Page 2536 - 2544 **DOI:** *https://doij.org/10.10000/IJLMH.11774*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Cyber Delinquencies

SANJEEV KUMAR[1] AND DR ANUPAM MANHAS[2]

ABSTRACT

Present century is considered as the era of technology, internet where the things or transitions are usually done on the internet. Internet is considered as the stage of the world where one can access any information from any corner of the world. But some money minded people using it as a weapon for criminal monetary benefits. Cybercrime is one of the fastest growing criminal activities on the planet. It covers a huge range of illegal activity including financial scams, computer hacking, virus attacks, stalking by e-mail and creating websites that promote racial hatred. As internet technology advances so does the threat of cyber crime. In times like these we must protect ourselves from cyber crime. Antivirus software, firewalls and security patches are just the beginning. Never open suspicious e-mails and only navigate to trusted sites. These offensive acts are termed as cyber crime or cyber delinquency. In order to punish these cyber criminal IT Act, 2000 was enacted and some important changes were made in Indian Penal Code, 1860. The objective of writing this paper is to spread the information regarding cyber crime among the public.

Keywords: *Cyber, Crime, Juvenile, Delinquency, Bullying.*

I. INTRODUCTION

Whenever any wrongful act is committed with the support of data and communication technology such crimes are referred as cybercrimes. Nowadays society is becoming a technology driven society as new technologies being invented day by day. Our connections are getting quicker, our financial dealings are getting easier and our businesses are flourishing thanks to new software to speed up the system. As we are growing into an E-world we are getting more vulnerable towards various threats which come hand in hand with technological advancements. The term cybercrime has nowhere been defined under Indian law but Information Technology Act, 2000[3] and Information Technology Amendment Act, 2008 deals with various cybercrimes and rules governing them[4]. The development of internet nowadays

[1] Author is a Research Scholar at Career Point University Hmairpur Himachal Pradesh, India.
[2] Author is an Assistant Professor (HOD) at Career Point University Hmairpur Himachal Pradesh, India.
[3] For detail, see Information Technology Act,2000
[4] Srivastava Astha & Sinha Shivangi,"Cyber Delinquency: Issues And Challenges Under Indian Legal System, available at https://www.ijeat.org/wp-content/uploads/papers/v8i5C/E12040585C19.pdf (Last accessed on 02.11.2020)

 [ISSN 2581-5369]

have both a positive impact in the same way as negative impact that targets everyone, including children[5]. When it involves access to the technology and computers there's no difference between a teenager and an adult. Social media platforms don't differentiate between child and adult and thus children even have access to all or any the data to which an adult has access. Nowadays technology is employed for many wrong motives and to harm other person. Cyber fraud and various other cyber-crimes are committed by juvenile and by others who are using technology for his or her wrongful gains. Various cyber-crimes committed by offenders are as cyber frauds, cyber bullying, cyber stalking, fraud, digital piracy, cyber suicides, cyber theft, illegal and hacking etc. The condition is worsening day by day but what's more bothersome is that these children who are committing these acts aren't even aware in most of the situations that what they're doing could be a crime. The main reason behind increasing cyber delinquents in India would be unawareness of effect of trivial acts. Most of the youth are obsessed by short-term pleasure and amusement and are unaware as when they start to transgress on the boundary of others rights. A horrible common example of this is Digital Piracy. Children usually download movies, songs etc. from untrustworthy site without even knowing that what they're doing is infringement of copyright of the owner. Sending hateful mails to classmates, downloading photos of others from social networking sites and depicting it in funny way these all are cybercrimes[6]

II. WHAT IS DELINQUENCY?

Delinquent means when someone who fails to do that acts which is required by law, duty, or contractual agreement. Cyber Delinquency in India has been increasing in numbers year by year. If we focus on the data as published by the national crime record bureau there is an increasing pattern in cyber delinquency. Internet exposure is increasing day by day and with it increases the vulnerability of our kids. Recently new forms of cybercrimes have been start committed by juvenile in India[7]. Cyber delinquency is carried out through computers or the Internet. The term juvenile delinquency applies to violation of criminal code and certain patterns of behavior that are not approved for children and young adolescents. It may be group delinquency in which delinquency committed in companionship and the cause is attributed not

[5]"Cyber crime and its impact on children and the alternative solution", available at https://www.indialegallive.com/top-news-of-the-day/news/cyber-crimes-and-its-impact-on-children-and-the-alternative-solutions (Last accessed on 02.11.2020)

[6] *Supra Note 4.*

5.snehal asthana, available at https://nitimanthan.in/blog-posts/blog-niti-manthan/2020/07/28/cyber-delinquency-india/ (last accessed on 02.11.2020)

 [ISSN 2581-5369]

to the personality of the individual but to the culture of the individual's home and neighborhood.[8]

III. CYBER OFFENCES

(A) Cyber Crime against Children

Kids generally get on with computers more quickly and easily than their elders. Today's children grow up with access to computers that are networked to the rest of the world through the Internet. Many of them love to explore and experiment. Unfortunately, that exploration and experimentation can lead them to virtual "places" that are legally off limits, and turn them into criminals even without their knowledge that they're doing anything wrong[9]. Morphing is a special effect in motion pictures and animations that changes one image or shape into another through a seamless transition. By committing cyber crime some person induces children to online relationship with one or more children for and on sexually explicit act and depicts children in obscene or indecent or sexually explicit manner.[10]

(B) Cyber Pornography

Display, Publish, Distribute, Create, import obscene or pornographic material via online platform. Technology is for the aid and advancement of human kind. Kids usually make use of technology for committing acts which are prohibited. One of such act is cyber pornography. Cyber pornography is not specifically described as a cyber crime under IT Act, 2000 but section 67[11] of the act provides punishment and fine for publishing, transmitting or causing to be published or transmitted any data which is obscene in nature. Sometime children tend to do acts which are contrary to the culpable interest of the society. The primary responsibility of the state is to focus on these children who are termed as juvenile in conflict with law and not juvenile delinquents under the Juvenile Justice (Care and Protection of Children) Act, 2015. [12]

(C) Cyber suicides

The term cyber suicide referred to the cases of suicide which have been abetted using technology in one way or the other. People record there suicide or display their suicide live

[8] Kalaivani R, Kumar Muthu, Juvenile delinquency in cyber crime, available at International Journal of Academic Research and Development 2020

[9] Deb Shinder, Juvenile cyber-delinquency: Laws that are turning kids into criminals, available at https://www.techrepublic.com/blog/it-security/juvenile-cyber-delinquency-laws-that-are-turning-kids-into-criminals/(last accessed on 03.11.2020)

10 BhardwajKiran, Cyber Crimes And Its Impact On Children And The Alternative Solutions, availble at https://www.indialegallive.com/top-news-of-the-day/news/cyber-crimes-and-its-impact-on-children-and-the-alternative-solutions(last accessed on 03.11.2020)

11 For detail see,section 67 of Information and Technology Act,2000

12 See, *Supra* Note 11

using internet. Recently a Blue Whale game started in Social networking sites, the final task of this game was to commit suicide. Many suicides happened which were influenced by this game. This game was created by a 21 year old Russian who admitted that he created this game so that children could commit suicide and the society is cleaned.[13] Under Indian legal system, Juvenile in conflict with law are reformed and not punished for their wrongful acts. The act is aimed at reforming the delinquent so that a minor who committed a wrongful act without being capable of understanding the nature of the act is not converted into a hardcore criminal. When it comes to cyber crime committed by minor the JJ ACT of 2015 and Information and Technology Act of 2000 will both be applicable together. But juvenile cyber delinquency is a grey area in these laws no specific provision is there providing for cyber crimes by minor.[14]

(D) Web Hijacking

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content. A web hijacking is a form of unwanted software that modifies a web browser's settings without the user's permission. The result is the placement of unwanted advertising into the browser, and possibly the replacement of an existing home page or search page with the hijacker page.[15]

(E) Cyber Stalking

Stalking can be termed as frequent acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victims property, leaving written messages or objects, monitor the use by a woman of the internet, email or any other form of electronic communication. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated threatening behavior of the cyber criminal towards the victim by using internet services. Section 354D Indian Penal Code, 1860 make staking punishable.

(F) Virus Attacks

The term 'computer virus' was first formally defined by Fred Cohen in 1983. Computer viruses always induced by people. After entering a computer, a virus attaches itself to another program in such a way that execution of the host program triggers the action of the virus simultaneously. Not all computer viruses are destructive though. However, most of them perform actions that are malicious in nature, such as destroying data. Viruses spread when the software or

13 https://www.ijeat.org/wp-content/uploads/papers/v8i5C/E12040585C19.pdf(last accessed on 03.11.2020)
14 See, *Supra* foot no.10
15 available at https://us.norton.com/internetsecurity-malware-what-are-browser-hijackers.html(last accessed on 03.11.2020)

documents they get attached to are transferred from one computer to another using a network, a disk, file sharing methods, or through infected e-mail attachments.[16]

(G) Software Piracy

Software piracy is defined as illegally copying software that does not belong to offender in a manner that violates the copyright.[17]Software piracy also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.

(H) Phishing

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Unawareness among public with regard to phishing attacks and policies is the main cause of phishing in India. [18]

(I) Online Gambling

Online gambling is a universal issue affecting virtually all countries in the world. There are millions of websites that suggest online gambling.

(J) Cyber Terrorism

Cyber terrorism is committed by using internet to conduct violent acts that result in loss of life or bodily harm, in order to gain some political objective through threat or intimidation. common cyber attacks in India are on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks Cyber terrorism is an attractive option for modern terrorists for several reasons.[19]

(K) Cyber Bullying

cyber bulling is nothing but bullying someone on online platforms such as Facebook, Whatsapp, Instagram,tweeter etc. but it is said o be bullied only when something negative is shared about someone which causes huge harm to their reputation. This is very dangerous as it has the ability to harass anyone in public through cyber devices. The main purpose of the cyber bullying is to harm a person mentally socially, psychologically or even physically.[20] . Cyber

[16] available at https://economictimes.indiatimes.com/definition/computer-virus(last accessed on03.11.2020)
[17] available at https://www.yourdictionary.com/software-piracy(last accessed on 03.11.2020)
[18] Phishing Scams in India and Legal Provisions, available at https://cyberpandit.org/?article_post=phishing-scams-in-india-and-legal-provisions (last accessed on 03.11.2020)
[19] Cyber crime in India, http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html(last accessed on 04.11.2020)
[20] Adrita, 'Cyber Bullying: A Disregarded Issue In India', http://www.legalserviceindia.com/legal/article-2358-cyber-bullying-a-disregarded-issue-in-india.html(last accessed on 04.11.2020)

 [ISSN 2581-5369]

bullying occur in many ways, like abusive text and emails, hurtful messages, image or videos, imitating others online, excluding others online, humiliating others online, nasty online gossip and chats**.** The IT Act, 2000 does not provides any provisions relating to prevention and punishment for crimes like cyber bullying by school students. There is no law mentioning the proper age to use cell phones. Students using mobile phones more as a fashion than as an essential commodity and thus make it a means to have fun by sending offending messages to their fellow school mates. The issue of cyber bullying by the school students has to be dealt with as per the Juvenile Justice Act as the offenders and victims are mostly not fully adults or young adults.[21]

(L) Debit card and credit card frauds

Credit card or debit card fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it.[22]

(M) Impersonation and identity theft

Impersonation and identity theft is an act of fraudulently or dishonestly making use of the electronic signature, password or any other unique identification feature of any other person.[23]

(N) Online Drug Trafficking

Online Drug Trafficking is a crime of selling, transporting, or illegally importing unlawful controlled substances, such as heroin, cocaine, marijuana, or other illegal drugs using electronic means.[24]

(O) Hacking

This action is penetrating into someone's system in unauthorized fashion to steal or destroy data, which has grown hundred folds in the past few years. The availability of information online makes it easier for even non-technical people to perform hacking.[25]

IV. REASONS RESPONSIBLE FOR CYBER DELINQUENCY

Cyber criminals always look for an easy way to make big money. They target rich people or rich organizations like banks and financial firms where a huge amount of money flows daily and hack sensitive information. Computers are vulnerable, so laws are required to protect and

21 See, *Supra* note 8
22 Available at https://cybercrime.gov.in/Webform/CrimeCatDes.aspx (last accessed on 05.11.2020)
23 ibid
24 ibid
25Cyber security: challenges and solution, https://www.convergenceindia.org/blog/cyber-security-challenges-solutions.aspx (05.11.2020)

 [ISSN 2581-5369]

safeguard them against cybercriminals. There are possible reasons responsible for cyber delinquency:

- **Easy to access** – Hackers can steal access codes, retina images, advanced voice recorders, etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.
- **Capacity to store data in comparatively small space** – The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for the people to steal data from any other storage and use it for their own profit.
- **Complex** – The computers run on operating systems and these operating systems are programmed of millions of codes. The human mind is imperfect, so they can do mistakes at any stage. Cybercriminals take advantage of these gaps.
- **Negligence** – Negligence is one of the characteristics of human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides cyber-criminal access and control over the computer system.
- **Loss of evidence** – The data related to the crime can be easily destroyed. So, Loss of evidence has become a very common & obvious problem which paralyzes the system behind the investigation of cyber-crime.[26]

V. LEGISLATIVE FRAMEWORK

As cyber crime is increasing day by day so we need some stringent law which could curtail these delinquencies. After the amendment of Indian Penal Code1860 in 2013 some sections were inserted to curb the cyber delinquencies in India such as section 499 of IPC as defamation, Section 292A printing matter intended to blackmail, Section 354A as sexual Harassment, section 354D as stalking. The Information Technology Act also provides remedies for cyber bullying, Section 66A of IT Act provides punishments for a person sending an offensive messages through any communicating device. Section 66E also provides stricter punishment for invading privacy and section 67 punishes publication of obscene pictures. Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to Rs. 1,00,000. As a consequences of IT Act Reserve Bank

[26] Bandakkanavar Ravi, https://krazytech.com/technical-papers/cyber-crime(last accessed on 05.11.2020)

of India Act and the Indian Evidence Act also amended. With the evolution of cyber law, almost all online activities came under scrutiny. However, one thing about cyber law is that there are certain areas on which cybercrime laws in India do not apply such as:

- Negotiable Instrument being other than cheque.
- Power of Attorney
- Will
- The contract for Sale or Conveyance of Immovable Property
- Central Government notified documents or transactions[27]

VI. RECENT DATA ON CYBER DELINQUENCIES AGAINST CHILDREN IN INDIA

Crimes against children include physical and emotional abuse and exploitation, such as through child pornography or sex trafficking of minors. Indian penal code and the special and local laws specifically mention the offences wherein most of the time children are victims.[28] A total of 3,350 cases of 'Sexual Harassment' of children were registered during the year 2015. 51 cases of 'Voyeurism' were registered out of which in Maharashtra (12 cases), Delhi & Telangana (6 cases each) have reported high number of cases in the country. Total numbers of victims were 56 in 51 cases. A total of 1,020 cases of 'Stalking' of children were registered. 348 cases of Insult to the modesty of women were registered. A total of 51 cases of 'abetment to suicide' of children were registered as compared to 56 cases in the year 2014 showing a decline of 8.9% during 2015. The NCRB's data stated that 4, 4546 cases of cyber crimes were registered in 2019 as compared to 28,248 in 2018. The data showed in 60.4 percent of **cases**, registered fraud was the motive followed by sexual exploitation (5.1%) and causing disrepute (4.2%).

The growth rate of cyber crimes had gone down in 2015 and 2016 before registering a sharp spike in 2017. In 2014, cyber crimes had grown by 69% compared to 2013. In 2015, 11,592 cyber crimes were recorded in India, which was an increase of 20.5% compared to 2014. In 2016, growth rate of cyber crimes fell further by 6.3% as 12,317 crimes were registered.

Cybercrimes in India almost doubled in 2017, according to statistics released by the National Crime Record Bureau (NCRB) on October 22. Cybercrime accounted for less than a percentage (0.43%) or 21,796 cases of a total of 50 lakh cognizable crimes in India. Karnataka had the

[27] https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/(last accessed on 06.11.2020)

[28] https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Chapter%206-15.11.16_2015.pdf(last accessed on 06.11.2020)

 [ISSN 2581-5369]

highest rate of cybercrime, followed by Assam, Telangana, Maharashtra, and Uttar Pradesh. India recorded over 9,500, 11,500 and 12,000 cases of cybercrime in 2014, 2015 and 2016 respectively. The data for 2017 comes after a two-year delay, with the Centre blaming states in providing statistics for compilation.

As per the report, "During 2017, 56% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by sexual exploitation with 6.7% (1,460 cases) and causing disrepute with 4.6% (1,002 cases).

(A) Cases related to violation of privacy in cyberspace under the IT Act

In 2017, Assam had the highest number of cases (60) registered for violation of privacy. On the other hand, Uttar Pradesh had 47 such cases, Karnataka had 38, Kerala had 35 and Maharashtra had 22 registered cases. States such as Bihar, Jharkhand, Goa, Chhattisgarh, Jammu & Kashmir (now union territories), Meghalaya, Manipur, Nagaland, Odisha, Tripura, and Punjab did not have any case registered related to violation of privacy on the internet. The total number of such cases registered was 245.

(B) Cyber terrorism (Section 66F) under the IT Act

There were 13 registered cases related to cyber terrorism across the country. Himachal Pradesh had 5 registered cases related to cyber terrorism, which was the highest in the country. While Assam had 4, other states such as Kerala, Tamil Nadu, and West Bengal had 1 each.[29]

VII. CONCLUSION

Cyber crimes started to operate when technology reaches its hit the highest point. The nature of these crimes is different from that of ordinary types of crimes. These crimes can be called as blue color and white color crimes. These are called blue color crimes because these are not very different from other prototype crimes, though recognized by various names. These are also white colour in nature because these crimes are generally committed by those who are having knowledge about science and technologies. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. By using strong passwords, anti viruses, blocking unknown bogus sites and by setting private settings in social media profiles and by using encryption we can protect ourselves from such cyber crimes. We must think before clicking on a link or file of unknown origin. We should never reply to emails that asking us to verify information or confirm user ID or password.

[29]Available at, https://www.medianama.com/2019/10/223-cybercrime-ncrb-2017/(last accessed on 07.11.2020)

 [ISSN 2581-5369]