec 509 of IPC.

Child pornography is a prevalent form online child sexual abuse and is considered a crime. There is also an increase in reported cases of blackmail, "sextortion" and revenge porn in relation to child pornography. Child pornography and child trafficking is also closely linked as in both crimes, children are sexually exploited. Cyber Pornography is the display, publishing, distribution, creation or importing obscene material online. The internet have aided children in their learning and developing and has become a necessity. However at the same time it has also been grossly misused by underaged children and other youths alike to search for pornographic content online. Interestingly, it has been found that children are both the victims and perpetrators of cyber pornography.

Revenge Pornography is also gaining ground among youth today, it is when private and sexual materials of another person are shared whether in the form of pictures or videos with the motive of distressing and embarrassing the victim and most importantly, without their consent. At times, private information about the subject like their full name and address are attached to such images or videos.

Fraud is another area of cyber-crimes that have caught the interests of youths and this includes identity theft, phishing, hacking and financial fraud. The fact that cyber

[5] Manish Kathuria Vs Ritu Kohli, C.C.No. 14616/2014

criminals are finding new ways of using the internet as a tool has been heavily included in the National crime statistics and these online attacks are of serious nature. Due to the advancement of the internet stealing has now become possible without the need to trespass upon property.

Phishing is the act of capturing personal information when users visit fake websites. This is mostly used to obtain bank account details and passwords to email-addresses and when this has been achieved, they then use the email id to send span and other malicious e-mails to other businesses. **Pharming** is the act of redirecting the unsuspecting users to the sites chosen by the hacker.

The most repeated and recognised kind of cyber-theft carried out by youth and young adults is **piracy**. Here, illegal copies of any form of digital media is downloaded without the explicit consent of the creator. Children and youth are also among the biggest downloaders of pirated music and movies which is a copyright infringement. Piracy is usually thought of very lightly as they are unaware of the serious implication of their actions.

CHAPTER 3:

ATTRIBUTING FACTORS TO JUVENILE DELINQUENCY

In order to understand why young adults and youth involve themselves in illegal online activity we must first understand the reason why they choose to indulge in delinquency behaviour in the first place. How do their very own nature, family and peers influence them? Do they commit such crimes on their own volition, or do circumstances force them to for the sake of survival? There is no clear-cut answer in answering these questions. Adolescents and youth are at their developmental stage where their interests and personality are being shaped by their experiences and circumstances. Additionally, many of them face various other constraints like unemployment, poverty, absence of the right role models, family disintegration, etc. and in such cases they may feel like they have no other choice but to become cyber delinquents

3.1. INDIVIDUAL FACTOR

The individual factors is of the view that the very nature of the person makes them naturally inclined to conduct themselves in a manner contrary to law. In other words, the individual cannot help but behave in a certain way. This will be explored in:

- Characteristics of personality
- Drug use
- Mental Disease

3.1.1. Characteristics of Personality

The tendency to commit a crime in closed linked with the characteristics of personality. Personality is the result of the interactions with different aspects and elements of a person’s environment, therefore the more an individual is exposed to negative elements, the more pessimistic an individual will be. And this can lead to children being exposed to such elements resorting to criminality. So the personality of Juvenile delinquents also throws light on the kind of environment they grew up in or were frequently exposed to. A normal child or youth is less impulsive and explosive and more obedient, social and peaceable. In contrast, such delinquents are found to be more disobedient, unsocial and explosive.

Emotional instability is a prime cause of commission of crimes. An individual’s personality is negatively affected from the lack of love and affection of their family. The parents exercise little to no discipline on their children and can lead to the child developing feelings of insufficiency, insecurity and inferiority.

3.1.2. Drug abuse

Drug abuse can promote deviant conduct and in turn deviant conduct can promote drug abuse, especially when surrounded by peers that does the same. Like any other drug addict, a child or youth abusing drugs will go to great extents to get their ‘fix’ even if it means resorting to illegal activities. Many children start their drug addiction at home, an early exposure to drugs can lead to a child to grow up to do the same as drugs are easily accessible at home. Similarly, a child using the internet is bound to be exposed and enticed by inappropriate content and may develop a notion that it is natural or ‘cool’ to take drugs and they in turn may influence their peers to do the same. It is believed that young persons who have been physically and emotional abused are traumatised finds comfort and solace in their drug abuse.

There is a high possibility that children will buy and sell drugs online through the dark web where they remain anonymous, their identities safe and their activities made untraceable through the Tor browser. The most sold and advertised product on the dark web are drugs Many companies use the dark web to sell drugs since it is prohibited in the usual e-commerce websites.. One study showed that, on examination of the demand-supply chain of the dark web, most of the ads were about drugs rather than hacking[6]

Young individuals are also extremely susceptible to online grooming where they can be lures in to entrapped them into a life of drug related crimes. For instance, in 2019 in UK, law authorities discovered that children as young as 7 were being groomed and used to sell drugs around their neighbourhood.[7] The children may first be tasked with

[6] Othmane Cherqi et al, *Analysis of Hacking Related Trade in the Darkweb*. 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), 79-84 (2018)

[7] Vikram Dodd, *Children as young as seven 'being enslaved by UK drug gangs'*, The Guardian (Jul. 9, 2019) https://www.theguardian.com/society/2019/jul/05/children-as-young-as-seven-being-enslaved-by-uk-drug-gangs

simpler things like stealing to prove their loyalty, then the complexity of criminality they are coerced into becomes worse. Another means to strengthen the criminal bondage is by feeding them drugs at an early age to get them addicted so that they will not be able to leave. Youths in gangs and cliques also sell drugs because it's the only way to fund their criminal activity. Glue-sniffing is particular popular among children that lives on the street.

Since drug use is associated with criminality, children who are addicted to it are also involved in producing and trafficking it and also in other kinds of illegal activities and exploitation.

Drug abuse definitely facilitates cyber delinquency but it also works vice versa where online deviancy also promotes drug use among the youth. We can see this in the case of internet addiction which plagues the modern society. Its addiction can be compared to something as strong as alcoholism and when the addict is unable to restrain their desires. Continued engagement in the internet for long period of time can lead an individual to consume 'soft' drugs like marijuana and eventually move on to 'harder' drugs like narcotics.

3.1.3. Mental disease

It can be said that a criminal is a mentally unstable person who needs treatment just as much as they need punishment for their crimes. Psychiatrists believe that psychopathic personality of a person can be one of the factors for their criminality. Psychopathic children are the result of them growing up in a family environment that was devoid of love, affection and control. The child may instead be anti-social, cruel, suspicious, self-centred, harbour feelings of revenge, hyper sexual, etc. In others cases like bipolar disorder, clinical depression, severe anxiety, etc. the children sometimes cannot physically control themselves in the things that they are doing or at time don't even care about the repercussions of their actions. Another example would be a sociopathic child lacking empathy and other normal human emotional responses to things and they would not understand between right and wrong but instead simply do whatever they want to without holding back. Similarly, individuals suffering from mood disorders will appear more anger, irritable and hostile, and may fly into fits of rage when slightly provoked. In most cases, the impact of anxiety disorders are less aggressive behaviours with the exception of PTSD.[8] The mentioned mental disorders are either hereditary or developed over time with the environment of the child or youth, or through circumstances and experience they go through.

Here, they may turn to drugs to ease their discomfort or simply out of curiosity and their inability to see the wrong in their action. In the online world, it may be easier to mask or hide their illnesses where they do not have to physically meet a person like the real world. The motivation for committing cyber crime by these youths is difficult to understand. It is easy to understand why a person motivated by money would commit such crimes but for children and youth suffering from mental illnesses, the reason behind their actions is not always apparent.

3.2. SOCIAL FACTORS

"You are the average of the five people you spend the most time with."

- Jim Rohn

Do the people you surround yourself with truly influence the choices you make? The answer is an affirmative, especially when persons are at an age where they are most susceptible to their social environment. A child or youth is influenced by the environment at their homes, schools and colleges. They may start with something as insignificant like bunking class, stealing, drinking and smoking but as they grow older, these former habits may evolve into more serious crimes like sexual crimes, theft, organised crime, etc. these social factors consist of:

- Peer Influence
- Family and Poverty

3.2.1. Peer Influence

According to the Differential Association theory, delinquent behaviours are learnt and this occurs when they associate themselves with criminal pattern and other means

[8] Lee A. Underwood & Aryssa Washington, *Mental Illness and Juvenile Offenders*, Int J Environ Res Public Health, 13(2): 228 (2016)

involved and it is also learned through interactions and communications.[9] The general strain theory as mentioned earlier also states that persons who are a victim of crimes also later develop a tendency and habit to commit similar crimes themselves.

In the adolescence stage, the need for an identity or the desire to prove themselves to their peers is a strong factor in delinquent behaviour. The urge to impress their peers trumps the need to take cautions online. The lack of proper role models has also made children more vulnerable to peer pressure and social influences. A study has shown that peer influence is the biggest factors for juveniles to engage in cyber-crimes and that having a low self-esteem also plays a part in creating cyber-delinquents.[10] The peers may also force or put immense pressure on the youth to commit certain cyber-crime in order to prove his loyalty or to be accepted in a peer group.

A person may influence or pressure his friend to take videos or pictures of their sexual encounters with their partner and later use that to threaten and blackmail or a group of friends may conspire to post mean and cruel pictures or messages about someone else with the intention to defame and hurt them. The General theory of crime states that since humans possess common sense, they weigh the pros and cons of every decisions including the ones that lead to criminal behaviour and then act accordingly, however low self-esteem may drive a person to be insensitive, impulsive, and short sighted and therefore prefer immediate gains through crime even though its repercussions are heavy. The consequence of having a low self-esteem also equates to a person hungry for acceptance and peer approval, and this makes them easily impressionable and also an easy prey to peer groups with a history of deviant behaviour.

The social learning theory, propounded by Ronald L. Akers contends that individuals develops deviancy and continues a criminal career because of an active social learning process depending on differential associations. In other words, individuals are exposed to deviancy, experiences and reinforcement based on the person they continually associate themselves with. This theory is essential in understanding why the youth commit cyber-crimes since these offenders not only need *to "learn not only how to operate a highly technical piece of equipment but also specific procedures,*

[9] Nana Yaa A. Nyarko et al., *Juvenile Delinquency: Its Causes and Effects*, 88 J.L. Pol'y & Globalization 166 (2019).

[10] Thomas J. Holt et al,. *Low Self-Control, Deviant Peer Associations, and Juvenile Cyber deviance*, 37 Am J Crim Just, 378–395 (2012)

programming, and techniques for using the computer illegally"[11] there are plenty of evidence by various scholars that have discovered that association with deviant peers is one of the biggest contributors towards cyber deviance.

It is found that even if some children and youths have extra ordinary computer skills, due to the lack of an appropriate teacher or guide to direct and encourage them, they choose to use their skill for the wrong reasons instead. Peer influence does not only present in the real world but in the virtual as well.

3.2.2 Family and Poverty

Children and youth from poor family backgrounds are more likely to take part in illegal online activity then that of children from a wealthy or normal economic family background. Or it could also be the desire of the youth to become financially independent and live a different lifestyle. Financial strain or desire of financial freedom coupled with peer influence is enough to persuade any youth to indulge in cyber delinquency. However, young persons who become delinquents often live in tough and difficult circumstances, where they are left to fend for themselves. Here, Poverty along with parental neglect and peer influence is instrumental in the formative years of the youth.

Most children do not become delinquents or criminal because their anti-social conduct was checked by their family but what happens when there are no adults to supervise and guide them? They become vulnerable to all kinds of influences. Most delinquents come from the slums of cities where poverty is present and crime becomes a norm. Children without a proper family structure or neglected by the parents seek love and comfort from other things and when they are given an opportunity to join a group, in real life or virtually, irrespective of whether their objectives are good or bad, they will mostly like jump on the idea of belonging somewhere. Similarly, with poverty, if a person is from an under-privileged family without the means to have proper meals and clothes, any opportunity to earn money will be an attraction, irrespective of how they earn the money and irrespective of the criminal nature of the act.

[11] W. F. Skinner & A. M. Fream, *A social learning theory analysis of computer crime among college students,* 34, J. Res. Crime Delinq, 495–518. (1997)

As discussed earlier it not only peer influence that shapes the child but also the family influences. When the natural intimacy of family is lost, the child looks for it elsewhere or if members of the family show criminal tendency or have a known record for criminal conduct and continue to commit such crimes, the child or youth at home are bound to pick up on these habits and manifest them in the real or virtual world. at times, a parent might even teach child the trick of their ‘trade’, therefore if a parent themselves hacks for a living and commits various kinds of cyber crimes, he may teach his child to obtain the same set of skills so that he may do conduct the same activities in the future. They may also be taught to steal more efficiently or to fight better, etc. another factor to consider is if the household that the child grow up in is violent and is scolded and beaten on a regular basis, he may develop resentment and hatred towards his parents and run away at an early and turn to the life of crime instead. If the parent of the child disregards their emotions, they may grow up to develop feeling of insecurity and other mental complexes. In order for children or youth to stop deviant behaviour and respect social norms and people, it is vital to create such an environment where the inspiration for criminal behaviour is minimized.

There have been a rise in the webcam phenomenon, where underage girls or young college girl act out the sexual fantasies of their clients. It is usually in the form of live streaming sessions and the clients pay these girls for requests and favours and this often associated with sexual conduct like taking off pieces of clothing or performing sexual acts. It is a particularly dangerous uprising trend as it leaves these underage girls exposed to paedophiles of the cyber world and very often these girls lie about their ages to appear older. However, the reason for becoming a cam girl varies to that of camgirls from underdeveloped or developing countries. In developed countries, most of the time it is a choice that the girls have independently made to earn extra cash or is a form of expressing their sexual freedom. However, the picture is much glummer in other parts of the world where the camgirls feel like they do not have a choice but to sell themselves online due to their poor economic condition in hopes of financial aid in return for sexual acts.

In general children and youths from the underdeveloped and developing countries are more motivated by financial gain. A study in Nigeria from a parent’s perspective where it states that due to the financial state of families, single mother are forced to leave their child alone while they go to their work in order to provide for the family and so the child is exposed to deviant elements in society.[12]

[12] Ibrahim S, *Causes of socioeconomic cybercrime in Nigeria*, IEEE ICCCF Canada, pp. 1–9 (2016)

CHAPTER 4: YOUTH AS PERPETRATORS AS WELL AS VICTIMS OF CYBER-CRIME

The internet is multi-faceted with endless possibilities and opportunities, however because of unlimited vastness, there are dangers lurking around. In cyber crimes the youths have been both the victim and perpetrator. Children are the ones that suffer the most with the growing insidious rise of child pornography and other sexual offences against children committed online however we must only examine this issue from a single perspective, in order to fully understand cyber crimes it is necessary to see the responsibility of the youth to act responsibly online and not just see them as victims. Victimization can turn a victim to become a perpetrator as well.

4.1. THE DARK WEB

The dark web cannot be reached through normal search engines, it has an encrypted online content. The websites that exist inside the dark web uses anonymity tools like I2P and Tor (the Onion router) to hide their IP address. The main attraction of this secret place of the cyber world is that it offers anonymity where their identity is hidden and their activities untraceable. Hiding the identity of persons online emboldens them to conduct themselves however way they want and this usually includes illegal activity.

The contents of the dark web are dangerous and there is a high risk of their computers and personal information being hacked. It is a space for more serious online offences and is considered as the underworld of the internet. The anonymity tool Tor was initially invented by the U.S military in the mid-1990s for the sole purpose of communicating anonymously between intelligence agent. Today, however, this tool has been misused by many for various kinds of communication, from government intelligence to spying to drug trafficking and paedophilia.

Children and youth are at first attracted to the dark web as they are curious about the mysterious nature of such a place but are soon be dragged into the illegal world. Children in conflict with law are especially at risk here, they may find that the dark web is a convenient place for them and may even find illegal jobs that interest them here. Hacking is rampant in the dark web and hackers often advertise their skill for a fixed price. Youths with special skills in unethical hacking may see the dark web a safe haven to put their skills to test and also bond with the booming hacker community there.

Although the dark web is like a playground for deviant behaviour without any rules or law to regulate them, youths have also become victims and prey to such places. Even though some may visit into the dark web for curiosity, even simply browsing through it poses a threat. The dark cyber world has the world's largest sites on child abuse and exploitation. In 2018, the US justice dept with the help of partners in U.K and South Korea charged a 23-year-old South Korean man named Hong Woo Son. His website named 'Welcome to Video' had over 200,000 videos involving children abuse and was worth approximately 8 terabytes of data.[13] There are countless more paedophiles lurking in the dark web hiding behind the anonymity it offers.

Children are groomed online by adults by befriending them first and making the child believe that they are harmless but soon, they convince them to send pornographic pictures or videos and these in turn would be uploaded in the dark web. A child can be in denial as in the case of Praniti, whose pornographic pictures was found on the internet. And when confronted by this she refused to believe that it was wrong and insisted the person responsible for those pictures was her friend. The biggest threat when children are being groomed is that child trusts the prey unconditionally, irrespective of what they've done. According to NCMEC based in the US, India has the most number of online sexual abuse images in the world, with Delhi at the top uploading maximum child porn, followed by Maharashtra, Uttar Pradesh and West Bengal.[14]

4.2. PORNOGRAPHY

This form of online sexual exploitation is unfortunately on the rise. In commercial exploitation of children, someone benefits from a commercial transaction. Paedophiles consider the cyber world to be the perfect place for grooming children, and also to solicit and entice them into sexual activity for financial gain. The sexually

[13] Zack Whittaker, *Justice Dept. says its taken down 'world's largest' child exploitation sites on the dark web*, Techcrunch (oct 16 2019, 7:52 pm), https://techcrunch.com/2019/10/16/doj-child-exploitation-dark-web/

[14] Sonali Acharjee, *The Dark Web of Child Porn*, Magzter (March 2, 2020) https://www.magzter.com/article/News/India-Today/The-Dark-Web-Of-Child-Porn

explicit images and videos of children obtained through grooming may also used for blackmail and sextortion and for prolonged sexual exploitation.

The production and distribution of pornography between two consenting adults is legal in many countries, however any material or data that depicts a child in a sexual activity is universally regarded as a crime. “The threat posed to children by predatory paedophiles, which conceal their true identity whilst using the Internet to ‘groom’ potential victims” was recognised in the report of the Parliamentary Committee on Information Technology in 2014. There are special websites in the dark web that allow their buyers to purchase child sexual abuse materials.

There is a different and new kind of demand of child sexual abuse material on the rise. This demand consist of self-generated content like sexting or live streaming of videos through webcams where the client pays a fee to see child sexually abuse live and also be able to instruct the live performance. Very often, the parents of these young children are also the perpetrators where they make their child perform sexual acts or take off their clothes in front of a webcam in return for a minimal fee. Such kinds of incidences have been reported in some parts of the world.

A documentary named *‘Mums Selling their Kids for Money’* by BBC sheds light on the atrocity of two mothers caught selling their own children online to paedophiles. The mothers, in return for money, were willing to commit sexual acts on their children by following the instructions of paying customers over a webcam. It is an undercover operation that investigates such acts before arresting the two mothers. These women also trafficked their children to travelling paedophiles, most of whom were from US and UK.[15] Almost every international cases of webcam child abuse stems from Philippines due to the presence of English speakers and good internet connections and international cash transfer systems coupled with prevalence of poverty and access to vulnerable kids.

The dark web and child pornography are also closely linked. Pornography is already a very common phenomenon easily available in normal internet browsing tool but because pornography is not only addictive but progressive as well the more pornography a person watches the more desensitized he becomes and therefore goes

[15] Natalie Corner, *Children as young as five are being sold to paedophiles by their own mothers in the Philippines, shocking TV investigation reveals*, Dailymail UK, (18 may 2017, 5:00 PM) https://www.dailymail.co.uk/femail/article-4507338/Children-forced-sex-mothers-money.html

in search for more shocking and depraved material, so it is no surprised to know that child porn is increasingly becoming more vile and widespread on the internet and because normal browsers are prohibited from showing child pornography, the dark web is utilised to showcase and advertise such content.[16]

One of the most prolific bust of a paedophile ring was *The Wonderland Club* in September 1998 and was described as "an international network of paedophiles involving the rape of boys and girls live on camera and the traffic in images of the torture of children as young as two months".[17] It was created by two Americans and consisted of 180 members.

There are also many children all over the world that willingly participate in conversations with explicit or implicit sexual undertones, and therefore may send messages and sexual images either of their own volition or due to peer influence or pressure, however sending of messages that contain sexually explicit images, videos or any other material only increases the vulnerability of children and young people online. There are others who use such material to harass, blackmail or threaten into sending more pictures or for sexual favours. The growing no. of reported cases of sexting, sextortion and revenge-porn all in turn point to the growing vulnerability of children and youth due to self-exposure.

Another factor for why children indulge in pornographic images and videos can be the lack of of a proper sex education in schools or homes. Their unawareness about these facts means that they are ignorant of the dangers of the online world and its repercussions. They can then unknowingly be committing crimes like cyber pornography themselves.

4.3. REVENGE PORN

[16] Schell, Bernadette et al., *Cyber child pornography: A review paper of the social and legal issues and remedies--and a proposed technological solution*, 12 Aggress Violent Behav, 45-63 (2007)

[17] Martin Bright & Tracy McVeigh, *This club had its own chairman and treasurer. Its business was child abuse*, The Guardian (Feb 11, 2001, 2:33 AM) https://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright

For millions of women, it is no longer safe to share contents of their personal or daily life online. This freedom to share has been taken away in personal and intimate ways. Revenge porn, also known as Non-consensual pornography (NCP), is when disgruntled or unhappy romantic interests post explicit and demeaning content online with an intention to humiliate and harass their former partners. Unfortunately, this cybercrime problem is without a uniform solution. Revenge porn according to the laws in England and Wales is classified as "photographs or films which show people engaged in sexual activity or depicted in a sexual way or with their genitals exposed, where what is shown would not usually be seen in public".

The explicit pictures or videos at the time being taken are consensual but later but when the relationship ends it is used by the spurned lover to misuse them as revenge.

There are two high profile Canadian cases concerning the deaths of Amanda Todd and Rehtaeh Parsons. Intimate images of the girls were cruelly circulated among their peers, including a picture of Rehtaeh parson where it indicated that she was a victim of gang rape. It was not long after that these girls decided to take their own lives. In December 2014 the Canadian Federal govt. banned the unauthorized distribution of nude pictures and videos.

A study done by University of Exeter in 2019 showed that 3 in 4 victims are females, 9 out 10 female victim face intimate image abuse and 9 out of 10 victims that are male suffer sextortion.[18] This has shed light on the striking gender disparity. The Revenge Porn Helpline revealed that 73% of the callers were female, out of which 97% reported intimate image abuse. Contrarily 27% were male callers and out of which 90% sextortion victims. Revenge porn can broadly be categorised into two categories:

- Intimate image abuse: this usually follows after a romantic relationship is over. It is used to 'punish' or control the victim. The perpetrators here can be ex-partners from months or years ago or the perpetrators can be someone the victim recently broke up with a likely history of abuse.
- Sextortion: Financial blackmailing the victims is the main focus here and can be done by hackers or criminals.

[18] Elena Sharratt, *Intimate image abuse in adults and under 18s,* University of Exerter Economic and social research Council, 12 (2019)

Unfortunately, in revenge porn, the victims are often shamed and thought of as someone having low morals and that she 'deserved' the harassment or ordeal she was going through. Society does not completely see her as a victim but as a blame-worthy person. The images or videos that are posted are sometimes accompanied with personal information about the victim like their address, full name and social media handles. There are numerous websites solely dedicated to humiliating their former lovers in the most perverse manner.

Revenge porn is a gross violation of privacy and trust but also an instrument to subjugate and discourage a woman from expressing her sexuality. What many people don't seem to be aware of is that revenge porn not only ruins lives but also comes with serious psychological cost to its survivors, where sometimes she feels compelled to uproot her entire life and move somewhere else because of the stigmatisation she faces in society. Victims also shy away from courts because they unable to bear the pressure and embarrassment

In April 2015, the police in the Nargol village of Valsad (Gujarat) booked a 21-year-old man for allegedly circulating photos of his teenage ex-girlfriend that were sexually explicit on various popular social media sites. A mobile phone was used to take the pictures which were circulated by the accused once when it came to his knowledge that the girl's parents were in search for a groom for her. The accused was charged with molestation under different sections of the Information Technology Act and the Protection of Children from Sexual Offences Act.[19]

Children and youth also share explicit content with one another using mobiles and internet for various reasons. In India, a clear expression and interest in sexuality through sharing of images or conversations among peers is part of growing up as a boy. In dealing and exploring their own evolving sexual identity, girls too, have their own means and ways.[20] Some wanting to fit in with or impress their friends boast about having photos in their phones or about sending the same. The widespread use of mobile phones and internet is an added advantage to criminals and predators who are

[19] Reasgan Gavin Rasquinha, *Are you a victim of revenge porn?*, Times of India, (April 19 2015, 00:00) https://timesofindia.indiatimes.com/life-style/relationships/love-sex/Are-you-a-victim-of-revenge-porn/articleshow/46852091.cms?

[20] UNICEF, Child Online Protection in India, New Delhi, 2016

capitalising from it through sextortion, and grooming for sexual purposes by e-mail and Voice over Internet protocol (VoIP).[21]

In the case commonly known as the *Delhi MMS Scandal* or *Bazee.com case*[22] a sexually explicit MMS of two students of the aged 17, belonging to a well-known school, were circulated online. A mobile phone was used to capture the act which was consensual but its distribution was illegal including the bid to auction the clip on bazee.com. The two students in the video were minors and therefore not prosecuted and because the possession of the video could not be established even the student responsible for its spread was let off. However, because the CEO of the website allowed the listing of the clip, he was booked.

The danger of digital content is that once sent it is difficult to control its unpredictable outcome. When sexting goes out of control, its consequences can range from criminal charges to trauma, damage to reputation and, in some cases, even suicide.

A grim case of sextortion can be seen when, in January 2016, six youths and two minors were arrested for their involvement in two different rapes at a homestay in Kerela. In both rape incidents, the assaults was recorded on the phone with the intention to blackmail the victims. Here, a youth and his female friend checked into the homestay. Eventually the youth was locked out and the female friend was sexually assaulted which was captured on the mobile phone. The culprits also took the girl's gold ornaments and fled in the youth's car, and before fleeing, threatened to upload the video on social media if they complained the police. In order to get his care back the youth had to pay. The youth even had to pay Rs. 100,000 to get his car back. However, he finally went to the police after he was with the release of the video if he did not pay 500,000. After the arrest of the offenders, the police discovered that there was another assault that took place earlier in the month from the images in the mobile phone.[23]

[21] D. Halder & K. Jaishankar, *Teen Sexting: A Critical Analysis on the Criminalization Vis-À-Vis Victimization Conundrums*, The Virtual Forum Against Cybercrime (VFAC) Review, Korean Institute of Criminology (2014)

[22] Avnish Bajaj v State, 2005 3 CompLJ 364 Del

[23] Shaju Philip, *Six youths arrested for 2 'rapes' at Ford Kochi,* The Indian Express (Jan 24 2016, 1:54 AM) https://indianexpress.com/article/india/india-news-india/six-youths-arrested-for-2-rapes-at-fort-kochi/#sthash.Faewe4ni.dpuf

In 2016 in Hyderabad another sordid case revealed shocking details of three years of sexual extortion, exploitation and criminal intimidation of a teenage girl. The youth, who was a college dropout, had intimate video footage of when he was in a relationship with the victim's sister and used this to blackmail and rape the 17-year-old victim in 2012. The victim's senior in college found out about the sexual relationship between her and the college and so started blackmailing and exploiting her for three months. The victim became pregnant but was forced to have an abortion by the second accused. The first accused, in turn, soon started blackmailing her about her relationship with the second accused in September 2015 and insisted that unless she lodge a complaint against the complaint he would release her videos with the second accused on Facebook and further demanded Rs. 100,000. Out of fear she paid Rs.30,000 but finally informed her parents who approached the police.[24]

4.4. HACKING

There are various kinds of cyber-crimes where the youth are both perpetrators and victims but hacking is one of the most prevalent. Hacking is not one action alone but consist of branches, through hacking, there can be copyright infringement or identity theft, etc. hacking has been recognised as deviant behaviour closely with teenagers. The hacking culture has always been appealing to teenagers and youth because of popular culture and movies where hacking skilled was glorified and considered 'cool' and the hackers were essentially teenage miscreants. Un-ethical hacking of course also depends on certain factor in the youth's life like peer influence, family relations, psychological state and subcultural associations.

Initially the term hacker had a positive connotation as a person highly skilled in solving computer problems, however the earlier understanding of who a hacker is has taken a negative turn focusing on the intrusion, theft, violation and sabotage of computer systems. Even the authorities and criminal justice refer to the negative construction of hacking as 'war on computer crime'. Hackers choose to act due to various motivations ranging from intellectual curiosity, self-assertion and thrill seeking, greed and hooliganism. It can also be a form of rebellion against corporate

[24] *Hyderabad: Arrest reveals shocking history of rape, blackmail*, Deccan Chronicle (March 22 2016, 2:08 AM) www.deccanchronicle.com/nation/crime/220316/hyderabad-arrest-reveals-shocking-history-of-rape-blackmail. html

domination and political authoritarianism or in support of expanding the boundaries of knowledge, free flow and exchange of information.

Studies have revealed that hackers are mostly young males, consisting of adolescents and teenagers that lack ethics and moral maturity and have little regard for the impact of their actions. Hacking is a gateway to other anti-social and delinquent behaviour. The relation between online hacking and familial problems must be considered to under why young hackers choose to behave in certain ways. In a study of teenage hackers, it was found that troubled family background was a crucial factor like divorce, parental conflict and alcoholism, physical abuse and a dysfunctional family environment.[25]

In 2014, 13-year-old Wang Zhengyang broke into his school system to get answers for his homework and subsequently called China's 'hacking prodigy'.[26] In 2015 a security breach was experienced by a UK telecommunication company and lost valuable data. The Five suspects that were arrested were all in the age group ranging from 15 to 20 years. It was reported that the company lost up to 60 million pounds due to the data breach.[27]

Hacking is integral to various cyber-crimes, be it pornography, copyright infringement (piracy), fraud, cyber bullying and stalking, pharming, phishing, etc. All these crimes involve taking and using display of specific images, video, document or any other information without the consent of the victim and for illegal activities. It is the blatant violation of privacy. Internet addiction makes a person more vulnerable to hacking. There have been shocking cases of hackers gaining access to webcams of young children and youth and spying on them. Cyber stalking is also a serious issue where the hacker after persistently pursuing a person may feel compelled to hack into the computer system of the victim personal information and images or videos in an attempt to feel 'closer' to the subject. And this may later evolve into a crime of

[25] Dan Verton, *The Hacker Diaries: Confessions of Teenage Hackers* xvii, xviii, 37, 86, 102, 105, 142, 145, 170, 188 (McGraw-Hill Education 1 ed 2002)

[26] Nelson Groom, *Is this the world's youngest hacker? 13-year-old boy hacked into school computer system to get answers to his homework... but says he was only 'testing its weaknesses'*, Dailymail, (October 8 2014, 9:22 PM) https://www.dailymail.co.uk/news/article-2784488/Meet-13-year-old-boy-hacked-school-computer-online-store-insists-hes-using-powers-good-just-trying-fix-websites.html

[27] David Bisson, The TalkTalk Breach: Timeline of a Hack, tripwaire (Nov 3 2015) https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-talktalk-breach-timeline-of-a-hack/

sextortion where the victim is threatened and blackmailed to indulge in sexual activities.

Adolescents have little reservations in approaching strangers or making friends online and social media platforms like facebook, Instagram, snapchat, etc make them even more vulnerable. Hackers choose vulnerable and helpless targets like children and youth when they are most active in social media, video streaming, online video games and chat room. Children are unfortunately good targets due to their high levels of trust in strangers and lack of knowledge in cyber security.[28]

[28] Luis Corron, *Social Cyber Threats Facing Children and Teens in 2018*, National Cyber Security Alliance (Jan 17 2018) https://staysafeonline.org/blog/social-cyber-threats-facing-children-teens-2018/

CHAPTER 5: IMPACT OF SOCIAL MEDIA AND OTHER TECHNOLOGICAL BOOM

Social Media is one of the many results of the advancement of technology today and it continues to grow. An entire social circle or group can be formed on social media without ever meeting in real life. According to a report called *DIGITAL 2020: GLOBAL DIGITAL OVERVIEW*[29] by Simon Kemp in collaboration with 'We Are Social' and 'Hootsuite', there were more than 4.5 billion people that were using the internet at the start of 2020 and there are over 3.8 billion people that use social media and the prediction is that more than half of the global population will be using social media by the middle of the this year. Facebook, Youtube, Whatsapp, FB messenger, Weiwin/ Wechat and Instagram are the top six social media platform of the world. Tiktok is also rapidly growing earning a spot as the 7th most popular.

Social media is often used as a platform to express their opinions and show off their present and past selves. Despite its easy accessibility and creative ways of entertainment, it has a downside that equally worth paying attention to. Social media seems to be a façade of positivity, a mask to hide to real world problems. All that glitters is not gold. Many are so lost in the highlights of someone's life that they do not realise the bleakness of the whole picture. Social media is not only a hunting ground for cyber criminals but also the cause for an array of psychological issues from depression to addiction. The price of constantly being overwhelmed with information causes us to lose the ability to be contemplative and to engage in deep thinking which requires concentration on one thing. [30]

5.1. PSYCHOLOGICAL EFFECTS.

The effect of social media on our mind, mood and emotions is staggering and its ddictiveness also attributes to it. Its association with mental-illness and negative emotions should be a cause of concern to all. A person may start to constantly

[29] Simon Kemp, *Digital 2020: Global digital overview*, Datareportal (Jan 30 2020) https://datareportal.com/reports/digital-2020-global-digital-overview)

[30] Gregoire, Carolyn, *The Internet May Be Changing Your Brain In Ways You've Never Imagined*, The Huffington Post (Oct 9 2015, 8:54 PM) https://www.huffingtonpost.in/entry/internet-changing-brain-nicholas-carr_n_5614037de4b0368a1a613e96?ri18n=true,

compare themselves to others and think less of their own lives. People use social media to show others the highlight reel of their lives and they soon develop a need of constant supply of support through likes or new followers. A study has shown that with the introduction of the internet there is growing number for its usage but a decrease in offline social involvement.[31] Human beings are naturally social creature and to limit our interactions to the virtual world is going against our very nature and a lack of face-to-face interaction can eventually lead a person to depression.

Social media can also lead to Fear of Mission out (FOMO) where a person feels pressured to do what everyone else is doing and to share every life experience on their social media. Apps like Facebook and Instagram exacerbate emotions that others are living a better life or are having more fun than the person experiencing these fluxes of emotions. This can evoke feelings of anxiety and restlessness. High usage of certain social media platforms like Facebook, Instagram and Snapchat can increase feelings of loneliness rather than decreasing it. Sharing endless selfies and posting thoughts about themselves can create an unhealthy level of self-centredness and develop a narcissistic view on life.

The mindless scrolling through different social media platform can become very addictive. The authors of a review study[32] examining previous research done on social media use, psychological characteristics and personality specifically mention that the 'Facebook Addiction Disorder' due to certain addiction criteria in persons who use social media excessively, like "neglect of personal life, mental preoccupation, escapism, mood modifying experiences, tolerance and concealing the addictive behaviour". Once a person stops using social media, they may undergo withdrawals along with feelings of anxiety.

Increase in use of social media does not equate to increased happiness. A study have found excessive use of Facebook has resulted to both less happiness and life satisfaction and because it allowed instant connection with people, instead of

[31] R Kraut et.al, *Internet paradox. A social technology that reduces social involvement and psychological well-being?* 53(9) Am Psychol 1017–1031. (1998)

[32] Daria J. Kuss & Mark D. Griffiths, *Online Social Networking and Addiction—A Review of the Psychological Literature,* 8 Int. J. Environ. Res. Public Health, 3528-3552 (2011).

enhancing the well being of the person like real world social relations, it undermines it.[33]

Feelings of depression and anxiety may be aggravated when faced with conflict on the internet like cyber-bullying or stalking. Various concepts such as self-identity, self-image and self-identity has been popular in its association with social media. Body image issues hit especially harder on the females. One study looks at a survey about online social networking use where body images were collected from over 150 high school students. The students stayed online for an average of two to three hours and it was found that social media usage was significantly related to an acceptance of certain social norms of being thin, having a certain appearance, being dissatisfied with weight, and drive for thinness.[34] Persons can lose empathy since social media stops a person from interacting one on one and the ability to genuinely react to real-life issue that are affecting others.

Addiction to social media can also have physical effects on the body. Social media distorts the perception on what is acceptable. Staying up late browsing social media and texting can lead a person to develop sleep disorders, stress and depression. It also promotes inactivity which in turn results in obesity, diabetes, breathing issues, blood pressure problem among many. Once health deteriorates, a person can become anxious and depressed and the vicious cycle will continues.

The sense of belongingness is crucial in every individual’s social aspect of their life and enables them to feel valued and needed in a group. In todays world, young persons use social media as an outlet to fulfil this need to belong however this can be dangerous because relations formed online are often fickle and the sense of belonging can be temporary.

5.2 DANGERS OF EXPOSURE IN SOCIAL MEDIA

[33] Ethan Kross et. al, *Facebook Use Predicts Declines in Subjective Well-Being in Young Adults,* 8 PLOS One e69841 (2013)

[34] M Tiggemann & J Miller, *The Internet and Adolescent Girls’ Weight Satisfaction and Drive for Thinness*, 63 Sex Roles 79–90 (2010)

5.2.1 Cyber Bullying

Social have externally affected its young users who use it for long extended period of time, making them susceptible to many of its dangers. Social media is also receptive to cyber-bullying where the perpetrators post harmful and mean post about the victim. There have been various research that acknowledges serious consequences of cyberbullying victimization. It is known that both online and offline bullies manipulate the knowledge of the victim's context and sensitivities. Severity and pervasiveness of such actions can cause the victim significant amount of distress, so much so that they become a danger to themselves. For example, victims committing of suicide because of intense cyber-bullying.

Some bullies create fake social media accounts with the purpose of bullying and tormenting the target. The anonymity that these social platforms easily offers is disturbing and alarming to say the least and at the same time poses a challenge to the authorities. Offensive content about a person reaches much faster to a wide global audience with the help of social media and the harm caused to a person by defamatory statements and exposure can have more damaging consequences than verbal statements done offline. Bullying is no longer limited to the school yard or college campuses but is now pervasive and all around us due to technology. Young children are not emotionally and mentally prepared to handle online intimidation and their immaturity also restricts them from fully appreciating the repercussions of what they send others via messenger or post online. A bullied person may also face social exclusion due to the a false rumour or because the other peers fear of also being bullied for associating themselves with the victim.

Internet trolling is another popular form of cyber bullying in the online community, and is especially prevalent in online gaming and social media. Trolling is when discord is created in the internet by upsetting people by posting inflammatory messages or by starting quarrels in an online community. Trolls have spread its toxic nature across the cyber world and have disrupted and made fun of various serious online communities. When messages and images are posted online for entire cyber world to see there is bound to be a person that disagree with what was said. Children and youth must exercise caution in expressing their opinions online especially if it is regarding controversial and sensitive issues.

5.2.2. Cyber Stalking

Cyberstalking is also a common form of bullying. It is a kind of harassment that uses electronic communications to stalk a victim and this poses a credible threat to the victim's safety. The perpetrator may stalk a person for various reasons, like:

- Jealousy, which is a strong motive especially when stalking ex and current partners.
- Erotomania, a mental condition where the stalker believes that the victim is in love with him.
- Obsession and attraction, the stalker could be sexually or mentally inclined to the victim. There is a fine line between admiration and stalking.
- Revenge and Hate, where the internet is the perfect platform for the stalker to vent out his emotions of hate and revenge and this is directed towards the victim whether or not they are the reason for such intense feeling.

New methods of cyber stalking has been created by social media. Cyber stalking can also lead to other cyber crimes like hacking, when the stalker's obsession grows he may feel compelled to dig deeper to find out more about the victim. Social media users also do not think twice about posting about themselves and their every move, the places they are visiting, this makes it very unsafe as anyone can know their exact location. An app called Find my Friends lets you know the exact location of your friends, this can only result in a disaster if this is used for wrong purposes. A lot of young person are also hesitant in reporting incidents of cyber stalking as they do not disclose or get in trouble if there are pictures of under-age drinking or other delinquent behaviours.

5.2.3. Clickbait

Clickbait headline is usually sensationalized encouraging viewers to click a link to an article, image, or video and spreads especially quickly with social media and sharing sites like Facebook and twitter It appeals to the curiosity and emotions of the viewer rather than presenting objective facts. The more views that an article gets the more revenue it generates. For example, a headline reads "The real Reason we don't hear from Joe Pesci Anymore", which sounds quite controversial but on clicking on the link we learn that he simple retired in 1999 and enjoys life from acting. This kind of journalism may be harmless but it is annoying. However, Clickbait becomes an issue when it promoting and sensationalising fake news, and this can be seen as a kind of fraud as well. This is not only a problem for developed countries but for developing countries as well like China and India where there are huge number of internet users.

Clickbait may seem like a minor issue compared to Cyber bullying, pornography, etc but its impact on the mind of the viewers cannot be underestimated as incomplete knowledge is far more dangerous than no knowledge at all. Such news are read by gullible viewers and spread through their social media accounts. It can even foster hate speeches and in some extreme cases, violence. It can spark heated debated among the online communities which is sadly based on fake news. Knowledge is always evolving but at the same its fake version is too.

5.2.4. Grooming

Grooming is act of luring a child to prepare them sexual abuse and exploitation through sexual conversations, or to prepare a child for violence and terror through religious or ideological conversations, or prepare them for drugs and other illegal activities. The act of trapping a child is as easy as starting chats with through popular social media sites and once they are accepted as a 'friend', personal information of the child is easily obtained by the groomer. Instagram has become the biggest social media platform to groom young children. It is an additional danger when a child or youth has an open profile as it makes it much more convenient to the groomer to trap the young person. The groomer may also adopt a fake identity to appear younger or as someone the child recognises and offer them advice and gifts to build their relationship.

BBC UK reported that Instagram has been used as grooming platform more than another social media sites. The Police in England and Wales in six months to September 2018 it recorded 1,944 incidents of sexual communication between the child and the groomer, where 32% of the total cases occurred in Instagram, Facebook at 23% and Snapchat at 14%, and in one a girl, when she was 13 years, was groomed by a 24-year-old man. He first posed as a 16 year old, which then changed to 18 years, and the texts they exchanged soon became sexual but he quickly became indifferent and dropped her off after their first sexual encounter[35].

[35] BBC, *Instagram biggest for child grooming online - NSPCC finds*, BBC news (1 March 2019) https://www.bbc.com/news/uk-47410520

Child grooming have also increased in India with the advent of the internet. In 2017, a 13-year-old girl from Tirupur was lured and raped by a 21-year-old man in Chennai. The victim was first befriended by the rapist on Facebook, and after he had gained her trust he sexually assaulted her. Similarly, the previous year saw the kidnapping and rape of a 15-year-old girl by two teenagers whom she befriended on Facebook.[36] With the expansion internet and use of social media, incidents of child grooming for sexual exploitation can only be expected to rise in future.

5.2.5. Glamorisation of drug use and self-harm

Unfortunately, social media does not have an effective or efficient filter with regards to the contents that are posted online. Content about drugs and self-harm have made its way to the smart phones of the younger population. This exposes and also provides new opportunities for children and young adults to entertain the idea of drugs and self-harm. Adolescents are uniquely vulnerable to what they see on social media as individuals in this age group are also highly susceptible to peer pressure and influences. Sites like Facebook, Instagram and Snapchat easy allows exposes them to normal or famous people consuming drugs and alcohol. If they see their favourite celebrity or role models doing drugs, they may feel an inclination towards it too. At the same time, such risky behaviour is also seen in their family and friends. Thus, this kind of content online normalises and glamorizes wrong and illicit behaviour, making teens and young adults believe that it is appropriate to do the same. The National Centre in Addiction and Substance Abuse of Columbia University conducted a survey in 2011[37] and found that the regular use of social media outlets were more likely to lead a teenager to take drugs, drink and buy tobacco as compared to adolescents who did not use social media or did not use it at all. Two thousand adolescents took survey and when asked about their habits on drug use and social media, out of which 70% said they used social media regularly. Researchers found that these group of adolescents were:

- Five times more likely to buy cigarettes

[36] Devika Agarwal, *Child grooming: India must take measures to protect children from online sexual abuse* (May 11 2017, 21:59 PM) https://www.firstpost.com/india/child-grooming-india-must-take-measures-to-protect-children-from-online-sexual-abuse-3438528.html

[37] QEV Analytics, Ltd. Knowledge Networks, *CASA National Survey of American Attitudes on Substance Abuse XVI: Teens and Parents*, National Center on Addiction and Substance Abuse at Columbia University, 5 & 7 (2011)

- Three times more likely to drink
- Twice as likely to use marijuana

Also, teens who had seen pictures of other teenagers drunk, passed out or using drugs were at an increased risk of substance abuse. They were

- Three times likelier to have used alcohol.
- Four times likelier to have used marijuana.

However, when it comes to social media and drugs, the problem is two-fold. Social media does not only promote drug abuse but also provide drug dealers an online platform to sell drugs. Therefore, teens and young adults are not only the buyers but the drug dealers as well or they facilitate and refer the interested customer to a dealer.

There are special online communities on social media sites that promote pro-harm behaviour. For example, Pro-ana and pro-mia communities promote and encourage eating disorders and also provide tips to their readers and members on how to become ‘better’ anorexics. As a precautionary measure they state that these communities are only for people who have an eating disorder and also include a disclaimer stating ‘If you do not have an eating disorder then it is better for you if you do not develop one’. At the same time, they encourage a sense of belonging and pride in being a part of such a community, and suggest different ways to amplify the eating disorder and absurdly celebrate it as a form of empowerment, liberation, perfection and superiority achieved through the ‘power of will over body’ and self-control. These communities are the antithesis of recovery.[38]

Studies have shown that those who wish to engage in self-harm behaviours (e.g., cutting, burning, attempting suicide) may not find social validation for that in the real world but may find acceptance in the online context.[39] These kind of site romanticises suicide and self harm and see it as a means of escape but not as something wrong. Adolescents and young adults that suffer from depression are especially susceptible to this kind of communities, where they are received with support and ‘care’, even though they are being encouraged to end their own lives. Different ways of ending

[38] Claudia Megele & Peter Buzzi, *Safeguarding children and young people online: A guide for practitioners*, 196 Policy Press (2017)

[39] Janis L Whitlock et.al, *The virtual cutting edge: The internet and adolescent self-injury*, 42 Dev. Psychol 407-17 (2006)

one’s own life are taught by online suicide communities or they connect them with others who have already attempted killing themselves. Social media offer such persons a sense of visibility in their invisibility.

5.2.6. Online gaming

Most online games are extremely aggressive and violent in nature, often involving war scenarios where the player must kill the enemy. This eventually effects the behaviour and personality development of the child and youth playing it. The gaming community is similar to social media in terms of displaying negative traits like bullying, trolling, cheating etc. Online gaming allows player from all over the world to connect and communicate with one another. The danger in this lies in the fact that not everyone participates in online gaming with the intention to play as there are various predators and paedophiles that are on the prowl waiting to approach their prey. The video game market is worth a staggering $138 billion, this draws in cyber criminals looking to scam and fraud young gamers. Hackers are also ever-present in the online gaming community ready to commit their phishing scams that have become common place in the gaming world and one of the methods used are Account takeovers (ATOs) where they hide behind real accounts to engage in abusive behaviours, post spams and scams. These hacker/fraudsters acquire another gamer’s login either by purchasing them from the dark web and use stored payment information to make illicit purchases.

Addiction is another common feature associated with gaming, where gaming addict even skip classes to play games with their friends and soon their academics plummet and depression sets in. However, they continue to play as a mean of escape, it is a vicious cycle of hopelessness. This addiction can also manifest itself physically in the form of fatigue, migraines due to long and intense eyestrain, carpal tunnel syndrome due to overuse of the controller or computer mouse to name a few.

Gaming has different outcomes depending on intention or reason for gaming. When a person games to find escape from reality, or gain status, or simply because of demands from others leads the gamer to a higher probability of negative social consequences, like getting less sleep, less time to do school assignments, and also having conflicts with parents and/or siblings. On the other hand, if a person does gaming for fun or has social intentions then the probability for negative social consequences is reduced.[40]

5.3. AI AND ITS IMPACT ON THE FAMILY STRUCTURE.

Artificial Intelligence is said to be the simulation of human intelligence processes by machines, especially computer systems. It has immense potential to dictate how brands manage and create social media marketing. The use of AI in business has become more common and social media is no exception. It is considered as the way forward and its footprint are found all over facebook like neutral learning network, tagging and recognition of images. But what does that mean for the larger population? Social media has already penetrated into the lives of its user and with the coming of AI, will societal relations collapse with technology imitating humanlike emotions and responses? For better understanding one must look at the existing relationship between AI and society.

AI are programmed to accomplish certain goals by itself and has the ability to evaluate, process and even think. It can even be programmed to handle everyday tasks like monitoring the home via smart home systems. Even the AI algorithms in social media gathers information that may interest of the users and this can make a person addicted to the carefully curated social media feed. This simple browsing may take up hours, resulting in user forgetting to nurture family relations. Social media is becoming more personal with every use and because of our favourite topics are so accessible now, a parent may lose the ability to teach his child about hard work.

There is a growing dependency on AI for our daily activities with hopes of making lives easier, but what if it makes it too easy. Won’t people forget the virtues of hardwork? The simple joys of life would be buried beneath the technological wave that’s taking over. When it also comes to a love and affection, no robot or AI can replace families and friends. Dr V.S. Natarajan, known as the Father of Indian Geriatric said “While machines can fulfil daily requirements, I am sceptical about whether they can provide the care and empathy that geriatric patients require.” He

[40] C Hellstrom et. al, *Influences of motives to play and time spent gaming on the negative consequences of adolescent online computer gaming*, 28 COMPUT HUM BEHAV. 1379–87. (2012)

goes on to say that even though a robot can physically touch a body, it is incapable of expressing and interpreting feelings.

While India is still warming up to the idea of a robot care giver, Japan has created a robot 'ROBEAR', an experimental nursing care robot. The main challenge in India is the nuclear family set-up. Leaving senior citizens in genuine human care rather than leaving them in the care of a cold robot may be considered as a good kind of constraint.

The age of personal digital assistants is gaining ground and is encouraged and liked by the tech communities and also by persons that are too occupied with work. There is much potential for AI to affect the family structure very differently right to its foundations. AI has just started and yet the impact it has already made is seen everywhere. Soon, family connections will be lost, the virtual world will be preferred over reality. AI to a large extent promotes escapism.

AI like Alexa and Siri have special interactive feature where they can have simple and casual conversations. When we converse with these digital assistants, we bring them closer to our own level.[41] The companies responsible for its creation has grand ambition to occupy every space: home, car, office, etc. There is a high possibility that everything at home including the mundane activities will be taken over by AI. In the name of convenience human being may lose the ability to take care of the most basic tasks. Their capability of having simple conversations may be upgraded in the future to more meaningful and fulfilling talks, while this is extraordinary it also poses a danger to the structure of family. Members of the family may prefer to converse with technology rather than actual people.

Digital assistants are known to record our conversations, images and other sensitive personal information, including location via our smartphones which they use for machine learning to improve themselves over time. But what about the safety of these person? Are we really safe with a piece of technology absorbing our everyday routine. In one case, a couple in Oregon was forced to unplug their Alexa after their private

[41] Judith Shulevitz, *Alexa should we trust you?*, THE ATLANTIC, (November 2018), https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844/)

conversation was recorded and sent to someone else on their contact list.[42] Amazon explained that they must have spoken certain key words that triggered it. However, AI acting on its own without instruction is a cause of concern and a potential for more mistakes like this in the future. The concept of respecting a person's privacy is not known to AI and they simply do what they are programmed to do.

5.4. QUITTING SOCIAL MEDIA

While some are happy with perks that social media is offering, others are irked by its extensive exposure and therefore choose to quite social media entirely. Millennials are especially deciding to delete their account in social media sites mainly due to the fact that a huge part of their lives was starting to depend on it and eventually was starting to use social media extensively, from communication and entertainment to news and therefore becoming intrinsic in their life. They are in need of digital detox from all that social media is causing in their lives including depression, inferiority complex, unproductivity and materialistic mentality.

No sane person would consciously want to spend hours on social media and see what other people think about them but such behaviours are addictive behaviours and once a person is trapped in such a loop, it is difficult to break free. There is a need to take control of these devices and machines and used them for their proper ends. This growing trend of young persons choosing to quit social media is an attempt to be more present in the real world, it can also be seen as a rebellion against the fact that social media, in deep and pervasive ways, dictate and promote certain social behaviours. A break from social media can be seen as positive sign of taking care of mental exhaustion and refreshing the mind and refusing to let technology and social media dictate every sphere of our lives.

[42] Rozita Dara, *The dark side of Alexa, Siri and other personal digital assistants*, THE CONVERSATION, (Dec 16 2019, 12: 34 AM) https://theconversation.com/the-dark-side-of-alexa-siri-and-other-personal-digital-assistants-126277

CHAPTER 6: LEGAL APPROACH

6.1. LACUNAE OF EXISTING LEGAL FRAMEWORK.

How effective have the law been in tackling cyber-crimes against children and young adults and cyber delinquency? While there have been various legislation to address these types of crime, it has not been efficient and sufficient enough in serving justice. We will look at the national and international laws and policies and examine whether they have been successful in protecting children online and also look into the gaps it still has despite progress made.

6.1.1. National framework

The policy and legal framework for cybersecurity in India is evolving. There are various laws that addresses or implicitly deal with cyber-crimes and online protection of children. Young adults due to their maturity will be dealt as according to the law and POCSO will not be applicable. However, adolescents are dealt with specially by the law. The applicable enacted laws for cyber-crimes are:

- Information Technology Act, 2000.
- National Cyber Security Police, 2019
- Protection of children from Sexual Offences (POCSO) Act 2012.
- In Penal Code (IPC) 1860
- The Indecent Representation of Women (Prohibition) Act, 1986
- The National Policy for Children (NPC) 2013

While these laws are established to combat cybercrime against children, awareness is still lacking among parents, teachers, police and policymakers. Any effort by the government to strengthen online child safety must necessarily must go hand in hand with knowledge of the law, and its robust implementation and ultimately, comprehensive legislative review.

The case discussed earlier in *Avnish Bajaj v State*[43] or the Delhi MMS Scandal of 2004 two 17-year-old of a well-known school in Delhi is a benchmark for cyber-crimes involving children. This incident led to the questioning of the efficiency of the IT Act, 2000 and subsequently, its amendment.

[43] 2005 3 CompLJ 364 Del

Many online offences that have been criminalized in other countries are not considered as offences by the Indian law like sexting and cyberbullying. Legal provisions to deal with cyberbullying are lacking. Child trafficking is generally penalised but when children are trafficked for the purpose of producing child pornography and online ad for sex tourism, the law is unclear or does not exist at all in this regard. Due to the potential for misusing the law, the establishing of criminality of sexting and grooming is difficult and most unlikely desirable. Children and adults must be educated in exercising caution online and especially be made aware of the dangers of online grooming as grooming may be a gateway to other potential harm. Children must understand that sexting or voluntarily sending nude pictures to strangers online can be very harmful as self-exposure can enhance a child's vulnerability.

Privacy: When it comes to online safety of a child, there is a lack of clear guidelines for the law enforcement to follow. Therefore, while interpreting legal provisions there may most likely be conflicts. It is difficult to balance both the protection of the adolescents on one scale and their right to privacy on the other, but instead it has been pitted against each other. Protection of children's safety online often requires proactive steps, including surveillance, which always translates into the intrusion of the child's right to privacy. When it comes to children that are accused of cyber offences, i.e., cyber delinquents it is essential to develop approaches that do not criminalize children and adolescents.

The IT Act 2000 needs to exercise more stringent measures with public cyber cafes. Pornographic websites can easily be accessed in cyber cafes and so a mere notification to prevent the users to visit the pornographic websites will not be enough. According to the IT (Guidelines for Cyber Cafe) Rules, 2011 the cybercafes are must immediately report to the concerned authorities if there has been an access to any pornographic material online or simply have any reasonable doubt or suspicion of the same. However, in the absence of supervisors, these rules do not have the desired effect and with poor monitoring there is no information on how useful these guidelines are.

No uniform terminology: There is a lack of uniform terminology on online abuse and exploitation of children. A clear definition is necessary for better understanding and effective public discourse on these issue. This in turn would result in a better application and interpretation of law and enable the framing of extensive legal protection. When uniform terminology is absent in law it aggravates the already lacking framework in criminalising complex online child abuse and exploitation and such absence becomes an obstacle in protecting the child. There should be no disagreements in this regard as it will only further confuse and creates challenges in the formulation of policies, intervention legislation and public advocacy.

A careful application of the existing legal provisions may provide a way out. For example, the legal provisions for intimidation and harassment applied in cases of sexual exploitation for pornography and cyberbullying. But we must not look over the fact extraterritorial jurisdiction is not recognised by law when the victim of a child pornography offence is an Indian. When children is also the perpetrator in child pornography, their criminal liability is not mentioned in the law. The existing legal framework also does not establish whether the proceeds acquired from the sale of child pornography should be requisitioned.

Next, is a matter of child's consent which is a contentious issue. The law has mentioned that consent of children under 18 years, in matters of sexual abuse, do not arise. However, in the trend of sexting and sharing of selfies between teenagers, both sides are be willing in such exchange and when it later develops into when exploitation, the question on liability arises. Will both parties be treated as victim and be guided and counselled or will they be criminalized for their risky online behaviours? The law is yet again unclear in this regard.

Need for Amendment: There is a dire need to amend the existing legal framework as it does not adequately address the issues of child trafficking. Even though the overriding effect of the provisions of the Information Technology Act prevails when there is any inconsistency with the provisions of the POCSO Act or IPC, it lacks sufficient teeth in providing comprehensive protection to children. Considerable and deliberate effort is required in reviewing the IT Act so that these problems will be efficiently addressed during the detection, investigation and prosecution of child online abuse.

Legal Provisions and its subjective interpretations: a subjective interpretation must be opted for when applying legal provisions for online safety of children and also when dealing with cyber delinquency. Such interpretation is helpful in this current scenario when there is a lack of guidelines for Indian law enforcement agencies, including forensic labs for cyber cases which means that here are insufficient tools or devices needed to facilitate the investigation of digital evidence pertaining to illicit images/videos of sexually exploited children. Furthermore, there is difficulty in proving the age of the child when the victims are not available on images and videos.

Minors as cyber criminals: The Information Technology Act, 2000 only portrays the child as the victim of online sexual abuse and exploitation and does not sufficiently address cases when children are the offenders. The amended Juvenile Justice (Care and Protection) Act, 2016 states that if a child is above16 years of age and below 16 years if age and commits a heinous crime, they may be tried as an adult if Juvenile Justice Board recommends it.[44] It is, however, silent on cases about children committing cyber offences. Many underaged children open social media accounts even if they law bars them from doing so and this is usually done without the parent's consent. The minimum age to register is 13 years in Facebook and this is a standard form of contract for other social networking sites. However, according to the Indian Contract Law, only when a person completes the of 18 can he enter into a contract. Entering into a contract by falsifying the age would amount to misrepresentation under the Indian Contract Act.[45] And under the IPC misrepresentation of one's own identity is an offence. These legal provisions can also be applied to the virtual world. The consequences for children when they misrepresent their identity and a parent's abetment need to be seriously considered when such cases are being reviewed by the Juvenile Justice Boards.[46]

An uneasy co-existence of IPC and IT Act for hacking: There is an overlap between IPC and the IT Act which may sometimes be hard to solve, for example, certain offences are non-bailable under the IT Act but similar offences under IPC are bailable and vice versa. Similarly, certain offences are non-compoundable under the IT Act and compoundable under IPC and vice versa. In cases involving data theft and hacking,

[44] Section 15 of the Juvenile Justice (Care and Protection) Act, Delhi, 2016.

[45] Section 18 of the Indian Contract Act

[46] Kesavamoorthy, R., *Legal Study on the Protection of Children in Social Network: Special Reference to Indian Law*, 15 IOSR-JHSS 16-21 (2013)

Sec 43 of the IT act speaks of the punishment for destroying a computer system through a virus or contaminant but is compoundable however sec 425 of IPC which speaks of mischief, that is intentionally destroying a person's property, it is non-compoundable.

Furthermore, in the offence of receipt of stolen property, section 66B of the IT Act talks about the punishment for it but it is a bailable offence. However, under sec 411 of IPC, which also talks about the receiving stolen property, the offence is non-bailable. Similarly, when it comes to identity theft and cheating by personation, the punishment prescribed under 66C and 66D of the IT Act are compoundable and bailable while the offences of forgery mentioned in sections 463, 465 and 468 of the IPC are non-compoundable and the offence of cheating under sections 420 and forgery in sec 468 of IPC are non-bailable.

Finally, offences of obscenity mentioned in sec 292 and 294 of IPC are bailable, while offences of the same nature mentioned under sections 67, 67A and 67B of the IT Act are non-bailable. Sec 408 and 420 which deals with breach of trust and cheating, are non bailable and non-compoundable unless the permission of the court is taken to kake them compoundable, this was held by the Bombay High Court has dealt with this issue in *Gagan Harsh Sharma v. The State of Maharashtra*[47]. However this is in conflict with offences relating to damage to or tampering with computers or any offences related to the computer under sec 43, 65 and 66 of the IT Act which are bailable and compoundable.[48]

6.1.2. International Framework

The international legal instruments seem to be outdated when compared to the fast-changing and new methods of child exploitation through technology. In some instance, a few of the key legal instruments precede significant technological advances. For example, the leading children international instrument UNCRC, in one

[47] 2019 CriLJ 1398

[48] Vinod Joseph & Deeya Ray, *India: Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence,* MONDAQ (Feb 10 2020) https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence

of its Optional Protocol[49] prohibits the sexual exploitation of children but does not criminalize live-streaming videos of child sexual abuse or online sexual grooming.

The Luxembourg Guidelines is a global terminology guideline which is available to all major child protection organisations and agencies around the world, including the media and lawmakers. These guidelines consist of standard

These guidelines have introduced standard interpretations of terminology relating to sexual abuse and exploitation of children. Through practical guidance on how to use these terms including their online dimensions, it strives to enlighten the discourse and joint effort in the backdrop of a common framework for child protection.

In the contemporary global legal scenario, the UNCRC basically dictates the rights of the children all over the world. The prima facie problem is that there are no rights explicitly prescribed to the children in cyberspace by the UNCRC. Hence, on the surface, it appears that the children lack any sort of enforceable legal rights in the cyberspace. International law with regards to the child online protection lacks policies on cyber literacy and resilience cyber know-how

Due to the high complexity, fast-changing and transnational nature of socio-technological infrastructures challenges international and national policy-makers. It is also problematic when the internet is largely blind or disregards the criteria of age, as this treats children and adults equally and instead of treating children according to their "evolving capacities", as required in the CRC articles 5 and 14. This concept of "evolving capacities" recognises the growing responsibilities of a child and therefore encourages a child to make their own decisions according to their capacity and competency.

There is a lack of international instruments for cyber crimes concerning sexual exploitation and abuse of children. The first and only existing convention at the moment is the Budapest Convention for combatting cyber-crime. However, India did not opt to become a party to the treaty mainly on two grounds:

- It did not participate in the drafting and

[49] UN General Assembly, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 16 March 2001, A/RES/54/263,

- The convention through art. 32b allows for transborder access to data and thus infringes on national sovereignty.

This treaty seeks to harmonize nationals law, improve investigation techniques and increase cooperation among nations. The problem that has always plagues international law and has acted an obstacle in the fully implementation and realization of the any international instruments and treaties is that it lacks teeth. When a state party has breached its obligations or have failed to perform them, there is no real sanction in the sense that, there is an absence of penalisation. At the most, they are shamed and ostracized by the global community but that does little in the context of individual rights.

The burden of actual execution of cyber laws for online child protection is then placed on the states. What is must be then analysed is the role of individual sectors of society and for this the Government has a major responsibility. The mammoth role of effectively enforcing children's rights in a civil society is placed on the shoulders of the Govt. This is also where NGOs and national human rights institutions have a part in the protection of children's rights in the cyberspace. For example, in the crime of revenge porn the question is of how best to frame the its criminalization within the Convention and whether or not victims will receive justice? However, the process has not only been slow but also lacks uniformity and is sometime more or less a matter of chance, left to the laws of states and/or jurisdiction, irrespective of whether they have any law applicable to the subject at all. Enough time has lapse to solidify Non-consensual Porn (NCP) as a serious cybercrime and take effective global action to come up with a solution. One way in achieving this goal is to integrate NCP with the Budapest Convention on Cybercrime in order to provide global guidance on this particular issue and encourage uniform standards of criminalization.

Japan has passed the Revenge Porn Prevention Act in 2014, criminalizing "the provision of a private sexual image of another person without the person's approval via means of telecommunications to an unspecified number or to many people", with imprisonment up to three years as provided in article 3 of the Act.[50] Moreover, France's Penal Code has also been amended to prohibit the unauthorized circulation of sexually-explicit recordings, which is punishable with imprisonment up to two

[50] Sayuri Umeda, *Japan: New Revenge Porn Prevention Act* (Nov 26 2014) http://www.loc.gov/law/foreign-news/article/japan-new-revenge-porn-prevention-act/

years in jail and/or a hefty fine.[51] 2014 saw the state of Illinois in the United States make the intentional “non-consensual dissemination of private sexual images” an offence and is punishable with imprisonments up to three years and a fine up to $25,000 fine.[52]

Keeping these frameworks in mind, an additional protocol with regards to the criminalization of NCP should be disseminated through computer systems. Criminalizing NCP is riddled with challenges in all parts of the world but its victims deserve an effective solution that acknowledge their real harm and punishes offender effectively.

The Yokohama Global Commitment 2001 provides a framework for action at national and international levels to eradicate commercial sexual exploitation of children. In the *Report of the Second World Congress against Commercial Sexual Exploitation of Children* by the General Rapporteur, Professor Vitit Muntarbhorn, it was stated that the effective implementation for guarantee of child rights is particularly challenged by five C's “Crime, Corruption, Collusion, Clientelism and Complacency”. Commercial sexual exploitation of children is ever changing and intensifies with each alteration in its nature. It has becomes both national and transnational. International cooperation continues to be an issue with the prevalence of some negative traditional practices in some countries (eg. child temple prostitution by Devadasi system) and also crippling socio-economic conditions of certain countries leading to exploiting children for financial gain. The report also mentioned the Declaration of the Arab-African Forum against Sexual Exploitation of Children which stated the fact that the problem of sexual exploitation of children remains a taboo in numerous countries. It is only though concerted effort globally and locally that the taboo can be broken

As long technology continues outgrow the legal spaces, effective laws at the international scale will be in want. This is especially true in dealing with young hackers or young victims of hackers. The prevalent problem is that in identifying the exact origin of the cyber-attack is extremely difficult. The characteristics of cyber

[51] Nicolas Boring, *Online Privacy Law: France*, *Library of Congress*, (updated 4 may 2018) https://www.loc.gov/law/help/online-privacy-law/2017/france.php

[52] Kim Bellware, *Illinois Passes New 'Revenge Porn' Law That Includes Harsh Penalties* (31 Dec 2014, 12:29 PM) https://www.huffingtonpost.in/entry/illinois-revenge-porn_n_6396436?ri18n=true

space which is anonymity and lack of boundaries makes it hard for states to identify accurately the perpetrator responsible for a specific cyber attack.

So, what is the response of the State to a cyber-attack? Legal complexities are difficult to sort out even if legal attribution is established. International law affords a state only few mechanisms respond effectively to a cyber-attack once it has occurred. Only in armed attacks is a state allowed to use force in self-defence as a response. In this context an armed attack refers to only the gravest use of force. Therefore, It is highly improbable that crimes of cyber espionage whose aim is primarily on gathering data or intelligence could ever be described as an armed attack under this definition.

Similarly, while under certain circumstances international law allows countermeasures, they are of limited use in the context of cyber-attacks because of the conditions imposed. For example, except in urgent circumstances, the injured state must notify the decision to take countermeasures to the state responsible for the cyber-attack and also offer to negotiate with them before any countermeasures are actually taken. However, considering the speed and reach of such attacks these procedural requirements only prove themselves to be impractical when responding to cyber-attacks.

6.2. ASSOCIATION OF CYBER CRIMES WITH AGE

Are adolescents and young adults at a certain age more susceptible to either being the perpetrator or victim of cyber crimes? The attribution of age does have a certain sway as adolescents and young adults may have a juvenile interest in cyber-crimes with its intention often being to simply impress their peers. Especially with adolescents, where peer influence is most felt at this age. The factor of immaturity here makes the young offender to be reckless and ignore the consequences of the crime.

At the same time because of the gullible nature and minority of adolescents they make easy targets. It is evident that in recent hacking cases young people have been arrested. According to behavioural sciences, it is well established that throughout the formulative teenage phase impulsivity and risk-taking behaviour increases. Supporting this there are numerous reports indicating the increase in involvement of youth in online criminal activity. The Australian Bureau of Crime Statistics and

Research in 2015 reported that in the previous two years cyber fraud offences committed by people under 18 years of age had jumped by 26% and 84% in the previous three years.

However, the commission of cyber-crimes is not strictly related to age, there are other factors and reasons why an adolescent or young adult chooses variant behaviours online. The peer influence, family environment, socio-economic factors must be taken into serious consideration. For example, one must also look at the adolescent and development psychology as this approach helps in understanding the general behaviours and maturation of teenagers. This includes factors that can influence anti-social behaviour and criminality, such as impulsivity, mood disruptions and problems with authority. Similarly, understanding development of morals and the internalising of attitudes, norms, subjective beliefs and the establishment of identity whilst in a state of role confusion, arguably compounded by differences between real-world norms and moral judgements, and those that prevail online.

A study was held based on the national crime records bureau from the year 2008 to 2012. It was found that age group 18 to 30 years had a crime record of an alarming 6173. People belong to this age are normally college students and young working adults.[53] Therefore, it is not necessarily only children that take up cyber-crime, however with young adults the intention may be different. In adolescents, hacking or surfing through illegal content, etc may have been simply our of curiosity or to impress friends or an attempt to fit in with their social peers, however as an adult, the motive may be more serious like financial gain or a larger and more complex conspiracy in motion.

As technology advances and electronic devices become cheaper, it is possible for anyone at any age to own a mobile phone, and with that, social media then becomes easily accessible. It then becomes a convenient platform to take advantage of other young people. Cybercrime if done carefully is thought to be easy money, which is not surprising as the damages cost by cybercrimes are anticipated to cost 6$ trillion per year by 2021. According to cyber statistics, the United States holds the first place for

[53] Sankara Moorthy et. al, *Analysis of Indian cybercrime dataset for age demography*, 10 , INT. J. APPL. ENG. RES. 1855-1861 (2015)

cyber security attacks[54] and another study states in 2015 that the average age of suspected cyber criminals featured in investigations was 17 years old.

There was a study done based on the data from the press releases of the U.S. Department of Justice between January 2009 and December 2017. It included a sample of 225 offenders who were citizens of a foreign country and have been involved in 123 cases in which 414 crimes were committed. It was found that the minimum age of cyber offenders is 19 years and the maximum is 73.[55]

Studies have shown that "stereotypical" perpetrator of a cybercrime is "male, 12-28 years old, single, and socially dysfunctional, possibly from a dysfunctional family".[56] However, the study also adds that these particular components are not the most essential in determining a profile for cybercriminals; rather, understanding the context guiding the unlawful activities is more important. It is also essential to focus on individualized profiling by to collecting information about the perpetrator's level of technical skill, their social characteristics, personal traits and their motivation.[57] some citizens of other nations also frequently commit cyber fraud and most of them are males below the age of 30, this supports the findings of the average cyber offender.[58]

However, considering the age alone with be an inaccurate assumption. Age alone cannot determine the criteria for cyber delinquency or victimization, while it does hold considerable weightage, it is not a stand-alone factor. Cyber crimes does seem to pull in a younger population because of their vulnerability and curiosity over the limitless cyber world but when pursuing children who are caught up in cyber crime whether they are the perpetrators of victims, it would be more effective if other factors are examined, especially their perspective on their worth as a person and the peer and family influences. Therefore, age and the other ingredients of cyber delinquency and victimization must go hand in hand.

[54] Casey Crane, *Eye-Opening Cyber Security Statistics for 2019*, HASHEDOUT, https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/#cyber-security-statistics-victim-data-and-compromised-records-%E2%80%94-by-the-numbers

[55] Lora Hadzhidimova & Brian Payne, *The profile of the international cyber offender in the U.S.*, 2 (1) IJCIC 40-55 (2019)

[56] M. K. Rogers, *The psyche of cybercriminals: A psycho-social perspective*. in *Cybercrimes: A Multidisciplinary Analysis*, 217-235. (Springer-Verlag Berlin Heidelberg 2011)

[57] Saroha R, Profiling a cyber criminal. International Journal of Information and Computation Technology, 4(3), 253-258 (2014)

[58] Warner J, Understanding cyber-crime in Ghana: A view from below. International Journal of Cyber Criminology, 5(1), 736-749. (2011)

CHAPTER 7 - FOR A BETTER AND BRIGHTER FUTURE

7.1. EDUCATION AND AWARENESS

One of the key gaps identified is the lack of understanding among policy makers, professionals and society as a whole of the threats and risks posed to children by social media and information and communication technology. Children often indulge in various risky behaviours online and this is undetected by unsuspicious parents. Early exposure to social media and technology has made them more proficient at using technology in their daily lives than their parents.

In a research on urban Indians, it was found that parents and children are concerned about online risks equally like sharing of personal information and its consequences and contact with strangers online. There is a somewhat vague but general awareness of the prevalence of risks online by the parents and children but children show a wider range of awareness of those risks. This is because children are now habitually seeking information online for assignment or leisure, as well as conversing both offline and online with their peers.

In prevention of cyber-crime, creating basic awareness is one of the simplest and easiest ways to significantly reduce the effects of various forms of fraudulent social engineering. Mostly due to a poor cyber hygiene and lack of awareness, there is a risk of cyber frauds occurring. Cyber awareness campaigns that are innovative and appealing can help in this regard. It is the duty of these campaigns to inform, the citizens about the most recent cyber-crimes, as a way of making them seem more real to the general public and also provide them means to tackle it. Sometimes there is a the fear of being ridiculed or harassed for reporting certain cyber-crimes, so these awareness campaigns should encourage them to report all incidents of cyber-crimes.

Both adolescent and young adults need to be educated on exercising caution in the cyber world, especially when it came to dangers of grooming, as it can lead to other potential harm. Furthermore, their vulnerability is enhanced through sexting and self-exposure. The laws addressing sexting and self-exposure remains in a grey area, while the law specially forbids obscene language or text.

Youth should then perhaps be educated through youth training centres or sensitized through mandated classes on social and law studies in order to understand and recognise the destructive effects of piracy, fraud and other Internet crimes. In order to understand the emerginf technologies emerging in the market better, the learning institutions like universities, colleges and schools should appoint their IT staff and system administrators in annual training, since technology is ever evolving, it is not enough to know but to be updated and ready.

Unfortunately, instead of having a proactive approach most organizations and individuals have a reactive approach to information security. Usually it is only after an attack that the system's vulnerability is evaluated which only results in expenditure that could have been avoided, money is spend on recovering lost data and business and fixing the security holes. This approach is expensive and ineffective. What must be emphasized on is physical data security in order to prevent unethical data loss, meaning confidential information must be securely locked securely from unauthorized users. Additionally, potential threats should be looked into by all technology and young people should be given special attention by showing them how to practice safety and responsibility online.

Still, most children and parents seem to not be able to grasp and understand the full extent of online risks. For example, parents in the United States largely seem to be satisfied using offline means in protecting their children online and not using any of the available online apps and tools. Indian parents show similar behaviours. Norton Security, a firm that provides online security and protection, found that young adult Indians were less aware of online risks when compared to the global levels of awareness of online risk because of the "it won't happen to me" syndrome. This misplaced confidence only aggravates the online risks faced by children.

Experiences from other countries show that children and young people have a large role to play in safeguarding themselves and their peers from child online abuse. Examples of a few promising practices include the constitution of peer groups in schools called cyber congress, scouts or cyber security ambassadors. However, such practices have not been properly documented in India and there is little understanding of how digital literacy and safety programmes can be implemented effectively

UNESCO promotes the fostering of a digital citizenship.[59] The widespread use of ICT also means that there is an urgency in reducing and addressing the risks associated with it like online abuse and threats, misuse of information and harming mental and physical heath, while simultaneously learning how to responsibly use these technologies and the opportunities it offers. Functioning in a digital world means being aware of the risks involved and also leveraging the benefits of ICT by being equipped with the appropriate knowledge and skills. It also helps teachers, leaders in the technological field and parents to use technology appropriately and responsibly and in turn teach the young internet users. The digital citizenship education adopts a proactive approach that prepares the child for current challenges and with the support from schools, parents/guardians, teachers, policy makers and other key stakeholders, fostering a favourable environment to encourage safe and responsible use of ICT among children and youth will be made possible. Therefore, digital citizenship education constitutes of:[60]

- Internet safety
- Cyberbullying and digital drama
- Information literacy
- Privacy and security
- Self-image and identity
- Relationships and communication
- Creative credit and copyright
- Digital footprint and reputation

7.2. POLICIES NEEDED AND STEPS TO BE TAKEN

Keeping in line with national interest every country has enacted its own cyber laws. The necessity of multinational conventions dealing with cybercrime is vital in ensuring legal rigor is coupled with investigation and subsequent for bringing cybercriminals to justice. It is well known by now that cyber-crime is a growing threat

[59] UNESCO Bangkok & Asia and Pacific Regional Bureau for education, Fostering Digital Citizenship through Safe and responsible Use of ICT (2015)

[60] UNICEF, Child Online Protection in India, 75 (2016)

to society and commission of it by a minor it poses a threat to the future of the state. Therefore, it is of paramount importance to task the concerned authorities as well as society prevent and curb the commission of cybercrimes by minors, however for that to happen there needs to be various reforms and amendment in our current existing legal system. Legislatures must first understand the peculiar nature of the cyber crimes so that they do not treat cyber delinquents as any other minors criminals. Sometimes cyber-crimes are committed unintentionally or out of unawareness and curiosity without knowing the real consequences. While some cyber crimes are committed through preparation and pre-planning. Therefore, it is not same all cyber delinquent which is why they should be treated as a separate category.

Till date, there exist no treaty between India and any other countries to extradite any cyber criminals. In India, most of the cyber crimes are provided under the Information Technology Act. The other related statutes are listed under the Indian Penal Code 1860, The Evidence Act 1872, The Negotiable Instrument Act 1881 etc. However, none of them have a straight-forward answer for crimes committed by the juvenile in the virtual world. when it comes to child pornography, the law enforcements and other professional needs to be trained in addressing the evidential issues of pornographic pictures and videos, emphasizing on tracing the original producer by following the chain of postings. To be able to do this effectively requires knowledge and understanding of the downloaders' and producer's behaviour and also the language they use to communicate with one another.

Furthermore, a law should be enacted for the mandatory reporting in cases of child pornography. Issues about censorship and privacy may be raised if such a legislation existed, but this crime must be stopped. In case of countries that continue to assist in production and consumption of such material, certain Protocols or even strict global penalties should be enacted to deter them.

The demand prospect of the commercial sexual exploitation of children was raised during the Yokohama Congress, as a predominant concern. Male behaviour is closely interlinked with the such an issue and it is men who carry out such crimes in majority of the cases relating to sexual exploitation of children. However, this does not ignore the fact that at times women are also the perpetrators, but the prime discussions at

Yokohama was to tackle the problem and relation between the male perpetrators and the demand factor for CSEC. This is not to drive the wedge further between the sexes but to truly examine the factors and understand why certain genders are more inclined to crimes such as this and such study is done with hopes in bridging the gp between these raging issues and justice.

In India, the IT Act should promote creating safe space for children where they can go online without cyber risks, like opening of cyber cafes for children only. The Indian legal framework is fairly enabling but there are certain limitations that needs to be not only recognised but addressed especially in cyber offences against children. The laws are insufficient in dealing with various cyber threats that the children online are exposed to like cyberbullying, cyberstalking, grooming, sexting and child pornography. Indian law does not explicitly recognise sexting and cyberbullying as offences but they have already criminalized in other countries.

Intermediaries and credit card companies should hold a mandatory duty to report child sex abuse incidents online. Sec 79 of the IT Act provides intermediaries the due diligence guidelines, however there should be an additional provision restricting for blocking and pre-filtering child sexual abuse material, the website's capability in data retention should be reviewed, and a period for log retention should also be specified in Section 67C of the IT Act.

In sec 79 of the IT act the govt. needs to insert additional guidelines to directing intermediaries on specific steps to protect children from potential online abuse/threats. Sec13 of POCSO Act requires clearly defined guidelines which only mentions images of the child "real or stimulated", but does not clarify if sketches, animation, cartoons and drawings are counted. A thorough enquiry must be conducted in cases where the cyber criminals are below 18 years. It is essential that children and adolescents are not criminalized for their deviant behaviour online.

The International Centre for Missing and Exploited Children presented six criteria to gauge the competency of laws enacted by the state in protecting children in its 2016 Global Review of Legislation on Child Pornography, and they are:

- Whether the state legislation have specific provisions relating to child pornography?
- Whether the state legislation clearly defines child pornography?
- Whether the offences that are computer-facilitated criminalized?
- Whether the possession of child pornography constitutes criminalization?
- Whether the Internet Service Providers are directed to report suspected child pornography?
- Whether the state legislation requires ISPs to develop and implement provisions that allows data retention and preservation?

Upon testing Indian laws against these parameters, it seems to be adequate but for many Indian law enforcement agents and legal experts the challenge lies in the application of the law in order to prosecute offenders. Adequate protection is not provided in the existing legal provisions largely because of differences in definition and terminology, lack of guidelines and proper operational procedures and poor functioning of the law enforcement agencies.

7.3. MENTORS TO GUIDE

Any person at their formulative years need a mentor to offer guidance, be it a parent, guardian or teacher. The dependence on someone who has had more life experiences and therefore have more wisdom to impart is a very important factor for the growth of the child. However, there have been times when mentoring has not gone where it is most needed and while mentors may have wisdom to share they often lack the resources sustain and create long-term results. A strong relationship between the mentor and mentee are at times not enough to hold against eh strong institutional and structural influences in the child’s life. But it is a fact that mentors have always been able nudged their mentees towards the right path and mentorship is the most deployed method to reach out to delinquents. Finding the right mentor along with the right approaches in helping the youth can be blessing and aid the development of the youth greatly and may also see the reformation.

There is little research and literature on mentorship of young cyber criminals, but heart issue is that the sense of belonging that every individual and when not fulfilled, they can turn to anti-social behaviour. So the mentorship can use the development approach such as social-emotional, cognitive, and identity development. Serious cyber offenders have often been associated with certain behavioural traits like narcissism, lack of empathy, depression, anxiety, to name a few. The personality and character of every troubled adolescent and young adult have been shaped by various factors in their life. The mentorship must challenge their negative perspective of life, their peers, and even themselves. This must be done through effective and mature conversation.

The mentor may also include various experiences and experiments like collaborative learning to improve the thinking and broaden the mind and appreciate the values and norms and perhaps come to realise why their actions were wrong. In identity development, mentoring relationships can shift the youth’s perspective about who they are and where they are headed in their future. such development can soon result in a youth learning how to behave. Increase in substantial sessions with mentors can encourage the youth to develop interests in new activities and even consider education and vocational opportunities. However, in assessing and mentoring the youth it is also important to acknowledge the links between educational performances, certain physical and mental conditions, health and tendency towards delinquency.

These young cyber criminals must learn to direct their existing skill set towards positive or meaningful purpose. For example, young hackers have incredible skills of going to complex security systems without getting caught. They can be taught to use their skill for ethical hacking instead of using it in a variant manner. This kind of mentorship will require a mentor that is knowledgeable in hacking themselves. Here, the youth can be encourage to use their skill for cyber security and protection. The combination of cyber security and mentorship can be achieved through recruitment of young person experienced with computer systems and in turn the youth can inform the mentor and companies of the gaps in their systems.

The mentorship must not only focus on making the youth stop their illegal activities but also redirect their skill towards something more meaningful and towards doing things that are bigger than themselves and helping others.

CONCLUSION

With the introduction of the internet, it was the dawn of a new era and the entire world went experienced age of digital revolution. Suddenly, everything became fast paced and accessible, people became more connected but at the same time disconnected. People soon preferred virtual and online interactions rather than meeting others face-to-face. The internet have affected every aspect of life, creating new opportunities but also bringing a whole plethora of new problems. Cyber crimes is expanding and dangerous to society, billions of people are affected by online criminal behaviour. It is high time for nations to start adopting a proactive approach in tackling this issue. The internet is dynamic and ever-changing, therefore it is pertinent that the law adapts to this as well, otherwise cyber criminals will always a be a step ahead of us.

In revenge porn, the conversation should be pulled away from victim-blaming, and all the questions as to why a girl shared her nude pictures in the first place and instead focus on sensitizing and spreading awareness and most importantly teaching respect and the rule of obtaining consent. Children must be instilled with the fear of the law especially young offenders as most of them do not realised the severity their actions and its consequences.

It is also time to recognise the role of men in these crimes, especially when children are sexually abused and exploited online. It is not a man-hating agenda but looking at the issue objectively where majority of its perpetrators are male. This is an important subject to understand as we can see that men are intrinsically involved in the educational and socialisation processes. And this discourse requires cooperation from both men and women, young and old.

Crimes committed by adolescents and young adults should not be quickly disregarded as issues of mere delinquency and rebellion. There is always more than what meets the eye. The constitution of a child is different and unique when compared to that of other adult criminals. Here, children, in their formulative years picks up certain habits and are shaped by various factors and influences. Therefore, in order to understand and reform a child, we must look more closely at the environment of their lives. We come to see young cyber criminals are often a product of their unfortunate circumstances. However, because of their youth, there is still hope for change and reform. Young cyber hackers are in fact intelligent individuals able to understand complex systems in the cyber world and so they only need to shift their perspective and attitude and use their skills for the good of society.

Children should no longer be left alone with their devices, parental monitoring of their online activity is of extreme importance. Social media if unchecked is the most dangerous place to be for a young impressionable mind. It has become tools used for exploiting the vulnerability of the child. They are not only exposed to hackers and paedophiles but also exposed to psychological traumas that may manifest itself in adulthood as well. Parents must also be firm and warn their children about online friendships and romantic relationships.

The children are in dire need of a cohesive global response and obligation to protect them from paedophiles, hackers, fraudsters, etc. At the state level, the authorities should be more vigilant and aware. The traditional views of cyber-crimes must be challenged and improved upon. The is the duty of all states to protect the younger generations. The current legal framework at best is victim-oriented but still fails to address the emergence of new kinds of cyber crime. It is even more minimal when it come to dealing with cyber delinquents. Youths as both victims and perpetrators of cyber crime is a problem that needs much discourse. It can be an endless cycle of victimization and committing online offences, however the cycle can only be broken with the appropriate intervention measures with the help of new policies and law.

BIBLIOGRAPHY

- PRIMARY SOURCES

- Information technology Act, 2000
- The Indian Contract Act, 1872
- Juvenile Justice (Care and Protection of Children) Act, 2015
- Indian Penal code,1860
- UN General Assembly, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 16 March 2001, A/RES/54/263,

- SECONDARY SOURCES

Articles and journals referred to:

- R Kalaivani & Muthu Kumar, *Juvenile delinquency in cyber crime*, 2 Int. j. acad res & dev, 624-626 (2017)
- Othmane Cherqi et al., *Analysis of Hacking Related Trade in the Darkweb*. 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), 79-84 (2018)
- Lee A. Underwood & Aryssa Washington, Mental Illness and Juvenile Offenders, Int J Environ Res Public Health, 13(2): 228 (2016)
- Nana Yaa A. Nyarko et al., *Juvenile Delinquency: Its Causes and Effects*, 88 J.L. Pol'y & Globalization 166 (2019).
- Thomas J. Holt et al,. Low Self-Control, Deviant Peer Associations, and Juvenile Cyber deviance, 37 Am J Crim Just, 378–395 (2012)
- W. F. Skinner & A. M. Fream, A social learning theory analysis of computer crime among college students, 34, J. Res. Crime Delinq, 495–518. (1997)
- Ibrahim S, Causes of socioeconomic cybercrime in Nigeria, IEEE ICCCF Canada, pp. 1–9 (2016)
- Schell, Bernadette et al., Cyber child pornography: A review paper of the social and legal issues and remedies-and a proposed technological solution, 12 Aggress Violent Behav, 45-63 (2007)

- Elena Sharratt, *Intimate image abuse in adults and under 18s*, University of Exerter Economic and social research Council, pg 12 (2019)
- D. Halder & K. Jaishankar, *Teen Sexting: A Critical Analysis on the Criminalization Vis-À-Vis Victimization Conundrums*, The Virtual Forum Against Cybercrime (VFAC) Review, Korean Institute of Criminology (2014)
- R Kraut et.al, Internet paradox. A social technology that reduces social involvement and psychological well-being? 53(9) Am Psychol 1017–1031. (1998)
- Daria J. Kuss & Mark D. Griffiths, *Online Social Networking and Addiction—A Review of the Psychological Literature*, 8 Int. J. Environ. Res. Public Health, 3528-3552 (2011).
- Ethan Kross et. al, Facebook Use Predicts Declines in Subjective Well-Being in Young Adults, 8 PLOS One e69841 (2013)
- M Tiggemann & J Miller, The Internet and Adolescent Girls' Weight Satisfaction and Drive for Thinness, 63 Sex Roles 79–90 (2010)
- QEV Analytics, Ltd. Knowledge Networks, *CASA National Survey of American Attitudes on Substance Abuse XVI: Teens and Parents*, National Center on Addiction and Substance Abuse at Columbia University, 5 & 7 (2011)
- Janis L Whitlock et.al, The virtual cutting edge: The internet and adolescent self-injury, 42 DEV. PSYCHOL 407-17 (2006)
- C Hellstrom et. al, Influences of motives to play and time spent gaming on the negative consequences of adolescent online computer gaming, 28 COMPUT HUM BEHAV. 1379–87. (2012)
- Kesavamoorthy, R., Legal Study on the Protection of Children in Social Network: Special Reference to Indian Law, 15 IOSR-JHSS 16-21 (2013)
- Sankara Moorthy et. al, *Analysis of Indian cybercrime dataset for age demography*, 10 INT. J. APPL. ENG. RES. 1855-1861 (2015)
- M. K. Rogers, The psyche of cybercriminals: A psycho-social perspective. in Cybercrimes: A Multidisciplinary Analysis, 217-235. (Springer-Verlag Berlin Heidelberg 2011)

<u>Books referred to:</u>

- Dan Verton, The Hacker Diaries: Confessions of Teenage Hackers xvii, xviii, 37, 86, 102, 105, 142, 145, 170, 188 (McGraw-Hill Education 1 ed 2002)
- Claudia Megele & Peter Buzzi, Safeguarding children and young people online: A guide for practitioners, 196 Policy Press (2017)

Websites referred to:

- Vikram Dodd, *Children as young as seven 'being enslaved by UK drug gangs'*, The Guardian (Jul. 9, 2019) https://www.theguardian.com/society/2019/jul/05/children-as-young-as-seven-being-enslaved-by-uk-drug-gangs
- Zack Whittaker, *Justice Dept. says its taken down 'world's largest' child exploitation sites on the dark web*, Techcrunch (oct 16 2019, 7:52 pm), https://techcrunch.com/2019/10/16/doj-child-exploitation-dark-web/
- Sonali Acharjee, *The Dark Web of Child Porn*, Magzter (March 2, 2020, 5:00 PM) https://www.magzter.com/article/News/India-Today/The-Dark-Web-Of-Child-Porn
- Martin Bright & Tracy McVeigh, *This club had its own chairman and treasurer. Its business was child abuse*, The Guardian (Feb 11, 2001, 2:33 AM) https://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright
- Reasgan Gavin Rasquinha, *Are you a victim of revenge porn?*, Times of India, (April 19 2015, 00:00) https://timesofindia.indiatimes.com/life-style/relationships/love-sex/Are-you-a-victim-of-revenge-porn/articleshow/46852091.cms?
- Shaju Philip, *Six youths arrested for 2 'rapes' at Ford Kochi*, The Indian Express (Jan 24 2016, 1:54 AM) https://indianexpress.com/article/india/india-news-india/six-youths-arrested-for-2-rapes-at-fort-kochi/#sthash.Faewe4ni.dpuf
- *Hyderabad: Arrest reveals shocking history of rape*, blackmail, Deccan Chronicle (March 22 2016, 2:08 AM) www.deccanchronicle.com/nation/crime/220316/hyderabad-arrest-reveals-shocking-history-of-rape-blackmail. html

- Nelson Groom, Is this the world's youngest hacker? 13-year-old boy hacked into school computer system to get answers to his homework... but says he was only 'testing its weaknesses', Dailymail, (October 8 2014, 9:22 PM) https://www.dailymail.co.uk/news/article-2784488/Meet-13-year-old-boy-hacked-school-computer-online-store-insists-hes-using-powers-good-just-trying-fix-websites.html
- David Bisson, The TalkTalk Breach: Timeline of a Hack, tripwaire (Nov 3 2015) https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-talktalk-breach-timeline-of-a-hack/
- Simon Kemp, Digital 2020: Global digital overview, Datareportal (Jan 30 2020) https://datareportal.com/reports/digital-2020-global-digital-overview)
- Gregoire, Carolyn, The Internet May Be Changing Your Brain In Ways You've Never Imagined, The Huffington Post (Oct 9 2015, 8:54 PM) https://www.huffingtonpost.in/entry/internet-changing-brain-nicholas-carr_n_5614037de4b0368a1a613e96?ri18n=true
- Luis Corron, Social Cyber Threats Facing Children and Teens in 2018, National Cyber Security Alliance (Jan 17 2018) https://staysafeonline.org/blog/social-cyber-threats-facing-children-teens-2018/
- BBC, Instagram biggest for child grooming online - NSPCC finds, BBC news (1 March 2019) https://www.bbc.com/news/uk-47410520
- Devika Agarwal, *Child grooming: India must take measures to protect children from online sexual abus*e (May 11 2017, 21:59 PM) https://www.firstpost.com/india/child-grooming-india-must-take-measures-to-protect-children-from-online-sexual-abuse-3438528.html
- Judith Shulevitz, *Alexa should we trust you?*, THE ATLANTIC, (November 2018), https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844/)
- Rozita Dara, *The dark side of Alexa, Siri and other personal digital assistants,* THE CONVERSATION, (Dec 16 2019, 12: 34 AM) https://theconversation.com/the-dark-side-of-alexa-siri-and-other-personal-digital-assistants-126277
- Vinod Joseph & Deeya Ray, *India: Cyber Crimes Under The IPC And IT Act An Uneasy Co-Existence,* MONDAQ (Feb 10 2020)

https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence

- Sayuri Umeda, *Japan: New Revenge Porn Prevention Act* (Nov 26 2014) http://www.loc.gov/law/foreign-news/article/japan-new-revenge-porn-prevention-act/
- Casey Crane, *Eye-Opening Cyber Security Statistics for 2019*, HASHEDOUT, https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/#cyber-security-statistics-victim-data-and-compromised-records-%E2%80%94-by-the-numbers
- Nicolas Boring, *Online Privacy Law: France, Library of Congress*, (updated 4 may 2018) https://www.loc.gov/law/help/online-privacy-law/2017/france.php
- Kim Bellware, *Illinois Passes New 'Revenge Porn' Law That Includes Harsh Penalties* (31 Dec 2014, 12:29 PM) https://www.huffingtonpost.in/entry/illinois-revenge-porn_n_6396436?ri18n=true

Cases cited:

- United States v Lori Drew, 259 F.R.D. 449 (C.D. Cal. 2009)
- Manish Kathuria Vs Ritu Kohli, C.C.No. 14616/2014
- Avnish Bajaj v State, 2005 3 CompLJ 364 Del
- Gagan Harsh Sharma v. The State of Maharashtra, 2019 CriLJ 1398