CYBER FELONY: A TECH ADVANCEMENT OR CURSE TO YOUNGSTERS?

Satish Kumar Mishra[1] & Sanjay Chaudhery[2]

[1]Assistant Professor, IMS, Unison University, Dehradun, Uttarakhand, India
E-mail: *satish.mishra@iuu.ac*
[2]PhD Research Scholar, Department of Law, Graphic Era (Deemed to be University), Dehradun, Uttarakhand, India
E-mail: *sanjaychaudhery.phd@geu.ac.in*

Abstract

This article focuses on cybercrime in the context of the tech advancement being a curse for the youngsters and, for parents, a mode of reliance to have some personal time. The ambit of cybercrime is quite huge and is boundless, with no restriction, making anyone addictive to the same. Thus, not only the youngsters but also the adults today are more prone to such technicalities, which is also very tough work. This article focuses on how the environment is essential for a child's initial years of his/her life and that a healthy environment really helps, whereas a bit of early restriction from social media and cyberspace can safeguard the youngsters.

Keywords: *Cybercrime, Meta-World, Environment, Minor, Youngsters, Cyber Felony*

Introduction

"Data is the pollution problem of the Information Age, and protecting privacy is the environmental challenge," well said by Bruce Schneir. Cyber Felony, or explained in a generic language is Cyber Crime, a crime created by the womb of Information Technology, from the birth of the most useful component of the Modern Era, surrounded now by evil deeds very much like our societal issues.[1] Cyber alone means a large meta-world, spreading its webs faster than the spider and even more dangerous than spider's poison and crime itself is sufficient to define something of dangerous motives.[2] Together it formed a huge concept and a potential threat for the Modern mankind, entering into a meta-world full of unanimous strangers which can have any identity because meta-world has lots and lots of layers of curtains, hard to fold and even more hard to see through it.[3]Today we see each and every person having access to this Tech-world, with their smart phones or mobiles it has even become more fun to get into a new tech field, without the boundaries and without dwelling much into the potential harm it can cause to you, but more than the adults, current lifestyle of youngsters has changed even more, especially after the hard times of COVID period which made everyone relied on the Tech-support, from attending the office online from home, a new word "Work from Home", literally came into being with its full power, to watching online series, kids, teenage youngsters taking their classes with the help of this boundless network, further for a fun hobby using this mechanics for playing games, making dance videos, popular term "reel" came into trend, usage of Social media application enhanced as people were trying to find escape from their lonely life which was once filled with hustle, there was no time to dwell upon one's own thoughts and action, Covid phase provided time to reflect.[4] Youngsters were once treated as "infants", according to law in a basic language, meaning that youngsters or teenagers mind is quite similar like an infant with no proper knowledge of how the world works, and no evil deeds, they do not carry basic understanding and logic behind any motive of the next person as their own mind is in a state of mess due to growth and hormonal disbalances.

Youngsters are prone to be deceived and can easily be influenced that is what have been seen, as they have less emotional tolerance due to Hormonal game going on in their body, they can be easily provoked. In the phase of Covid many such incidents happened which support my above-mentioned wordings, one such case was of Snapchat- Locker Room. Covid phase has been many a times clearly seen as one among the most crucial time of mankind in the entire history of human beings, largely, because of the deadly disease consuming people at a large scale, youngsters at major tried to seek comfort & distraction by entering into the world of technology and parents were more than willing to give proper access to the youngsters into this new world. According to certain researches, use of phone alone for a growing child is an issue, because not only usage of a smartphone for a long period of time and specially during nights have severe effects on health but have a dire effect on mental health too.

Certain Researches right after the Covid clearly portrays the growing use of Smart phones, Internet, Social media, and along-with that grew this invisible yet visible world around us, this world is seen addictive to the society, be it terms of online classes, help from teaching software's, be it work from home, various cases floated around during Covid period which were observed as inter-related with Cyber Crime and Youngster, they truly are a deadly combination, because being falling under the wide ambit of tech world instead of falling while playing in the park both are way too far from each other, along-with that in physical world, we know the person who is going to attack you, might attack, and if attacked you can get punished but in this metaphysical world there could be anyone from anywhere, might be stalking, using dark software's tracking anyone.[5] When the crime arises, so the law is made, IT Act 2000 came into being in India after the introduction of ARPANET. Technological mechanisms have truly helped the modern society for sure, but it has become a curse too, there is phrase in Hindi language meaning, "everything in access today is a harm for future" which could be clearly interpreted in today's scenario.

Meaning of Cyber Felony

The word "Cyber Space" was used for the first time by William Gibson in his science fiction "Neuromancer" in 1982. It is described as a metaphysical world, an intangible area where nothing could be seen or touched yet a lot to learn and explore, as the connection of the real world and virtual world and vice versa have real world effects.[6]

1 Publishing date 1st July 1984.

2 Asian School of Cyber Laws: Fundamentals of Cyber Law (2005) p.93.

Cyber Space is said to be connected to the physical world by a tech-word "portals", what allows people to explore the insides of this metaphysical arena, there may be different ways and layers to have access to those portals one way such as television, two ways such as telephones, third way such as internet.[7] Briefly stated, cyberspace may be described as a conceptual collegium where world's where world's information resources fall together without being seen or sensed.

Cyber Crime

The offences which supersede while using the Internet are known as cybercrimes.[8] These include multi-folds of illegal activities. The term cyber space has been defined as an 'Umbrella', underneath which various illegal activities could be grouped together, being of an anonymous nature the internet becomes a wide ambit for cyber criminals to play their cybercrime tricks.[9] The weapon used by the perpetrators of the cybercrime is technology, hence the cyber-criminals are very much technically skilled persons who have studied and worked underneath the ambit of the internet, knowing all the pros and cons of the tech crime they are going to commit.[10] Some of the very basic cyber-crimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber defamation, polymorphic virus, worms, trojan virus, etc. along-with this there are certain conventional crimes such as theft, mischief, cheating, fraud, misrepresentation, pornography etc.[11] which are not only considered punishable under Indian Penal Code but now under information technology Act 2000 too opened its forum to provide remedies to the victim of such crimes.

Information Technology Act 2000 in Brief

IT Act came into being on October 17th, 2000. Though this law specifically focuses on punishments regarding the cyber-crimes and cyber terrorism, but it also covers pornography under meta-ambience. United nations commission on international trade law (UNICITRAL) adopted the model law on electronic commerce (e- commerce) to bring uniformity in the law in different countries in 1996[12]., Further the general assembly of the united nations recommended that all the countries must consider the recommended model law before amending to their own laws.[13] India was the 12th country to start-up the Cyber Law after passing the Information Technology Act, 2000.[14] Objective of this Act was as simple as the meta-world is complicated, IT Act gives us brief insight and provides the legal recognition to the transaction done via electronic exchange of data and other electronic means of communication.[15] The evolutionary change to the use of this electronic facility as an alternative of papers is also applicable under IT Act 2000, along-with amending the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Books Evidence Act 1891.

There are various features that have been constituted the IT Act 2000 which consists of all the electronic contracts made through secure electronic channels are stated as legally valid, legal recognition or digital signatures, security measures for electronic records and also the digital signatures are in place, a procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized and various others[16]. It is said to be a revolutionary statute constructed for safety from evil side of cyber world.

TOP FIVE CYBER CRIMES IN INDIA

Phishing –

"Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit cards numbers, bank account information.[17]

Ransomware

Ransomware Attacks – Ransomed ware is a malware designed to deny a user or institutions to access the files on their computer systems.[18] By encrypting these files and demanding a ransom payment for the decryption key, cyber-attackers place organizations in a position where paying ransom is the quickest way to gain access to their files.[19] Ransomware is most convenient and most visible type of malware.[20]. Identity theft - identity theft itself suggesting about itself that it is a sort of theft where thief uses the identity of the person or use their personal information without one's consent such as one's credit card information, bank account information, social media passwords etc., to gain financial benefits or commit frauds to gain undue advantage.[21]

Online scams and text scams – online scam mean scams in digital form, or via internet or online.[22] There are various kinds of scams such as text or SMS scams, phone scams, email scams, social media scams, website scams, in – person scams.[23]

Trojan Horse – A trojan horse is a software package containing malicious code that appears legitimate, similar to the ancient Greek myth of the deceptive trojan horse in the odyssey that cause severe damage despite having a harmless exterior.[24] A trojan horse, unlike computer viruses cannot manifest on its own. It requires to be downloaded the client-side of the application for it to function. The executable (.exe) file must be implemented and the software installed for the trojan to attack the device.

CONTEMPORARY ISSUES ARISING OUT OF SOCIAL MEDIA CREATING CYBER CRIMINALS

The new problem is at the face of India as after the introduction of AI, that is artificial intelligence, a new instrument of war. Many cases of advance morphing or realistic morphic could be seen in various social media platform where the cybercriminal imitates the physical identity of other people and edit the face portion of the picture, so purely that the picture looks like a real photograph, famously known as deepfake and either such cyber criminals ask for ransoms or they do it out of revenge.[25] The voice imitation is also one such tool. The social media itself has become a tool of massive exploitation where any type of content is promoted and provided these days irrespective of the age of the person, though the Indian Government

has put on a restriction of age on the same, yet children those are minor are still used as bait under the internet regime.[26] For example, the reel feature in the Instagram and Facebook which is almost an imitation to the TikTok software application which was banned by India in the year 2020 because the application was found to be stealing the data in an unauthorised manner. The violent videos are circulated due to which many state violence cases between religions could be seen, the defamation of one's culture via meme is exploited as well.[27] The most common of all is sedation which has no bounds, every now and then hate speeches and hate comments are circulated on twitter without any legal action been taken.[28] Online sentences lead to major riots and crimes between people, where innocent people lose their lives .A new form of arrest is out in the market named as 'Digital Fraud" or "Digital arrest scam" which according the article published in The Hindu means "digital arrest scam is an online scam which defrauds victims of their hard-earned money. The scammers imitate the higher official such as CBI Officials, ED officials, Custom agents etc. and initiate contacts with victim via phone calls and ask the victim to switch into video consultation through WhatsApp, skype etc. and also show proof like warrants as well in which the victims are duped into payment of high amounts. "The digital area is leading all of us into a cyber-spread illusions so wide that it is unable to return back, as they as "once uploaded on net; stays on net" the perks are numerous of the technological advancements but there are danger lurking behind every advantages.[29]

PARENTS AVOIDANCE AND EXTEME RELIANCE ON TECHNOLOGY

As we all went through the rough phase of Covid everyone started using online mode, again the tech-based working system so that work all around the world could go on smoothly but along -with it brought bombardment of cyber-crime, cyber bullying.[30] Our parents struggled with tech-based system and we became their saviours, they were clueless about this meta-world enjoying their joyful life with the hustle of a bit busy and yet peaceful habitual environment.[31]The sudden charge for some was lot to take in because since the birth of technology in India, COVID was the only phase where in actual use of technology was in real sense came forth with its full pace. During Covid use of making videos, vlogs came to trend, especially you-tube and other social media became a close friend of human, because Z Gen is scared to be alone.[32] These video making trends were sudden exposure of a lot of unimaginable stuff that literally took place in India during Covid phase, one such social media content posting platform was You-Tube, it became a hub of vlog during the harsh period and a well source of income for people so much so that if we take a rough guess six out of ten videos would be of pregnancy vlog or baby's cute photoshoot vlog, isn't it using a child as an object to earn hefty income? It is a topic of fruitful debate, which will lead us to the question of consent, without a child's consent parents clearly showing private moments to the strangers in the world full of danger, you-tube is also a meta world, full of different kind of unknown people, with different intentions, by only just going through the comment section of you-tube obsessed and malicious filled people can clearly state the harmful dimension of such useful source of technology. These days smart phones are in hand of everyone, be it adult, youngsters, or a toddler, yes, a toddler, these days the new soothing lullaby to the infant's ear is notification of a smart phone, parents sooth children giving them phone for playing rather than giving some valuable times and to focus on child's physical sports well- being.[33] Use of phone is so harmful for adults then it could be off the charts for the toddlers and youngsters, along-with that tech is a food that derives a human mad by making them a prey of addiction.[34] Technology is addictive, because it has no dimensions like the real-world having boundaries, it is boundless and that is the kick of the entire process of technology being the centre of our word these days. In fact, nowadays schools who were considered as kind of jail to the student, have also started giving the ease of use of smart phones to children, so basically, in the age of being active in sports and other physical activities, they sit and play video games, see those trendy videos, talk to strangers on social media, and keep sitting at one place, consuming junk food, arresting in obesity and facing various physical diseases such as weak eyes, fatigue, weight gain, diabetes etc., and it doesn't stops there youngsters or teenagers are more prone to the emotional or anger outbreak, being rebellious due to the restricting behaviour of the parents rather than being understanding.[35] The youngsters due to the hormonal disbalance are easily to be provoked to either become the victim of an abuse or they themselves become the agent of the crimes recent news is that in fit of anger a student killed one of his class-mate just to get rid of his studies.[36] Cyber space or to be more precise social media platforms such as Instagram, Facebook etc., gives sense of acceptance to the youngster that makes them trust the strangers, falling under the pit

of cyber-crime, there was a reason that law in India by minor use to mean "infant" meaning a child born, because of them getting influenced pretty easily.[37] Though it is a need of our present environment, but parental dealings should remain like earlier, to ease out the childhood of a child.[38] Child pornography is still a very dreadful thought, though it is a punishable offence, and banned by the government of India, young girls still become a victim of such abuses through the cyber space, morphing, sharing private pictures are one such examples.

CASE LAWS PERTAINING TO CYBER FELONY OR FRAUDS

SMC PNUEMATICS (INDIA) PRIVATE LIMITED VS. JOGESH KWATRA[39]

FACTS – The defendant in this case is an employee of the plaintiff's company who started forwarding derogatory or defamatory remarks to all other employers and other various subsidiaries of the company all over the world to defame the company and its director Mr. R K Malhotra. On finding out, the email originated from a local cybercafé of New Delhi, the owner of the said cybercafé was interrogated and on 11 May 2011, the Defendant was removed from his post by the plaintiff.

DECISION – The hon'ble court directed that the absence of direct evidence that I was the defendant who was sending those e-mails, the court was not in a position to accept even the leading evidence. The court also restrained the defendant from publishing, transmitting any information in the Cyber regime which is defamatory or abusive of the plaintiffs.

HARE RAM SINGH V. RESERVE BANK OF INDIA & ORS. (W.P.(C)[40]

FACTS – This case was regarding the digital fraud conducted in the banking system, one banking system was exposed to the cyber-crime.

DECISION- On November 18 2024 the landmark ruling by the Delhi High Court cleared financial institutions duties to protect customers and implementing a strong security system or measures in the place or in the ambit of net-banking. Presided over by Justice Dharmesh Sharma, the court's decision has set noble standards for the addressal of online fraud and e-banking crimes. The judgement put reference for the balance of technological innovation vis a vis the accountability with reference to the protection of the consumers.[41]

CONCLUSION

According to the subject research of Penology & Victimology Subject, many researches have shown that the reason behind the minor criminals are the effect of environment around them which affects them severely mentally more than physically. The environment clearly is responsible to shape up any youngster's childhood, it was seen in the above-mentioned researches that the youngster who grow up watching domestic violence, and extreme fights in the families turned out into thieves, criminals, and various term which they never want to turn out ever. It is seen that the healthy environment does not only includes the green serene area with fresh air and a good school ambience, the first teaching starts from home, which should be peaceful too and not a warzone because outer world is already filled with so much of hatred. It is also seen that the minor's found to be in such conditions and environment are also more prone to mental illnesses such as depression, anxiety issues, aggressive disorders, panic attacks and paranoid schizophrenia, which further leads them on the way of lack of understanding, certain youngsters fall for intoxicant substances too, which leads along-with mental illness to lack of rationality and judgement lacking mind, it is a root cause which in my opinion can be cured if certain parents watch out for red signs of the child and keep a watch on them especially the usage of Internet and various software applications which directly leads them of fake path of glory which is crashed under ashes as soon as the reality kicks in.

References

1. https://www.britannica.com/topic/Neuromancer
2. https://www.toppr.com/guides/business-laws-cs/cyber-laws/information-technology-act-2000/

3. https://www.acmlegal.org/blog/justice-in-the-digital-age-a-landmark-judgement-on-cyber-fraud-by-the-delhi-high-court/
4. https://enhelion.com/blogs/2021/03/01/landmark-cyber-law-cases-in-india//#_ftn9
5. https:/www.cloudflare.com/en-in/learning/access-management/phishing-attack/
6. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
7. https://www.investopedia.com/terms/i/identitytheft.asp
8. https://www.scamwatch.gov.au/types-of-scams
9. https://www.kaspersky.com/resource-center/threats/trojans
10. https://www.spiceworks.com/it-security/application-security/articles/what-is-trojan-horse/
11. https://www.thehindu.com/news/national/digital-arrest-scam-how-to-protect-yourself/article68806494.ece

Work Cited

1. Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age.* John Wiley & Sons.
2. Kostick, C. (2012). *Saga.* The O'Brien Press.
3. Rinman, M. L. (2002). *Forms of Interaction in Mixed Reality Media Performances-a study of the artistic event DESERT RAIN* (Doctoral dissertation, Numerisk analys och datalogi).
4. Kynard, C. (2020). "All I Need Is One Mic": A Black Feminist Community Meditation on the Work, the Job, and the Hustle (& Why So Many of Yall Confuse This Stuff). *Community Literacy Journal, 14*(2), 5–24.
5. Sinnreich, A., & Gilbert, J. (2024). *The Secret Life of Data: Navigating Hype and Uncertainty in the Age of Algorithmic Surveillance.* MIT Press.
6. Paterson, M. (2020). *The senses of touch: Haptics, affects and technologies.* Routledge.
7. Lotz, A. D. (2017). *Portals: A treatise on internet-distributed television.* Michigan Publishing, University of Michigan Library.
8. Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age.* John Wiley & Sons.
9. Haynes, N. (2018). *Cyber Crime.* Scientific e-Resources.
10. Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime.* Routledge.
11. Bano, L. (2020). *Cybercrime and cyber terrorism in India.*
12. Overby, A. B. (1999). Will Cyberlaw be uniform--an introduction to the UNCITRAL Model Law on electronic commerce. *Tul. J. Int'l & Comp. L., 7*, 219.
13. Holtzmann, H. M., & Neuhaus, J. E. (2015). *A guide to the 2006 amendments to the UNCITRAL Model Law on international commercial arbitration: Legislative history and commentary: Legislative history and commentary.* Kluwer Law International BV.
14. Mathur, S. K. (2006). Indian Information Technology Industry: Past, Present and Future& A Tool for National Development. *Journal of Theoretical and Applied Information Technology, 2*(2), 1–68.
15. Boss, A. H. (1991). The international commercial use of electronic data interchange and electronic communications technologies. *The Business Lawyer*, 1787–1802.
16. Chetty, P. (2013). *An analysis of electronic signature regulation in South Africa.* University of the Witwatersrand, Johannesburg (South Africa).
17. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.
18. Liska, A., & Gallo, T. (2016). *Ransomware: Defending against digital extortion.* O'Reilly Media, Inc.
19. Ryan, M. (2020). *The ransomware revolution: How emerging encryption technologies created a prodigious cyber threat* (Doctoral dissertation, UNSW Sydney).
20. Kok, S., Abdullah, A., Jhanjhi, N., & Supramaniam, M. (2019). Ransomware, threat and detection techniques: A review. *Int. J. Comput. Sci. Netw. Secur, 19*(2), 136.
21. Subramanian, R. (2014). *Bank fraud: Using technology to combat losses.* John Wiley & Sons.
22. Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408.
23. Falade, P. V. (2023). Analysis of 419 Scams: The Trends and New Variants in Emerging Types. *Int. J. Sci. Res. in Computer Science and Engineering, 11*(5).
24. Pitman, L. (2019). *The Trojan Horse in your head: Cognitive threats and how to counter them* (Doctoral dissertation, Old Dominion University).
25. Delfino, R. A. (2019). Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic act. *Fordham L. Rev., 88*, 887.
26. Arora, P. (2019). *The next billion users: Digital life beyond the West.* Harvard University Press.
27. DeCook, J. R. (2018). Memes and symbolic violence: #proudboys and the use of memes for propaganda and the construction of collective identity. *Learning, Media and Technology, 43*(4), 485–504.

28. Freccero, C. (1997). Historical violence, censorship, and the serial killer: The case of American Psycho. *Diacritics, 27*(2), 44–58.

29. Tene, O., & Polonetsky, J. (2013). A theory of creepy: Technology, privacy and shifting social norms. *Yale JL & Tech., 16*, 59.

30. Srivastava, S. (2012). Pessimistic side of information & communication technology: Cyber bullying and legislature laws. *International Journal of Advances in Computer Science and Technology, 1*(1).

31. Sodargye, K. (2019). *What Makes You So Busy?: Finding Peace in the Modern World.* Simon and Schuster.

32. Ji, S., Feng, S., & Xie, M. (2022). Generation Z users' attitudes towards online video advertising: YouTube video platform.

33. Clark, L. S. (2012). *The parent app: Understanding families in the digital age.* Oxford University Press.

34. Kersting, T. (2020). *Disconnected: How to Protect Your Kids from the Harmful Effects of Device Dependency.* Baker Books.

35. Bernstein, N. I. (2000). *Treating the unmanageable adolescent: A guide to oppositional defiant and conduct disorders.* Jason Aronson, Incorporated.

36. Heide, K. M. (1994). *Why kids kill parents: Child abuse and adolescent homicide.* Sage Publications.

37. Davis, M. S. (2015). *The concise dictionary of crime and justice.* Sage Publications.

38. Bronfenbrenner, U. (1979). Contexts of child rearing: Problems and prospects. *American Psychologist, 34*(10), 844.

39. CM APPL. NO. 33474 OF 2016

40. 13497/2022

41. Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework 1. *European Law Journal, 13*(4), 447–468.