American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-12, Issue-2, pp-73-78
www.ajer.org
Research Paper Open Access

A Study On Protecting Child Rights In Digital Space And Emerging Challenges In Investigating Online Abuse Of Children

Blessy Rachel.J
B.A.L.LB (hons),
Saveetha School of Law,
Saveetha Institute of Medical and Technical Sciences (SIMATS)

ABSTRACT
Over the past few years the internet has become an integral part of our day to day life . From the concept of the internet being a source of making life easier with all its features and uses , it has slowly creeped into the lives of our younger generation especially children .There is no doubt that the Internet provides numerous opportunities and benefits for children to learn and express themselves. However, it has also exposed children to dangers that defy age, geographic location and other boundaries which leads to abuse and exploitation of their innocence. UNICEF reports published in 2022 shows that 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online.This has resulted in risks to children and young people having abusive images of them shared on the internet of being groomed or lured into sexual conversations or exploitation by adult offenders and of being bullied or harassed online. With increasing crimes and harm inflicted on children arises strong prevention and investigation to identify the online abusers .To control these issues, the legislature has passed following Acts i.e. The Information Technology (IT) Act, 2000 and The Protection of Children from Sexual Offences (POCSO Act) Act, 2012 wherein punishments and legal actions has been clearly defined.Whenever a mechanism is found to prevent the abusers they invent new technologies and loopholes to exploit children using new techniques.The objective of the research is to analyze the pattern in which online exploitation of children occurs, to study the various techniques used by hackers and abusers ,to learn about the challenges faced by police and investigators and to study the ways to prevent online abuse and how cyber abuse is affecting child rights This research paper uses the doctrinal and descriptive method to find the emerging challenges in investigating online exploitation of children in various aspects and suggests preventive measures to avoid them .
Keywords: *Online abuse , children , challenges, investigation ,Child rights ,cybercrime*

Date of Submission: 01-02-2023 Date of acceptance: 10-02-2023

I. Introduction

The topic of emerging challenges faced during recent times in the field of online exploitation of children and infringement of child rights is of utmost importance . As we all know during the Pandemic, parents were forced to buy a gadget for their children's education. The screen time children were exposed to was beyond safety limits . Not every parent was able to monitor their children . Children present during today's timeline have the Internet, mobile phones and other technologies as a constant source of entertainment upto the point that the distinction between online and offline has become hard for them and prefer spending time online more .Many children were introduced to online gaming during the covid pandemic and that includes unannounced advertisements and harmful clickbaits. Many adult pedophiles mislead the children with obscene images and texts before videos and games . Many children do not have the knowledge to report such activities. The majority of children featured in child abuse images currently online are Caucasian, prepubescent girls (between the ages of less than 1 and 10) says child abuse linked to information and communication technology. The Protection of Children from Sexual Offences Act, 2012 (POCSO) was introduced to protect children below 18 years from offences of sexual assault, sexual harassment and pornography and provide for the establishment of Special Courts for the trial of such offences and for related matters.". UNICEF report shows that a third of young

persons in 30 countries report being cyberbullied, with 1 in 5 skipping school because of it . UNICEF prevents online child sexual exploitation in over 20 countries – using the We PROTECT Global Alliance model – and strengthen the capacity of on-the-ground responders to provide services to victims . United Nations Convention on the Right of Child (UNCRC) protects the rights of children in cyber world .Internet has affected the rights of children globally. Added to all the aforesaid grievances the fact that the online abusers are hard to track down and investigate has made cybercrime a big world threatening crime recently.

This research studies some of the major aspects that make online abuse investigations hard for law enforcement agencies and CBI .

Emerging Challenges in investigating online abuse

Hidden identity

The Internet is a wide space and through online unknown users behind masks play with children's innocence . Usage Of the Internet for criminal purposes is one of the most critical challenges faced by the FBI and law enforcement in general. Online criminals and perpetrators use security software such as a proxy server to hide their identity and deviate their communications through lots of different countries to confuse detection. These criminals can use advanced technologies like Tor browsers and third party encryption which includes VPNs and proxies to hide their true IP address enabling them to add multiple layers to mask their identity. This in turn causes confusion for locating and assigning jurisdiction against them. This makes it more difficult to identify hackers, it means the police can't apprehend them or track their residence.

Ransomware attacks

Ransomware is a dangerous software that locks your computer including all your files so you can't access them and your files will be 'held for ransom' and it will be unlocked only if you pay the price asked for . Ransomware is commonly spread through phishing emails that contain malicious attachments or through drive-by downloading viruses into our device . Usually children don't think twice before clicking into a link which leads to easy ransomware attacks that include child threats that instruct them to steal money or send obscene images in return . Most of the children are too scared to report such activities .November 16, 2021 Kaspersky released the results of a survey of parents of children in K-12 schools in the United States, revealing that 9% of respondents said their school has been hit with a ransomware attack while their child was a student there and 61% said their child's personal data was compromised in the attack. Some of the data is personal, like medical conditions or family financial statuses. In this case parents are ready to pay the ransom when it comes to their children and the hackers easily get away with it .

Online sexual harrasment

According to the report of National Crime Record Bureau in 2017, 17,557 sexual abuse cases were registered] and as per the report in 2018, 21,605 cases were registered under the Protection of Children from Sexual Offences Act (POCSO) . In the midst of the Coronavirus pandemic and lockdown, when the schools and colleges are conducting online classes, teachers and students are troubled by hackers who sneak into online classrooms, often displaying vulgar content on the screens. A established t school in Kolkata ditched online classes after hackers unlawfully entered into several lectures and displayed obscene videos on the screen and threatened the students and teachers online . Cyber bullying, terror recruiting, revenge porn and sextortion among Indian users as internet penetration shows an increase day by day.Anonymization techniques are used for legal and illegal reasons. There are major reasons for wanting to remain anonymous online and maintaining the protection of anonymity online inorder to hide their identity.

Cyberbullying

Cyberbullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Instagram , Facebook and Twitter and a lot of othe online r platforms to harass, threaten or intimidate someone. Provided with easy usage of facebook photographs, whatsapp messages are uploaded and shared by children without knowing the gravity of things and the impact that will have on their future. Cyberbullying is often done by children who are not actually professional hackers and these children are those who have early access to these technologies. Primary school children are becoming victims of cyberbullying and in most cases they refuse to report because there is a huge possibility of their information and chats being seen, shared and investigated during the process . So children rather keep such threats of cyberbullying to themselves which leads to a lot of mental illness including fear and anxiety that even results in inflicting self harm and suicide . These make the investigations hard as the children will have trouble opening up on such delicate and sensitive issues.

Online child soliciting and grooming

Online child soliciting is an offence where the adult commits the offense by openly communicating in a sexualt way with a minor or by distributing sexual material to a minor via the Internet or an electronic messaging or through texts. The National Commission for Women (NCW) in April wrote to the Gujarat Director General of Police after a hacker breached into an online class of a university and started masturbating when the class was going on . In India use of any electronic channel , online or mobile, for such purposes would be treated as a criminal offence under the new IT Act section 67 (A) that states that anyone who transmits in the electronic form any material which contains sexually explicit act or conduct shall be punished with imprisonment which may extend to five years and with fine upto to ten lakh. However to avoid such well established punitive actions there exists various countermeasures to evade being accused, "One such technique is the use of proxy servers . It can open along with an app which is used for educational or entertainment purposes . Kids have developed a craze for online gaming where they download random games online and agree to its terms and conditions. This has made the children more vulnerable to these online abuse .

Abusers having easy access to children

Another avenue where children are targeted by online soliciting other than online classes is found through online gaming and socializing websites. . The common venues where such instances of online child soliciting occur are found in chat rooms, websites that pair random strangers such as Omegle, online game lobbies, online community chat apps etc. In these online venues almost everyone's identity is anonymous making it impossible to know for sure if a person is who they claim to be. This makes it easy for creepy adults to access these same venues by posing as a child themselves. This shows how the majority of minors can be deceived by pedophiles posing as kids their age to deceive them and gain their trust without their parents having any knowledge of what events take place . This is also agreed upon by the data presented by the Crimes Against Children Research Center that states that One in five teenagers that regularly access the Internet say they have received an unwanted sexual solicitation through this venue. Such solicitations were defined as requests to engage in sexual activities or sexual talk, and/or to give personal sexual information. It was also found by eMarketer that 75% of children are willing to share private information online about themselves and their family in return for goods and services as an incentive. This problem of online solicitation of minors becomes harder to tackle when we take into account the unlikeliness of such events to be reported by children to their parents let alone the required authorities. This is proven problem by Crimes Against Children Research Center as they found that only 25% of children that encountered an online sexual solicitation informed a parent or any adult.

Reasons for increased online abuse of children

1) The lack of harmonized national cybercrime laws

It is important to note that a nation’s white-hat hacker is another nation’s black-hat hacker, and vice versa.We cannot charge people with crimes if their actions have never been defined as criminal now in the current law system . That’s why it’s so important for new laws to be introduced, to keep up with the latest technology and ideas the hackers come up with .Today, cyber crime laws are much more revised , but they’re relatively new, and there is l no doubt that it needs to be updated again in the future.

2) Crimes not being reported and convicted

Children in particular have become new victims of cybercrime recently . Children avoid telling their parents about their mistakes made online which causes furthermore trouble. The victims of online exploitation are forced to live with their abuse for the rest of their lives and It also affects the overall mental development of children. children often unknowingly or deliberately share personal information without realizing that by just forwarding this message they can be made to suffer penal charges. Conviction in cases of cyber crime in India continues to be low, even as cybercrime has doubled in the last two years, according to the latest home ministry data. The lack of standard and easy procedures for seizure and analysis of digital evidence contributes to fewer convictions in cyber crimes. Added to that the judicial procedure of our country takes enormous time for conviction. The judiciary often fails to “appreciate" digital evidence and conviction happens when the investigating agency, the prosecution and judiciary come together .

3) Proxies And Other Technology

There exists various methods for an individual to hide/mask his online presence or to make it so that his identity and location cannot be traced back to him. Such facilities are provided through custom networks commonly

referred to as VPNs ie: Virtual Private Network and proxies. They were initially created to protect a person's identity and data when using unknown public networks that may be Monitored without consent or by any prying individuals. However as time progressed online abusers realised they also enable them to hide their IP address, which makes it extremely difficult to find out their identities and even where they're really located. Only the service provider of such a VPN will have the original data containing their customers true IP addresses however they do not share this information as it would amount to a breach of privacy to their innocent customers.
The most commonly used and relied upon vpn service provider is the Onion Router (or Tor), their services allow for anonymous communication, access, and information sharing online, like many other VPN service providers TOR too was originally developed by the for the sole purpose of protecting intelligence by the US navel research laboratory,(Maras, 2014) . Ever since Tor has been made publicly available, it has also been used by individuals to protect themselves against private and government surveillance of their online activities.

Lack of Digital forensic devices
4)

In Order to spot a cybercrime the need for numerous digital devices requires the use of specialized tools to identify, collect, and preserve digital evidence.Other obstacles to cybercrime investigations include the limited abilities of law enforcement agencies to conduct these investigations. Specifically, information and communication technology is continuously evolving. Because of this, cybercrime investigators must be "lifelong learners," continuously training to remain current on technologies, cybercriminals, and their motives, targets, tactics, and methods of operation is of utmost importance .

II. Suggestions

- Parents can teach their children to limit their online information and availability .
- Awareness must be given to children on what is a cyber crime and how it can take place and when it does how to report it and deal with it by teaching them good netiquette
- Read the terms and conditions of an app or any other platform before signing in or downloading
- Installation of a protective VPN to be safe from online viruses corrupting our data
- Reporting of a cybercrime without hesitating will be a milestone of an improvement
- Enforcing the cyber laws present more strictly and enlighten people who are unaware of them
- Not using public wifi for sensitive transactions
- Secure your internet network with a strong encryption password and a VPN
- Getting educated about Proxy and other technologies involved in a cybercrime
- Don't fall for pop-ups and beware of fraudulent emails and text messages
- Protection of your identity online such as your name, address, phone number and/or financial information on the Internet.
- Increasing the knowledge among investigating agencies in collecting digital evidence
- Speeding up our judiciary process in a way that it results in conviction and faster results
- Having a friendly relationship with foreign countries by knowing their cyber laws and crimes in order to prevent malware practices that take place from abroad
- Among all these elders must keenly observe the apps and websites children use
- Government can enforce laws for apps to have mandatory disclaimer that can't be skipped before starting a game that gives guidelines on how to use and the dangers of cybercrime and who to report and how to report .
- Make game developers have software that track certain words that pedophiles might use and the pattern of photos and texts they send .
- Including software for games that require parents to consent and not let kids below a certain age have access for game chats. These are some suggestions from the researcher to prevent cyber crime .

III. Conclusion

Therefore from this small study we can realise that any child irrespective of the gender is vulnerable to cyber attacks and all that we can do is get knowledge and empower children with the knowledge that we possess in order to prevent these attacks . New data released by the National Center for Missing & Exploited Children shows a 35% increase in reports of suspected child sexual abuse online in 2021 where a total of 29.3 million reports - the most ever in one year was reported. Indian laws are coming up with various processes and punishments to reduce cyber attacks with the help of IT Act 2000. As we all know when there is a disease there is a cure so we as a Nation must continue to implement these cyber laws more religiously whenever we sense any clue of cyber attacks and report them to the concerned authority . The major solutions include criminalizing breach of cyber laws , increasing public awareness on cyber crimes and types of attacks , strengthening law

enforcement investigation procedures, speedy adjudication, higher penalty to abusers and increasing parents' attention to the topic of cyber attacks . Added to that the suggestion made will be a milestone of an improvement if implemented . The most important role is to be played by the elders of the society and the surrounding of the child .

Reference

[1]. Protection of Children from Sexual Offences Act, 2012 (POCSO)
[2]. United Nations Children's Fund(UNICEF),The Convention on the Rights of the Child of 1989(Liefaard and Sloth-Nielsen 2016)
[3]. https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926(Collier 2021)
[4]. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.htm(Collier 2021; "Website," n.d.)
[5]. https://www.ojp.gov/ncjrs/virtual-library/abstracts/methodology-computer-crime-investigation(Collier 2021; "Website," n.d., "METHODOLOGY OF COMPUTER CRIME INVESTIGATION" n.d.)
[6]. Shannon v. Latvia, no. 32214/03, 24 November 2009
[7]. Reviewing India's protection of children from sexual offences act three years on. (2015, December 18). Retrieved July 7, 2020 from South Asia @ LSE website:
[8]. https://blogs.lse.ac.uk/southasia/2015/12/ 18/reviewing-indias-protection-of , Sakshi vs Union Of India on 26 May, 2004("Website," n.d.)
[9]. M.Veersamy vs State Of Tamilnadu on 7 March, 2012
[10]. https://blog.tmb.co.uk/why-is-it-so-hard-to-catch-cyber-criminals
[11]. https://www.outlookindia.com/website/story/india-news-online-classes-disrupted-by-hackers-schools-fight-flood-of-obscene-and-abusive-messages/355420(Roy 2022)
[12]. ("METHODOLOGY OF COMPUTER CRIME INVESTIGATION" n.d.)
[13]. https://www.researchgate.net/publication/348191254_CRIME_AGAINST_CHILDREN_IN_CYBER_WORLDhttps://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html .("Website," n.d.)
[14]. https://www.unicef.org/protection/violence-against-children-online
[15]. https://www.globenewswire.com/en/news-release/2021/11/16/2335481/0/en/Nine-percent-of-parents-say-their-child-s-school-has-been-hit-with-ransomware.html
[16]. https://usa.kaspersky.com/blog/ransomware-in-schools-2021/25721/(Navar 2021)
[17]. (Trend 2022)
[18]. https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html. https://www.mbfpreventioneducation.org/stop-cyberbullying-and-prevent-online-harassment/("Website," n.d.)
[19]. https://www.dcyf.wa.gov/safety/prevent-child-abuse("Ten Things You Can Do to Prevent Child Abuse" n.d.)
[20]. Stader, D. L., & Graca, T. J. (2007). student-on-student sexual orientation harassment: Legal protections for sexual minority youth. The Clearing House, 80(3), 117-122. Retrieved from JSTOR
[21]. Tara Dutt vs State on 29 April, 2009
[22]. https://www.dcyf.wa.gov/safety/prevent-child-abuse("Ten Things You Can Do to Prevent Child Abuse" n.d.)
[23]. https://www.myadvo.in/blog/cyber-crime-in-india/(MYADVO TECHSERVE PRIVATE LIMITED n.d.)
[24]. Rogers, P., Wczasek, R., & Davies, M. (2011). Attributions of blame in a hypothetical internet solicitation case: Roles of victim naivety, parental neglect and respondent gender. Journal of Sexual Aggression, 17(2), 196–214. https://doi.org/10.1080/135526010036648("Website," n.d.)
[25]. Child Rights and You (CRY), 2020, "Online Safety and Internet Addiction (A Study Conducted Amongst Adolescents in Delhi-NCR)", February 2020; New Delhi
[26]. Rogers, P., Wczasek, R., & Davies, M. (2011). Attributions of blame in a hypothetical internet solicitation case: Roles of victim naivety, parental neglect and respondent gender. Journal of Sexual Aggression, 17(2), 196-214. https://doi.org/10.1080/135526010036648

(Website)

[27]. Collier, Kevin. 2021. "Hackers Are Leaking Children's Data — and There's Little Parents Can Do." NBC News. September 10, 2021. https://www.nbcnews.com/tech/security/hackers-are-leaking-childrens-data-s-little-parents-can-rcna1926.
[28]. Liefaard, Ton, and Julia Sloth-Nielsen. 2016. *The United Nations Convention on the Rights of the Child: Taking Stock after 25 Years and Looking Ahead*. BRILL.
[29]. "METHODOLOGY OF COMPUTER CRIME INVESTIGATION." n.d. Accessed September 25, 2022a. https://www.ojp.gov/ncjrs/virtual-library/abstracts/methodology-computer-crime-investigation.
[30]. ———. n.d. Accessed September 25, 2022b. https://www.ojp.gov/ncjrs/virtual-library/abstracts/methodology-computer-crime-investigation.
[31]. MYADVO TECHSERVE PRIVATE LIMITED. n.d. "How to Prevent Cyber Crime in India?" MyAdvo.in. Accessed September 25, 2022. https://www.myadvo.in/blog/cyber-crime-in-india/.
[32]. Navar, Erica. 2021. "Ransomware Attacks on US K-12 Schools." Kaspersky. November 16, 2021. https://usa.kaspersky.com/blog/ransomware-in-schools-2021/25721/.
[33]. Roy, Lachmi Deb. 2022. "Online Classes Disrupted By Hackers; Schools Fight Flood Of Obscene And Abusive Messages." Outlook India. February 14, 2022. https://www.outlookindia.com/website/story/india-news-online-classes-disrupted-by-hackers-schools-fight-flood-of-obscene-and-abusive-messages/355420.
[34]. "Ten Things You Can Do to Prevent Child Abuse." n.d. DCYF. Accessed September 25, 2022a. https://www.dcyf.wa.gov/safety/prevent-child-abuse.
[35]. ———. n.d. DCYF. Accessed September 25, 2022b. https://www.dcyf.wa.gov/safety/prevent-child-abuse.
[36]. Trend, Law. 2022. "Is Sexting Illegal in India? Know Here." LAW TREND. April 15, 2022. https://lawtrend.in/is-sexting-illegal-in-india-know-here/.
[37]. "Website." n.d. https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.htm.
[38]. ———. n.d. https://blogs.lse.ac.uk/southasia/2015/12/ 18/reviewing-indias-protection-of , Sakshi vs Union Of India on 26 May,

2004.
[39]. ———. n.d. https://www.researchgate.net/publication/348191254_CRIME_AGAINST_CHILDREN_IN_CYBER_WORLDhttps://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html .
[40]. ———. n.d. https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html. https://www.mbfpreventioneducation.org/stop-cyberbullying-and-prevent-online-harassment/.
[41]. ———. n.d. Rogers, P., Wczasek, R., & Davies, M. (2011). Attributions of blame in a hypothetical internet solicitation case: Roles of victim naivety, parental neglect and respondent gender. Journal of Sexual Aggression, 17(2), 196–214. https://doi.org/10.1080/135526010036648.