CHETANA
INTERNATIONAL JOURNAL OF EDUCATION (CIJE)

Peer Reviewed/Refereed Journal
(ISSN: 2455-8729 (E) / 2231-3613 (P))

Impact Factor
SJIF 2023 - 7.286

Prof. A.P. Sharma
Founder Editor, CIJE
(25.12.1932 - 09.01.2019)

Cyber Crimes against Children: A Disregarded Issue in India

SEEMA SHARMA
Research Scholar
DR ASHISH KUMAR SINGHAL
Associate Professor
The ICFAI University, Dehradun
Email- simigaur2@gmail.com, Mobile- 9664123798, 8947986608

First draft received: 12.11.2023, Reviewed: 18.11.2023, Accepted: 27.12.2023, Final proof received: 30.12.2023

Abstract

The rights of children, such as the rights to participation, development, protection from exploitation and abuse, access to legal aid, and protection from violence and abuse, are neither respected nor protected by the current criminal justice system. It is too severe and complicated for kids to comprehend. Children have many rights granted to them under the Indian Constitution and the 1989 Convention on the Rights of the Child, which India has ratified. Youngsters now have rights. Children who interact with the criminal justice system as witnesses, offenders, or victims run the danger of experiencing physical, sexual, or psychological abuse. They are more vulnerable because of rules pertaining to required reporting, sexual consent age, minimum age of criminal responsibility, preliminary assessment, and difficulties obtaining legal counsel. It is evident that abuse and violence against these children are decreased and their rights are upheld when they are taken out of the intricate and severe criminal justice system. The present criminal justice system's breaches of children's rights are examined in this article. It presents recommendations for legislative changes to safeguard children's rights and makes the case for a juvenile justice system that kids can rely on, understand, and be empowered by.

"The true character of a society revealed in how it treats its children". *-Nelson Mandela*

Keywords: *Child, Child Protection, Cyber Abuse, Cyber Bullying, social networking sites, IT Act, IPC etc.*

Introduction

Digital media has transformed the way individuals use and share data, and it is now an essential part of any company, be it public or private. By eschewing traditional media platforms, it provides users with a platform to effortlessly exchange ideas and information with a sizable portion of the public. People's ideas and opinions have been greatly influenced by social media. Data from social networking sites is a valuable resource for studying the exchange of ideas, perspectives, and opinions, among other things.[1]

Cybercrimes are offences committed using a computer. On the other hand, any illegal behaviour that involves a computer network or other electronic equipment is called a "cyberattack." Cybercriminals have easy access to our personal information on social networking sites, e-commerce websites, and other online services. They can also use advanced methods like malware to attack our social media personas. Making up a false online identity with the goal of libelling someone or obtaining

[1] Priyanka Mittal, Social Media Platforms and Cyber Crimes: An Entangled Relationship, Eur. Chem. Bull. ,12(Special Issue 7), 5558-5566.

their credit card number and other easily acquired information from online retailers is another tactic. Gender-based assaults and teenage attacks are two of the more serious types.

This is in addition to the previous revelations with kids allegedly planning to rape a young girl via social media. The Instagram problem is a contemporary illustration of the "Bois locker room." The chief of the National Investigation Agency (NIA), Alok Mittal, states that digital media is where every sixth cybercrime in India is recorded. In our country, there were about 250 incidents of digital media-related cybercrimes in 2019 and 400 cases in 2020.Furthermore, there have been instances where social media usage increased by 53% in 2021.

India is ranked third in the world for cyber bullying, as per a recent Microsoft Corporation report on the prevalence of online bullying among children ages 8 to 17. The poll revealed that 22% of children reported being cruel or unfriendly, 29% that they had been teased or made fun of, 25% that they had been called names, 70% that they were aware of cyber bullying, and 79% that they were concerned about it.[2] The National Society for the Prevention Cruelty of Children (NSPCC) discovered that almost one in five children who use social networking sites have encountered negative socialising experiences like bullying and unsolicited sexual messages.

Future higher education will surely be primarily conducted online, however "Protecting Children from Internet" is the fundamental barrier preventing widespread adoption of an online learning environment where information is freely disseminated via the internet. social networking sites' widespread use among youth, who primarily rely on the internet for communication, involvement, and education. [3]

Types of Cyber Abuse

The term "cyber abuse" has interpreted and defined in a variety of ways, depending on their study and subject-matter knowledge. Sameer Hinduja and Justin W. Patchin's research focuses on cyberbullying, which they characterise as wilful and persistent harm inflicted through electronic devices. Cyber violence, as defined by the World Health Organisation (WHO), is the deliberate inflicting of pain or suffering via the use of online platforms. This concept covers a broad spectrum of improper behaviours and activities. The Digital Trust Foundation (DTF) defines "cyber abuse" as the use of technology to damage someone else physically, psychologically, or emotionally. It recognises the complexity and diversity of harm caused by technology.[4]

Cyberbullying: An online abuse tactic known as "cyberbullying" is used. Digital communication tools, including social media, instant messaging, and online platforms, are purposely used to harass, threaten, or hurt individuals. Creating deliberate and repeated mental suffering, social isolation, or humiliation for their victims is the main objective of cyberbullies. Online and offline, this activity is possible. Numerous jurisdictions have enacted laws to address cyberbullying, and as a result, victims are now protected legally. Laws in various nations have varying aspects that are pertinent. A person's right to privacy may be violated, for instance, if they take, publish, or transmit a picture of a private area of their body without that person's permission. This is stated in Section 66E of India's Information Technology Act, 2000. In this section.[5]

In 2015, the highest court of the nation heard a noteworthy case called Shreya Singhal v. Union of India. In this case, the validity of Section 66A of the Information Technology Act—which outlawed the sending of pornographic electronic messages—was contested. The Supreme Court's decision declaring Section 66A unlawful brought to light the potential for misuse and infringement on people's right to free speech. This historic ruling acknowledged the need to safeguard people's rights to free speech while simultaneously shielding them from cyber bullying.

The Allahabad High Court heard the cyber bullying case Rajesh Kumar v. State of Uttar Pradesh (2019), in which the accused sent filthy and insulting messages to a woman on WhatsApp. The defendant was found guilty of violating sections 66A (sending offensive messages using a communication service) and 354D (stalking) of the Indian Penal Code, as well as section 66E (violation of privacy) of the Information Technology Act. The legal provisions pertaining to charges involving cyber bullying were clarified by this case. The Indian Penal Code and the Information Technology Act both have these clauses.[6]

In order to gain a better understanding of the prevalence of cyberbullying, numerous surveys and research studies have been conducted. In these types of studies, self-reporting is a common technique in which participants discuss their own experiences as cyberbullying victims or perpetrators. The findings consistently show that a significant number of people have been victims of cyberbullying in some way. However, it is important to recognise that cyberbullying may not be reported as frequently as it should be. Many cyberbullying victims may be hesitant to report incidents due to fear, shame, or a lack of knowledge about the available reporting mechanisms. Underreporting may result in an underestimation of the true prevalence of cyberbullying due to the possibility of underestimation.

[2] http://www.endcyberbullying.org/india-ranks-third-on-global-cyber-bullying-list/

[9] Gontard, *Buddhist Understanding of Childhood Spirituality: The Buddha's Children* 55-56 (Jessica Kingsley Publishers, London, Edition- 2017).

[6] *History and definitions of child Maltreatment* 13. available at: https://us.sagepub.com/sites/default/files/upm-assets/47853_book_item_47853.pdf, (visited on June 25, 2023. p.15).

Cyberbullying is detrimental to an individual's mental health and overall wellbeing. This could lead to worsening anxiety, despair, low self-esteem, and even thoughts of suicide. Cyberbullying can cause long-term psychological trauma, therefore seeking help from qualified professionals is necessary.[7]

Cyber harassment: The term "online harassment," also known as "cyber harassment," refers to repeated and unwanted behaviour directed at individuals via online platforms that causes distress, fear, or emotional harm. It includes targeted abuse campaigns, sending threatening messages, and using online platforms to stalk or intimidate others. Online harassment is addressed in the context of Indian law by applying relevant sections and case laws. The penalties for transmitting threatening or offensive messages via electronic communication were previously outlined in Section 66A of the Information Technology Act, which was passed in 2000. The Supreme Court of India ruled in the landmark case Shreya Singhal v. Union of India (2015) that Section 66A was unconstitutional because it could be abused and violate citizens' free speech rights. This decision recognised the importance of striking a balance between protecting individuals' freedom of expression rights and preventing online harassment.

Online abuse often follows gendered patterns and disproportionately targets women and members of underprivileged communities. Women occasionally experience sexist insults, sexual harassment, objectification, and threats of violence. Disenfranchised groups may be the target of harassment because of their sexual orientation, race, or religious affiliation. Targeted online harassment occurrences in recent times emphasise how critical it is to combat systematic prejudice and foster inclusive and courteous online environments.[8]

Revenge porn: This refers to the practise of publishing or disseminating private or explicit photos or films of someone else without that person's consent. Another name for this is "revenge porn." This is typically done in an attempt to degrade, embarrass, or otherwise coerce the person portrayed in the content. A person's privacy, autonomy, and trust may be violated when they participate in revenge porn, which can have detrimental effects on their mental and social functioning in addition to their emotional health. In India, publishing or transmitting pornographic material in an electronic format is punishable under Section 67 of the Information Technology Act, a 2000 law. Legal provisions pertaining to the sharing of explicit content, such as revenge porn, without the agreement of the individual are addressed in this section. It recognises that these activities have the potential to be harmful and works to shield people from the illegal sharing of personal images or videos.[9]

Obscene content: According to Section 67 of the Information Technology Act, sending or sharing pornographic material is prohibited and subject to penalties. In one of the major judgements, the Supreme Court defined obscenity as "offensive to modesty or decency; vulgar, dirty, and unpleasant. Additionally, the Supreme Court distinguished between pornography and obscenity.[10]In addition, criminals create pornographic content, edit photographs from social media, and post it online with no regard for the victim. The Hindustan Times reports that a man was arrested for creating, disseminating, and uploading images of Hindu deities on the internet.

Doxing: is a type of cyberbullying in which someone's private or personal information is illegally disclosed or published in a public forum without their consent. This could include information such as a person's home address, phone number, email address, and social media profile. The goal of doxing is often to harass, intimidate, or otherwise harm the victim, and this can happen online or offline. The perpetrators of doxing intend to expose the victim to multiple forms of abuse, including online harassment, offline harassment, and identity theft, by making this personally identifiable information (PII) public.[11]

Impersonation: is the act of taking on another person's identity, either online or offline, with the intention of misleading, defrauding, or causing harm to others. It involves taking on the identity of someone else in order to benefit personally or influence others. Impersonation can take many different forms, as the following instances show: One popular kind of internet imitation is social media impersonation. In this instance, someone creates a phoney social media account in the name of another and uses their profile photo to impersonate them. By using the person's name, profile photo, and other personal information, they might trick people into believing they are the real deal.

Impersonation is also a risk in professional situations. For instance, someone can pretend to be a licenced professional, such a contractor, lawyer, or doctor, in order to win over clients and reap the associated financial rewards. By making exaggerated claims about their qualifications or degree of experience, these impersonators deceive potential clients, which can lead to money loss, legal issues, or subpar and sometimes

[7] Pollock. L., *Forgotten children: Parent-child relations from 1500 to 1900* 234 (Cambridge, England: University Press, edition – 1983).

[8] Swaswati Das, *Social Life in Ancient India: 800 BC-183 BC* 147 (BR Publishing Corporation, New Delhi, 1994).

[9] Raj Kumar Sen and Asis Dasgupta, *Problems of Child Labour in India* 270 (Deep & Deep Publications Pvt. Ltd. New Delhi, Edition – 2003).

[10] Ranjit D. Udeshi vs. State of Maharashtra, AIR 1965 SC 881, Para 7, p. 885

[11] S. N. Tripathy and S. P. Pradhan, Girl Child In India 93 (Discovery Publishing House, New Delhi, Edition -2003).

dangerous advice or services.[12]Section 416 of the Indian Penal Code (IPC) pertains to the offence of deceit by impersonation and is pertinent to our issue. As mentioned in this section, a person found guilty of deceiving another person by adopting their identity or behaving purposefully under a fake persona may be subject to fines and/or imprisonment.

India's Cyber Security Infrastructure:

Different countries have varying degrees of cybersecurity infrastructure, depending on factors including their level of technological progress, the size and complexity of their digital networks, and the amount of money they have invested in cybersecurity. "Many nations have legislation in place to handle cybercrime, and law enforcement agencies in various countries, including the USA, the UK, and China, have created specialised teams to investigate and prosecute these types of offences."[13] Due to the widespread use of social media and the country's digitization, India must also have a robust cybersecurity infrastructure. Cybersecurity threats are constantly evolving, and the associated dangers are rising at a rapid pace. Following recognition of the threat, the Indian government has taken a number of actions to fortify its cyber security infrastructure.To control the rising number of crimes, Indian law has put in place a number of regulations. Its most notable example is the passage of the Information Technology Act in 2000. The IT Act of 2000 provides a legal framework for the prosecution of cybercrime and specifies penalties for a number of offences. The following are a few pertinent clauses from the 2000 Information Technology Act:

Section 43: This section of the IT Act applies to persons who perpetrate cybercrimes, such as damaging a victim's computer without that victim's consent. In the event that a computer is destroyed in this way without the owner's consent, the owner is fully entitled to a reimbursement for the entire cost of the damage.

Section 66B: This section outlines the consequences of acquiring computers or other electronic equipment that has been gained by fraud, including a maximum term of three years in jail. There could also be a fine of up to Rs. 1 lakh, depending on how serious the offence is.

part 66C: Digital signatures, password hacking, and identity theft in its various manifestations are the main topics covered in this part. This section carries a maximum sentence of three years in prison as well as a fine of one lakh rupees.

Section 66D: This section addresses using computer resources to pretend to be someone else in order to cheat. A conviction carries a maximum term of three years in prison and a maximum fine of one lakh rupees.

Section 66E: This law prohibits publishing or transmitting photographs of private areas that are taken without the owner's consent. Penalties for a guilty verdict include a fine of Rs. 2 lakh and/or a maximum sentence of three years in prison.

Section 67: This clause addresses the electronic publication of pornographic material. If proven guilty, there is a five-year maximum sentence in prison and a fine of up to Rs. ten lakhs.

Where the IT Act prove insufficient to encompass all cybercrimes, law enforcement agencies may concurrently employ the subsequent pertinent provisions of the Indian Penal Code:

Section 292: Originally intended to prohibit the sale of pornographic materials, this provision has now been broadened to cover a number of internet offences. The electronic sharing of young people's sexually suggestive or explicit actions or experiences is also covered by this section. Penalties for such offences include up to two years in prison and fines of Rs. 2000. For repeat (second-time) offenders, any of the aforementioned crimes may result in a fine of up to Rs. 5000 in addition to a maximum sentence of five years in jail.

Cybercrime is defined in Section 354C as the capture or sharing of images of a woman engaging in private or intimate activities without her consent. Since it is forbidden to watch a woman have sex, voyeurism is the only topic covered in this section. Sections 292 of the IPC and Section 66E of the IT Act are sufficiently broad to include similar offences in the absence of the criteria specified by this section. For first-time offenders, the maximum sentence is three years in prison; for repeat offenders, it is seven years.

Section 354D: Both offline and online stalking are prohibited by this section, which also defines it. Cyberstalking is the practise of reaching out to or trailing a lady using technology, like email or the Internet, even though she does not seem interested. For a first offence, this felony has a maximum punishment of three years in jail and a fine. For a second offence, the maximum sentence is five years in prison and a fine.

POCSO Act, 2012:

The Protection of Children from Sexual Offences Act was passed to safeguard children under the age of 18 against all sexual offences, including child pornography, sexual assault, sexual abuse, and sexual harassment. The POCSO Act's Section 11 defines sexual harassment. Anyone who regularly approaches a child via any form of electronic communication or makes threatening to use the child's body or involve the youngster in sexual activity—whether such threats are true or made up—is engaging in sexual harassment. The legal restriction against utilising children for pornographic purposes is outlined in Section 13 of the POCSO Act. The Act's Section 14 outlines penalties for employing a youngster in a pornographic manner.

Positive Steps taken by Government to curb Cyber Abuse:

The Digital Personal Data Protection Act, 2023 The Information pertaining to an identified or identifiable person is known as personal data. Personal data is processed by both government and business

[12] Nilanjana Ray, *wither childhood? child trafficking in India* 74 (Social Development Issues 29 (3): 72 - 82, January 2007).

[13] Bhaskar, U. and Kodackal, S. M. "Cyber Crime: A Review of the Evidence" (2011) 5(1) International Journal of Cyber Criminology 1-21.

organisations in order to provide goods and services. Processing personal data enables the knowledge of users' preferences, which is helpful for suggestions, targeted advertising, and customization. Processing personal data could benefit law enforcement as well. Unrestricted processing can have negative effects on people's privacy, which is acknowledged as a fundamental right. People could suffer from things like financial loss, reputational damage, and profiling as a result.

In order to provide stringent legislation Committee of Experts on Data Protection was established by the national government in 2017 to look into matters pertaining to data protection in the nation. Justice B. N. Srikrishna serves as the committee's chair. In July 2018, the Committee turned in its report. In December 2019, the Personal Data Protection Bill, 2019 was presented in the Lok Sabha, based on the Committee's recommendations. A Joint Parliamentary Committee was assigned the Bill, and it turned in its report in December 2021. The Bill was removed from Parliament in August 2022. A draught bill was made available for public comment in November 2022. The Digital Personal Data Protection Act, 2023 was passed in Parliament in August of this year.

Main Elements of this Act:

Application: The Bill covers the processing of digital personal data in India that is either (i) digitally collected offline or (ii) digitally gathered online. If personal data is processed outside of India in order to provide products or services in India, this will also be covered. Any information on an individual who may be identified from or in connection with such information is referred to as personal data. Processing is defined as an automated operation or series of automated processes carried out on digital personal data. It covers gathering, keeping, utilising, and sharing.

Consent: Only with the individual's consent may personal data be handled for a legitimate purpose. Prior to requesting consent, notice must be given. Information regarding the personal data that will be gathered and the reason for processing it should be included in the notification. The ability to revoke consent is always available. For "legitimate uses," which include the following, consent will not be needed: (i) a specific purpose for which a person has willingly submitted data; (ii) the government providing a benefit or service; (iii) a medical emergency; and (iv) employment. Consent will be given by the parent or legal guardian for those under the age of eighteen.

Rights and obligations of the data principal: The person whose data is being processed (the data principal) is entitled to the following: (i) information about the processing; (ii) the right to request the rectification and erasure of personal data; (iii) the right to designate a substitute to exercise rights in the event of the data principal's death or incapacity; and (iv) grievance redress. The roles of data principals will be specific. They are prohibited from: (i) filing a baseless or fictitious complaint; (ii) providing any misleading information; and (iii) impersonating someone else in certain situations. The punishment for breaking your obligations might be as much as Rs 10,000.

Data Protection Board of India: The Data Protection Board of India will be established by the national government. The Board's primary responsibilities are to: (i) oversee compliance and levy fines; (ii) instruct data fiduciaries on what steps to take in the event of a data breach; and (iii) hear complaints from individuals who may have been impacted. Members of the board may be reappointed after their initial two-year term. Specifics like the Board's membership count and the selection procedure will be set by the national government. TDSAT will hear appeals on the Board's rulings.

Lacunas in Data Protection Act 2023:

- Data collection, processing, and retention beyond what is necessary may result from exemptions to the State's right to handle data based on things like national security. The fundamental right to privacy might be violated by this.
- The Bill does not control the dangers that could result from processing personal data. The right to data portability and the right to be forgotten are not granted to the data principal by the bill.
- The Bill permits the transfer of personal data outside of India, with the exception of nations that the federal government notifies. It's possible that this process won't provide a sufficient assessment of data protection laws in the nations where personal data transmission is permitted.
- The terms of the appointments to the Data Protection Board of India are two years, after which they can be renewed. The Board's short tenure and possibility for reappointment could undermine its independence. [14]

Suggestions to prevent Cyber Crimes:

Numerous countermeasures can be employed in the fight against cybercrime. These defences include Education, one of the most effective ways to combat cybercrime is to raise awareness and spread knowledge. People must understand the risks associated with social media and how to protect themselves from cyberattacks. This entails teaching people how to recognise phishing emails and protect their personal information. Tools for cyber security like Firewalls, antivirus programmes, and intrusion detection systems are examples of cyber security technology that can help thwart cyberattacks. These technologies assist in preventing fraudsters from gaining access to private information by identifying and stopping unlawful communication. Strong passwords are essential for safeguarding personal data. Platforms should have robust security mechanisms in place, such as encryption, to prevent unauthorised

[14] The Digital Personal Data Protection Bill, 2023, Ministry of electronics and information technology, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

access to user information. They also need to alert users when they think their accounts have been compromised, and keep a watch out for any suspicious activities, such as persistent login attempts or strange behaviour patterns. Users on social media sites should have access to tools for reporting and blocking suspicious activity, such as spam, fraudulent accounts, and phishing scams. Two-phase verification: Two-factor authentication provides an additional degree of security by requiring users to provide two distinct forms of identification. password.

Every country has its own set of cyber regulations. In fact, the majority of nations lack distinct cyberlaws. Every country with computer infrastructure should adopt cyberlaws to discourage cybercriminals. Forensics should be prepared not only to stop cyber incidents but also to collect evidence to bring criminal charges against those responsible. It should be tried to create Cyberlaws who are all the same. A true international treaty to police cybercrime through international cooperation is desperately needed, and such treaty is the Cybercrime Convention. A comprehensive strategy is needed for cybercrime prevention and controlling measures. When creating strategies to counter cybersecurity risks that erode confidence and trust in the online environment, cooperation between the public and private sectors, as well as users, is essential.

Changing Passwords Frequently: Since the introduction of multi-user systems, password security has been essential. Passwords to sensitive data should therefore always be kept secure. This can be achieved by regularly altering them and initially keeping them suitably complex. Make sure the password is secure. Safe Surfing: Every user on a network should adhere to safe surfing practises. Maintaining the privacy of one's email address, avoiding open networks where conversations take place without proper security measures, and sticking to secure websites are all part of safe browsing.

Risk can also be reduced by accepting data from only verified persons, downloading files cautiously, and only from reputable websites.

Conclusion

Cybercrime is already a significant issue on a global scale, and it is spreading quickly. Cybercrime is not only a legal issue but also a social one. Use of strategies and tools, such as the judicial system, peer pressure, and new and developing technologies, is required to stop cybercrime. In the absence of sufficient measures to safeguard against cyberattacks, the entire globe will undoubtedly experience catastrophic cyberattacks that will do severe damage to our economy and result in fatalities. Collaborative efforts and the exchange of knowledge and skills across several domains are the only ways to combat cybercrime. If cybercrime is to ever become a manageable issue, policymakers, businesses, and consumers must all adopt a consistent strategy.

Myths and mythology have always been considered to be primordial and universal. George Grote, a Greek historian is of the opinion that “myth belongs to a past that has never been present.” (qtd in Connor 263). It is due to this “temporal deracination” that makes myth universally accessible and literature and culture seem to draw from it without the fear of the myth getting depleted. (Connor 263)

While myth as a category in literature started establishing around the eighteenth century, it was considered a metaphysics that was felt and imagined without the power of ratiocination. Thinkers like Giambattista Vico, Gottfried Lessing, J.G Herder, Schlegel Brothers, Gottlieb Heyne started exploring myths in order to understand human culture. The Romantic writers found their sources of writing in the myths. In the 19th and 20th century, myths were renewed to make sense of the modern world as T.S Eliot, W.B. Yeats used in most of their poems. It was during this time, that the Indian middle class was formulating its nationalist discourse in order to rebel against the powers of British colonialism. Revival of myths and looking back at a golden fabled past became the steering thought for the nationalist discourse.

Meenakshi Mukherjee in the chapter “Myth as Technique” talks about the importance of myths in the study of literature. She writes:

> One reason may be their quality of timelessness. Myths, in spite of their distance from contemporary reality, do have, for that particular group of men to whom they are culturally relevant, a kind of fundamental significance. (Mukherjee 134)

She further writes pertaining to the Indian context that the epics have served as a common background for literary works:

> If a world – view is required to make literature meaningful in terms of shared human experience then the Indian epics offer a widely accepted basis of such a common background which permeates the collective consciousness of the whole nation. (135)

While the writers like Raja Rao, Sudhin Ghose, R.K. Narayan, B. Rajan have employed the Indian mythology in their literary works. However, in this paper we shall concern ourselves with the use of mythology in Indian English children’s literature.