CHILDREN IN THE VIRTUAL SPACE - CRIME, LAW AND REMEDY

-Kamal Jeet Singh* & Manu Sharma**

bstract—With the changing time, the lifestyle has \mathbf{I} undergone a huge change. The revolution in information technology has brought corresponding challenges to make the best possible use of it for the young generation. One of the major areas of concern is to provide a safe e-environment for our children. The dependency of children on gazettes and the internet has become inevitable because of the introduction of Information Technology into education, online tutorials, and connecting with parents and family outside the home. In the hustle of a job, career and future, children are often left unattended on the pretext of becoming independent. The children are left in cyberspace all alone out of family and educational compulsion and this is the time when they become easy prey of cyber criminals. However, the biggest compulsion has been imposed by the covid pandemic which exaggerated the dependence on information technology and made it inevitable to avoid the use gazette and the internet. Since then, there is no looking back. With the increase in the use of gazettes and the internet, children have to encounter with cybercrimes like online harassment, online defamation, sexual abuse, sexting, cyberstalking, blackmailing, online fraud etc. Such experiences often leave children with lifetime scars of emotional and psychological imbalances, destroying their precious life in numerous ways. The data shared by NCRB Report 2021 has been quite shocking and disturbing for policymakers, law personnel and the public at large. There has been an unexpected rise in online offences against children. This directly poses questions

^{*} Ph.D. & Professor (Law), Vice-Chancellor, Madhusudan Law University, Cuttack, Odisha. <kamaljeetsingh.1089@gmail.com>.

^{**} PhD & Assistant Professor (Law), Career Point University, Hamirpur. <sharma7manu@ gmail.com>.

about the security of the children in cyber world. It's high time to review things legally as well as socially for providing a secure and safe environment for the children in virtual world. Childcare and protection are inevitable, not only for the effective growth of children but also for the growth of society at large. The present paper aims to critically analyse the problem of cyber safety of children and increasing online crimes against children for which doctrinal and analytical approach has been adopted. The present research paper aimed to critically analyse the reasons for increasing safety issues against children in the virtual world and effective measures to ensure safety standards for children in the e-environment.

Keywords: Information Technology, Cybercrimes, E-Environment, National Crime Records Bureau, Social-Media.

I. INTRODUCTION

In an ever changing society, nothing is static including the law. Crime is no exception to this. The mode of committing the offences has undergone a huge change with the advent of Information technology. That's why the law has to change itself to meet the needs of changing society. Information technology has become an integral part of the lifestyle. From personal dependence on information technology to e-governance, there is no sphere which has remained untouched by its impact. The mushroom growth of Information Technology over the past few decades has created numerous opportunities for children to learn and explore the world around them. The use and misuse of information technology have been a point of contention in the contemporary world. One such issue which is being witnessed by India is increasing cybercrimes against children. Most of the children due to their tender age are usually allured by free sites and social media and fell prey to cybercrimes. Children are easy prey to online sexual abuse and exploitation all over the world. According to NCRB, there has been a 400% increase in children's online offences. In 2021, there were 1,49,404 occurrences of crime against minors reported, up 16.2% from 2020, according to the National Crime Records Bureau (NCRB Report 2021). (1,28,531 cases). Kidnapping and abduction (45.0%) and Protection of Children from Sexual Offenses Act, 2012 (38.1%), which includes child rape, were the two largest crime heads under "Crime Against Children" in 2020. In 2021, there were 33.6 crimes reported per 1 lakh children, up from 28.9 in 2020. 52,974 incidents in total were reported as cybercrimes, up 5.9% from 2020 in terms of registration (50,035 cases). Under this category, the crime rate increased from 3.7 in 2020 to 3.9 in 2021. During 2021, in all of the cybercrime cases registered 60.8% were in the context of fraud (32,230 out of 52,974 cases). This figure had succeeded by sexual exploitation with 8.6% comprising 4,555 cases in all and Extortion with 5.4% (2,883 cases). In 2019 there were 306 reported cases of cybercrimes against children whereas this figure rises to 1102¹. The crime data is quite disturbing. However, this is only a partial picture as there might be so many cases which were never reported to the State authorities because of so many reasons like lack of legal awareness, lack of legal assistance, due to fear, shame etc, Children are the future of the nation and it is the responsibility of State to maintain and protect them from all forms of exploitation and to provide them a healthy environment to grow and develop.

II. OBJECTIVE

- 1. The present research paper aims at analysing the problem of increasing online crimes against children in India.
- 2. To critically evaluate the various legislative provisions dealing with the commission of cybercrimes against children and various other measures taken by the government to cope up with the present problem.

III. MEANING AND DEFINITION

The term "offence" has been defined under Section 40 of IPC as an act prohibited by the Act. That means offence includes only those acts which are included under IPC whereas the other acts are excluded from the purview of the term "offence". However, in a general sense, the term offence can be understood as any act which violates the law of the State for which a certain penalty will be imposed. Cybercrime is different from the term crime due to its nomenclature. Cybercrime is a crime in which a computer system or network is either the target or means of committing the crime. It might be used just as a repository to hide the evidence.

The term "child" has been defined by various legislations. According to Indian Majority Act, 1857 a minor means any person who is below the age of 18 years. However, for any child for whom a guardian has been appointed by the court the age of majority is 21 years.

The term "child" has been defined under the Prevention of Child from Sexual Offences Act, of 2012. It states that a person who has not crossed 18 years of age will come under the definition of a child.²

¹ Crimes in India 2021, Statistics, vol. I, NATIONAL CRIME RECORD BUREAU, https://ncrb.gov.in/ sites/default/files/CII-2021/CII_2021Volume%201.pdf (last visited on Nove 5 2022).

² S.2(d), Prevention of Child from Sexual Offences Act, Acts of Parliament, 2012 (India).

As per Section 2(da) of the Prevention of Child from Sexual Offences Act, "child pornography" means and includes any visual depiction of sexually explicit conduct involving a child which includes photograph, video, digital or computer-generated image indistinguishable from an actual child, and image created, adapted, or modified, but appear to depict a child.³

IV. E-CRIME AGAINST CHILDREN

The children in virtual space in prone to crimes and criminal activities. The major categories of cybercrimes committed against children in the e-environment can be listed below:

- **1. Phishing:** Phishing is an act of cheating or fooling someone to give them their login credentials by using the internet and frequently a bogus website or email. This is an easy way to trap the minors and get the cookies in a very easy manner, which can be misused later on.
- 2. Child pornography: Maybe the most generally perceived kind of digital violation against children is "kid digital sexual entertainment." Child digital porn has turned into the most debatable point rising out of the use of the Internet of late. It is a sort of business sexual abuse of children by the use of the Internet and is of exceptional interest. Truly expressed material exists on the Internet. Kid porn has been framed into a multi-billion-dollar industry, which can be shown up bogged down inside the exploiter's home. Every photograph or tape of kid porn is a verification of that youngster's abuse. In kid sexual entertainment, the expert association mutilates his person and dispatches a mail to a kid customer of PC for sending photographs for a carrier of plan or showing, with a deal, impetus or money and once in a while they ensure their losses that such pictures are intended for individual or private or secret use. Exactly when they get such pictures, they add something practically the same through the reasonable program and convert them to express pictures, for instance, putting the face of the individual or casualty on the exposed/naked body of the individual or converting them into cosy banners and conveyances through Modem by customers without the information on the individual being referred to/casualty.⁴ Child pornography is also known as CP, CSAM, child porn, or kiddie porn. It is a type of pornography that uses minors for sexual gratification without their consent. It may be created with a kid's explicit participation or sexual assault (also known as images of child sexual abuse), or it may be faked child pornography. Internet exploitation for sexual exploitation or labour is unlawful, and it involves the spread of child pornography and human trafficking.

³ S.2(da), Prevention of Child from Sexual Offences Act, Acts of Parliament, 2012 (India).

⁴ Raghunath Patnaik, Vulnerability of Children through Cyber Crimes, vol. XXX (2&3) INDIAN BAR REVIEW 406, 406-407 (2003).

- **3.** Cyber harassment: Cyber harassment is perhaps another of the most prevalent computer crimes on this list. This happens when someone intentionally stresses out another individual via technology, frequently by using inappropriate language or content. Sending undesired messages, such as harassing sexual or violent ones, by text or email can accomplish this. Sending threatening texts or releasing personal images of a person without their consent are two instances of cyber harassment. Bullying online frequently takes the form of cyber harassment.
- **4. Ransomware:** Ransomware is not exactly an offence but is a prominent way of committing cybercrime against children. It is a type of malware that encrypts data or a computer and then demands money to decode the data or device. Using ransomware, a computer or its contents are frequently held hostage until the victim pays the demanded sum. Like ransomware, there is other malware like skyware, bigware etc.
- **5. Online libel:** online libel covers the situation of posting some fabricated information about another person on an online platform with the intention of causing distress or emotional harm to such a person. In such an offence, the reputation and dignity of the person are at stake. It includes the posting of false information about a person in a public forum, such as a social media page, with the intent of tarnishing a child's reputation or imagining and causing humiliation. The famous case *Aflalo v. Weiner*⁵ relates to online libel. In this case, the petitioner, Alfalo filed a lawsuit alleging defamation per se and intentional infliction of emotional distress against Weiner.⁶
- 6. Eavesdropping cyberattacks: Cyberattack eavesdropping also refers to the practice of covertly watching someone else's internet activities. These cyberattacks frequently involve the use of spyware or trojans that are used to eavesdrop on people's online communications, such as keyloggers and other spywares.
- 7. Cyberbullying: The term cyberbullying was coined by Bill Belsey, Canadian educator. Cyberbullying is defined as, using both information technology and communication technology beyond the limit in order to harm a person's reputation, or state of mind, or to humiliate a person. It is an act by which the person being bullied suffers an adverse effect.⁷ Indian law has been silent on the problem and victimization of cyberbullying. The statute which addresses cybercrimes is the Information Technology Act 2000, it has not touched upon communication-related threats and offences in cyberspace. Indian Penal Code and IT Act 2000

⁵ Case No. 17-61923-CIV-MORENO (Southern District of Florida., United States District Court Jul. 2, 2018).

⁶ 17 Different Types of Cybercrime: 2022 List with Examples https://cuetolawgroup.com/ types-of-cybercrime/ (last visited on Nov. 10, 2022).

⁷ Saran Errakot & Rahoof V.K., Cyber Bullying - A Need for Separate Provision in Indian Law, vol. 5, issue 1 GLS Law JOURNAL 38, 38-40.

neither define cyberbullying nor punish cyberbullying. The following provision is used currently to fight against cyberbullying. Provisions under IPC Section 354A and Section 354D of the IPC provide punishment for sexual harassment and stalking against women. Cyber-stalking of women was recognized as an offence, subsequent to the insertion of section 354D in the IPC through the Criminal Law (Amendment) Act, 2013. However, if a man is a victim of cyberstalking, Section 354D will not apply. Section 509 IPC: punishes any person who utters any word, or makes any gesture or sound with an intent to insult the modesty of any woman Section 354A IPC deals with sexual harassment and punishment for Sexual harassment. Section 354D IPC defines stalking as any man who follows a woman, and contacts her for personnel interaction repeatedly, even after the clear intimation of disinterest of the woman. The provision covers both physical as well as online stalking and punishes the stalker.⁸

8. Cyberstalking: Cyberstalking can be defined as an act of following a person online. Cyberstalking includes the acts like repeatedly sending unwanted messages, using the internet to track their location etc.

V. REASONS FOR INCREASING CRIMES AGAINST CHILDREN IN E-ENVIRONMENT

Due to lockdowns and school closings brought on by the pandemic, an increasing number of kids have started spending more time online as of early 2020. UNICEF has noted that the growth in children's screen usage has jeop-ardised their online safety and raised the likelihood that they will encounter inappropriate behaviour and content. Cybercrimes against minors increased by more than 400% in India in 2019 compared to 2020. These offences involved the publication or transmission of materials containing child sexual abuse in almost 90% of the cases (CSAM). Children's online safety has been determined to be at risk due to rising social media usage, a large shift toward online schooling, and the use of educational apps.⁹

1. Tender age: The tender age of the child exposes him to the crime world easily. The child by its very age is fascinated by the new or adult things. Small offers and schemes also give incentives to teenagers to either follow any site or to become members of certain online groups or pages. This obvious fact is misused by criminals to attract children towards them.

⁸ Ibid.

⁹ Anirban Sarma, A Pandemic of Abuse: How India is Protecting its Children Online, https:// www.orfonline.org/expert-speak/how-india-is-protecting-its-children-online/ (last vidsited on Nov. 11, 2022).

- 2. Active & frequent users of the Internet: In the recent few years, especially due to covid pandemic the use of smartphones and the Internet by children has increased many folds. The schools being shifted to the online mode during the pandemic changed the concept of schooling and teaching-learning. Even after the schools turn back to offline modes, there is still dependency upon software and online academic activities.
- **3. Lack of security assistance:** The children being frequent internet users lack security assistance. They usually visit the free sites and intentionally or unintentionally leave their information in the form of cookies. These cookies are easily used by criminals for their benefit. Many times, they also share their confidential information being asked before using any site name, address, email, password etc.
- 4. Lack of Knowledge to address or report the illegal act: The children often use or visit sites which seem to them attractive or have content of their interest which includes free game sites, free pornographic sites, sites offering small cashback, free data etc. Unknowing they fell easy prey to preparators and things get worse when they hide or handle themselves without recourse of public authorities. Lack of awareness to report the matter further exaggerates the criminal issues.

VI. LEGAL PROVISIONS

- 1. The Indian Penal Code, 1860 provides for various offences and their punishments. The code defined various traditional offences and their punishment. As per Section 10 of the Indian Penal Code the term "woman" female human being of any age. In view of the increasing crimes against children and women in India, the parliament has passed Criminal Amendment Act, 2013 which provides for various new offences. One such offence is Section 354A sexual harassment. The offence of sexual offence covers various acts and makes them punishable such as physical contact and advances involving unwelcome overture, demand or request for sexual favours, showing pornography against the will of women etc. Section 354D of the Indian Penal Code provides punishment for stalking which includes stalking via computer resources. Section 354D covers the acts of following a woman and contacting such woman to maintain personal interaction despite the disinterest shown by such a woman. Secondly, it covers the act of monitoring women using the internet, email or any other form of electronic communication. However, these offences are generally defined, without any specific mention of a child. However, these provisions are general in nature and failed to meet the present tricky situation of the world.
- 2. The Information Technology (IT) Act, 2000 is the first legislation in India which tried to cover all the issues related to Internet technology. It covers both contraventions as well as crimes. Contraventions can be

described as violations of any rule or provisions mentioned under the Act whereas crimes include serious breaches of the right to life and liberty of an individual. The Act has adequate provisions to deal with prevailing cybercrimes. One such crime is Cyber Pornography which has become a global problem. The technology has its own advantages and disadvantages. Cyber pornography is the outcome of technological development which makes it easily accessible to people across the globe. With the easy and cheap availability of the internet, people cannot only view porn content on their mobile or laptops with just one click but they even upload pornographic content online. In the digital era, the concept of sexually explicit things has become broad. Nowadays pornography has been bifurcated - softcore pornography and hardcore pornography. The only difference between softcore pornography and hardcore pornography is only in the area of depiction. There is no depiction of penetration in softcore pornography, while hardcore pornography depicts penetration. Hence it cannot be denied that the internet has made child pornography more reachable to distributors and collectors but also made children easy prey for it¹⁰. Section 66E prohibits the transmission of images of "a private portion of any person" without their permission. A fine of not more than two lakh rupees or three years in jail is the punishment for the same crime. Private life is protected by the right to life in the Indian Constitution's Part III, according to a historic ruling by Justice K.S. Puttaraswamy v. Union of India (and Others). Article 21 of the Indian Constitution prohibits disseminating any information that infringes on a person's privacy.¹¹

Section 67B of the Act specifically provides strict punishment for publishing, browsing or transmitting child pornography in electronic form. Section 67B of the IT Act, 2000 makes it a punishable act to publish, transmit, view or download child pornography. The said provision provides for the different acts which amount to child pornography:

- a) That any material published or transmitted electronically that depicts the children to be engaged in any sexually explicit act or conduct.
- b) That depict the children in any obscene or sexually explicit manner.
- c) That induces the children to indulge in online relationships with one or more children for any sexually explicit act, or in a manner that may offend a reasonable adult on the computer resource.
- d) That facilitates child abuse online.

¹⁰ Nidhi Chillar, Cyber Pornography, https://blog.ipleaders.in/cyber-pornography/ (last visited on May 5, 2022)

¹¹ Sanjeev Kumar, Legal Perspective of Porn Production in India: A Study with Special Reference to Onlyfan.Com, vol. 28, No. 3 JOURNAL OF CONTEMPORARY ISSUES IN BUSINESS AND GOVERNMENT 351, 354-55 (2022).

e) That record own sexual abuse or sexual abuse of others¹².

In 2009 the first case *Wilhelmus Weideveld* v. *India* came up under Section 67B of the IT Act. In this case, the accused Wilhelmus was a Dutch Nation who came to India in 1980 as a tourist. Thereafter he started running an orphanage. He was intercepted by INTERPOL for uploading pornographic material.

In another famous case, *Avnish Bajaj* v. *State (NCT of Delhi)*¹³. The Delhi high court dealt with the matter of child pornography in detail. In this case, the website Bazee.com Carried a listing which offered for sale a video clip shot using a mobile phone of two school children indulging in a sexually explicit act. The listing escaped the filters installed on the website and was brought to the notice of the website on the same day. Despite this listing was put for sale for another three days and was purchased by eight persons. In this case, the Delhi High Court quashed the criminal proceedings against petitioners on the following grounds:

- a) The listing contained explicit words which left the person in doubt that what was sought to be sold was lascivious and therefore listing prima facie is obscene.
- b) Website owners and operators need to employ filters if they want to prove they did not want to permit such material. If the filter fails, the website's knowledge about obscene material is presumed under section 292 of IPC.
- c) IPC does not recognise the principle of automatic criminal liability. In the absence of a specific allegation in the charge sheet. So despite knowledge of the failure of filters, the petitioner cannot be held guilty.

Section 79 of the IT Act and The Information Technology (Intermediary Guidelines) Rules 2011 require that the intermediaries shall observe due diligence while discharging their duties and shall inform the users of computer resources to act accordingly.

The Protection of Children from Sexual Offences (POCSO) Act, 2012 has been enacted to effectively address the issues of sexual offences and sexual exploitation of children in India. The POCSO Act has been enacted with a view to protect children from sexually explicit offences like Sexual assault, Sexual harassment, and Pornography and to establish Special Courts so that such cases can be disposed of in a quick manner. Section 11 of the Act discussed in length the offence of sexual harassment. This offence covers various acts which amount to sexual harassment. Such acts also cover showing the

¹² *Ibid*.

¹³ 2004 SCC OnLine Del 1160: (2005) 3 Comp LJ 364 Del (India).

content with the help of media. The offence of sexual harassment is said to commit against a child when any one or more of the following acts are proven to be done:

- a) Speak word, produce a sound, make a gesture, or display the body of the child or some part of his body in order to make the words audible to the child, hear the sound, see the gesture, see the object or see the part of one's body, makes a child exhibit his body or any part of his body so as it is seen by any other person,
- b) exhibits any object to a child for pornographic purposes in any form or media,
- c) follows or observes a youngster regularly or continually, either physically or through electronic, digital, or other methods,
- d) threatens to use against the child any real or manipulated depiction of any aspect of the child's body or the involvement of the child in a sexual act which can be depicted via electronic or digital mode,
- e) allures a child for the purpose of pornography or offers gratification for indulging in such acts.

Section 14 of the POCSO Act, 2012 makes the use of a child or children for pornographic purposes a punishable offence. Such act shall be punished with imprisonment for a term which shall not be less than five years and shall also be liable to a fine. This section further provides for enhanced punishment in the event of a second or subsequent conviction which shall be imprisonment not less than seven years and also liable to a fine.¹⁴

Further Section 15 of the Act makes the storage of pornographic material involving children a punishable act. It states that any person, who stores or possesses pornographic material in any form involving a child and fails to delete or destroy or report the same to the designated authority with an intention to share or transmit child pornography shall be liable to a fine not less than five thousand rupees. In the event of a second or subsequent offence, the amount of the fine will be enhanced, which shall not be less than ten thousand. The sub-section (2) further states that any person, who stores or possesses pornographic material in which a child is indulged either for transmitting, propagating, displaying or distributing in any manner, however, it does not include such depiction for the use of reporting or as evidence in any court of law shall be punished with imprisonment which may vary up to three years or with fine or with both. Sub-section (3) further makes storing or possessing pornographic material which involves a child for commercial as punishable. On the first conviction, the accused shall be punished with imprisonment which

¹⁴ Ritika Sharma, POCSO Act - All You Need to Know, https://blog.ipleaders.in/pocso-acteverything-you-need-to-know/ (last visited on March 2, 2023).

shall vary from three years to five years, depending upon the gravity of the case or it may be the fine only, or it may be with both. In case of a second or subsequent conviction, the offender will be punished with more stringent punishment. Such subsequent punishment will be imprisonment which varies from five years to seven years, depending upon the gravity of the offence and a fine shall also be levied.¹⁵

VII. RECENT DEVELOPMENTS

Apart from legislations, the government is constantly trying to create awareness of online offences against children in the e-environment. The government has taken various initiatives to make the procedural process easy in case of the commission of such offences. The recent developments in this context can be discussed as follows:

- **1. Indian Cybercrime co-ordinator centre (I4C):** The Indian Cyber Crime Coordination Centre is a government initiative to deal with cybercrime in India, in a coordinated and effective manner. It is affiliated to the Ministry of Home Affairs, Government of India. The Indian Cyber Crime Coordination Centre has 7 components which are:
 - a) National Cyber Crime Threat Analytics Unit (TAU)
 - b) National Cyber Crime Reporting Portal
 - c) National Cyber Crime Training Centre
 - d) Cyber Crime Ecosystem Management Unit
 - e) National Cyber Crime Research and Innovation Centre
 - f) National Cyber Crime Forensic Laboratory (NCFL)
 - g) Ecosystem Platform for Joint Cyber Crime Investigation Team
- 2. National cybercrime reporting portal: It is a national cybercrime reporting portal established under Ministry of Home Affairs. It is available on the site- cybercrime.gov.in. NCRP is divided into two report cybercrime related to women and children and Report other cybercrimes. Report cybercrime related to women and children can be further done in two ways. First id report and track, and another report anonymously. under report, anonymous police will not report FIR. It is basically where the victim wants to keep his/her name secret. Under Report cybercrime related to women and children, the cases which can be reported are child pornography, child-related abusive material, obscene material etc.

¹⁵ Ibid.

VIII. CONCLUSION AND SUGGESTIONS

The above analysis depicts that there has been a rise in cybercrimes against children in India. The data of NCB includes only the on-record data. There might be many cases which go unreported due to lack of legal assistance, out of fear and shame. Hence, we can imagine the ground reality of cybercrimes against children. There are plenty of laws and legal provisions to deal with cybercrimes against children in India. However, the fact remains the same that spite of these laws cybercrime against children is on the rise and our system is not able to provide a safe e-environment for children. There are two major reasons responsible for this. Firstly, the concept of cybercrime/cyber abuse and the mode of commission of the offence in the cyber world is updating day by day and the law is not able to modify itself at the same pace. There are still various loopholes in this IT Act, 2008 as there are newly discovered and undiscovered cyber-offences for which the law needs to stretch its arms and improve the strictness to deal with. Also, there are offences which are not governed by the IT Act as they are already covered under other laws such as "Cyberdefamation" which is governed under Indian Penal Code, 1860, the term "Defamation" and its punishment is defined under this Act therefore, no specific definition is covered elsewhere because the impact of such online offence is the same as that of the offline. Secondly, there is a lack of awareness among children regarding illegal cyber activities and cybersecurity. However, what is required is to protect the child by making him or her aware of the misuse of technology. This awareness can be effectively done by small efforts on the part of parents and school authorities. There are a few suggestions in this context:

- a) Talk to your children about potential online threats such as grooming, bullying, and stalking, and keep track of their online activities. Set clear guidelines for internet and online games usage.
- b) Awareness programs regarding cyber safety and maintaining privacy are to be conducted at the school level. Like if anyone asks about their whereabouts, the family, school etc they are not supposed to revert and they have to report the matter immediately.
- c) The government should from time to time find out and block the sites which depict violence against children or any pornographic material to discourage the access of such things.
- d) Mass media, NGOs etc. should be motivated to create awareness through workshops or other programmes regarding protective laws for children.