

Legal Frameworks and Policy Gaps in Protecting Children from Online Exploitation in India: Challenges and Solutions

Aadhavan V¹, Keerthivasan T.K²

^{1,2}Studnets, 5th year B.A.LL.B.(Hons.)

ABSTRACT:

The swift expansion of internet in India has opened up numerous opportunities for kids. This includes chance to learn access information and connect with others. However, it has also exposed them to serious dangers. These include being exploited online subjected to abuse and at risk of trafficking. This study critically evaluates legal and policy strategies in place to shield kids from online exploitation in India. It pinpoints major shortcomings and obstacles that weaken their impact. The legal environment in India for protecting children includes various laws like Information Technology Act, 2000 Protection of Children from Sexual Offences (POCSO) Act, 2012 and Juvenile Justice (Care and Protection of Children) Act 2015. Although these laws are strong in theory, they encounter challenges in application. Factors such as a lack of resource and a low level of public awareness contribute to this. Moreover, the rapid developments of digital advancements often lags behind legislative updates. This leaves children to new online dangers like cyberbullying and sextortion. This study delves into these legal and policy deficiencies by examining recent cases. It reviews existing research on child safety online. Additionally, the paper looks into responsibilities of private sector entities. This includes social media companies and internet service providers in preventing and responding to online exploitation. Such aspects are not fully covered by current legal framework. To address these issues paper suggests various measures. It includes improved training for law enforcement. Additionally it involves the formation of specialized cyber protection units aimed at safeguarding children. It also calls for stronger cooperation among government agencies, non-governmental organizations and private sector to foster a safer online space for children. Furthermore paper highlights the need for digital literacy and awareness programs for children, parents and educators as a way to prevent online exploitation. This research adds to the understanding of complexities involved in protecting children from online exploitation in India. It provides actionable recommendations for enhancing the legal and policy framework to effectively tackle this critical issue

KEYWORDS: Cyberbullying, Online Exploitation, Child Safety, Digital Literacy.

INTRODUCTION

Online exploitation of children is a fast-growing global phenomenon, and India is no exception with its vast population and high internet penetration. As children increasingly spend time online, they expose themselves to various threats from Internet use, such as cyberbullying, grooming, and online sexual exploitation. This problem calls for strengthening and supplementing the current legal frameworks that exist and the launching of new policies to tackle this specific challenge of the digital land exclusively.

This piece will begin by reviewing the current legal and policy frameworks of India, scrutinizing the functioning of each one, followed by recommendations for a holistic approach to protecting children from this online world. Past and Present Legal Frameworks in India India has enacted a number of laws and policies to counter child exploitation, including the Protection of Children from Sexual Offences (POCSO) Act, 2012; the Information Technology Act, 2008; and the Juvenile Justice Act, 2015. Nonetheless, gaps do exist in most of the legal frameworks regarding effective protection of children from online exploitation. For instance, in the POCSO Act, no provisions are found regarding technological devices-related crimes, like child sexual abuse material production, distribution, and possession. Information Technology Act focuses on cybercrime but does not provide any provision about the issue of children being exploited through the online platform. The legal frameworks must be revisited and revamped to harmonize with the modalities of changing manifestations of online abuse. The legislation must be multilateral, thus covering all the roles of online child exploitation such as grooming and recruitment, and ensure penalties for exploitation in cyberspace are severe enough to discourage the perpetrator. In addition to developing the legal frameworks, this would entail equipping law enforcement agencies with the necessary tools and resources to make practical investigations and prosecution of online child exploitation cases. This would involve training law enforcement officers on specific advances in the latest technologies and investigative techniques on online child exploitation. Another improvement area would be in evidential collection and tracking of offences that could ensure high productivity for law enforcement agencies in the fight against online child exploitation. There also has to be the establishment of a framework that encourages public-private partnerships against online child exploitation. In this effort, the development of these public-private partnerships can evolve into sharing resources, expertise, and technology between private industry and the government regarding the detection and prevention of online child exploitation. Such partnership can include, among others, initiatives on child safety on the internet, parenting/child education programs on risks from the internet, and the development of technological solutions for identification and reporting as well as prevention of such offenses.

The parents of children, teachers, and caregivers themselves should be briefed on the danger and how they can recognize it. Outfitting them with basic knowledge and power tools on these issues would provide a proper avenue to address these issues with their children and monitor them on their usage without invading their privacy. This can be achieved through the promotion of age-specific educational materials for children and modules for adults on responsible technology use and the risks of online child exploitation. Furthermore, there is a need to implement and enforce stringent penalties for individuals who engage in online child exploitation.

BACKGROUND AND RATIONALE

Unlike adults, children are much weaker in their ability to protect themselves from the negative or damaging effects of the digital world. For services and products that are increasingly available—in particular, in urban areas—the mechanisms necessary for dealing with their negative effects are almost entirely absent. This includes exploitation of various types in physical and virtual space.

Online Child Pornography (OCP) entails depicting children in sexual scenes as prescribed under section 67 (2008) of the Information Technology (IT) Act, 2000. It is one specific form of child sexual exploitation and, in the opinion of international bodies, represents a 'failure of domestic systems to thwart this'.

There are still serious, yawning policy gaps in terms of defining minimum or core standards for children about age-appropriate governance, on the one hand, and specific laws that may be necessary to address

the different forms through which children can be exploited in the digital world. It is a universally acknowledged fact that India does not have any specific domestic law governing issues of OCP, such issues are dealt with as part of the large corpus of laws which deals generally with the issues of children, legal documents outlining preventive, penalizing, protective and auxiliary provisions in India to address OCP in children. It has also been hypothesized that this approach has not necessarily prevented the character and the scale of the problem from being addressed appropriately.

In fact, offenses against children have been criminalized under such provisions as the National Commission for Child Protection Act, 2005; the Juvenile Justice (Care and Protection of Children) Act, 2000; the Immoral Traffic Prevention Act, 1956; the Indian Penal Code 1860; the Protection of Children from Sexual Offences Act, 2012; and the Prohibition of Child Marriage Act, 2006. In this area, India has ratified and adopted six main conventions. However, in consideration of the possibility of permitting countries to formulate legislation according to their requirement, the United Nations Office on Drugs and Crime had already developed a Model Law Related to Child Pornography Offences and setting up a legal framework so that international cooperation may be made effective. This requires all-round legislation that specifically covered the problem. The issue has been pointed to by several practical, policy-based and enforcement challenges, thus requiring a scrutiny of the existing legislative framework applied to online exploitation.

LITERATURE REVIEW:

1. Research Note on Online Child Pornography Law in India Rahul:

Prior to the IT Act of 2008, India had no specific law addressing online child pornography, instead relying on general obscenity laws. After international pressure and signing the CRC-OP, India enacted Section 67B of the IT Act in 2009, followed by POSCO in 2012 to criminalize different aspects of child pornography. The IT Act targets production, publication, and distribution of child porn in various forms, while POSCO criminalizes the use of children in pornographic media. Both laws carry severe penalties for offenders. Intermediaries transmitting child porn are also held liable under the strict liability of Section 67B, but can use a due diligence defense. Intermediaries must follow guidelines to disable harmful content promptly upon complaint. Enforcement of child pornography laws in India remains weak, with few cases reported under both the IT Act and POSCO. UNICEF has urged for stronger legislation and mechanisms to combat child pornography. The government has taken steps to improve enforcement, including establishing e-boxes and a national helpline to report child pornography. Courts have also taken a tough stance on child pornography, with the Supreme Court directing a ban on websites containing such content and examining filtering mechanisms. Ongoing efforts include consultations with stakeholders and the consideration of a National Alliance against Online Child Sexual Abuse and Exploitation. Child pornography offenses are treated seriously by the Indian courts, as evidenced by recent actions against offenders. There is a clear push towards stronger enforcement of laws to protect children from online exploitation.

2. CRIME AGAINST CHILDREN IN CYBER SPACE IN INDIA: A SNAPSHOT Mr. Rahul¹, Shaifali Choudhary,² Maryam Azhari

Children are vulnerable to online exploitation, leading to rising instances of child abuse and exploitation through "sex tourism" and "people trafficking." Offenders use false identities to lure victims into in-person meetings, resulting in long-term repercussions for victims. Parents and older people must educate children on safe technology use to prevent cyberbullying. Cybercrime, including child exploitation, is

difficult to apprehend due to criminals using cutting-edge technology. Advances in technology have increased the risk of exploitation, such as the production of "made-to-order" child sexual abuse materials. Grooming, cyberbullying, online transaction fraud, gaming, and email scams are common forms of cyber threats targeting children. The Indian legal system has various provisions to address cybercrimes, including the Information Technology Act and Protection of Children from Sexual Offenses Act. Offenders face severe punishments, including imprisonment and fines, for crimes against children. Strengthening laws and raising awareness are essential to combatting child exploitation and cybercrimes in the digital age.

3. Child Protection in India: Issues and Policies Nidhi Marothiya, Shraddha Kapoor and Vinita Bhargava PhD Scholar, Department of Human Development and Childhood Studies, Lady Irwin College, Delhi University, India.

The failure to protect children globally is a major violation of their rights, impacting their well-being. Child protection policies like the JJ Act, CHILDLINE, and the POCSO Act have been launched by the Government of India to address this issue. Despite these efforts, many children die each year due to abuse, neglect, and exploitation. It is vital to raise awareness about legislation and prevention of child abuse to create a safer world for children to grow up in. There is a lack of knowledge among the public in managing child abuse in emergency settings, creating a gap in child protection services. Education and awareness are crucial in addressing this issue and ensuring a better future for children.

4. Challenges in Child Rights and Child Protection in India Dr. Dakshina Saraswathy, Associate Professor, Kerala Law Academy, Thiruvananthapuram

Protecting and defending children's rights is crucial in all cultures, including in India where children face issues like abuse, exploitation, and bullying. The status of children in Indian society, along with problems like child labor, child marriages, and sexual abuse are examined, as well as laws, implementation challenges, and the role of grassroots organizations in advocating for children's rights. To ensure a safe and healthy upbringing for every child in India, a comprehensive strategy must be enacted, utilizing infrastructure and services. However, gaps in institutional connections and compliance hinder the effective implementation of child protection laws and programs, making it imperative to address and overcome these obstacles to create a nurturing environment for all children.

5. CHILD PROTECTION IN INDIA , NICOLE RANGEL MENEZES

Child protection in India is influenced by various indicators such as health, crime, and education. The country's preference for sons is evident with 82 girls dying at birth for every 1000 boys born. States like Haryana, Punjab, and Rajasthan have high rates of crimes against children, showing a 500% increase since 2006. The implementation of laws like the POCSO 2012 has led to a spike in reporting crimes against children. Despite achieving universal primary school enrollment, dropouts increase as students progress through school, especially among marginalized groups. Issues like lack of interest, domestic responsibilities, and financial constraints contribute to the dropout rates. India's complex societal issues, including poverty and discrimination, contribute to child protection challenges. Concerns around online safety are also emerging, with millions of children having access to the internet, exposing them to cyberbullying and other online dangers. While there is a push for increased digital access, there is a lack of awareness and resources to address online abuse and exploitation of children. Legislation and services need to be updated to effectively respond to these threats and protect children in the digital age.

Research problem:

Presently, the laws and policies of India are not putting enough effort toward protecting children from the increasing threats of online exploitation. This is creating considerable gaps in prevention, detection, and prosecution, which put millions of children at risk. There is a need for the review and reform of existing laws and policies to further guarantee children's safety and rights on the internet.

Research objectives:

- To review and assess the current laws and policies that protect children from online exploitation in India.
- To identify the weaknesses and challenges in enforcing these laws and policies.
- To explore the role of important groups, such as law enforcement, policymakers, and internet providers, in tackling online exploitation of children.
- To suggest practical legal and policy changes, using examples from both India and other countries, to improve child protection in India's digital space.

Research question:

- What are the present key legal frameworks in India that could be used to protect children from online exploitation and how those are being implemented well.
- What are the major policy gaps preventing the protection of children from online exploitation in India, and the potential causes of such gaps.
- How the roles of law enforcement agencies and internet service providers affect the efficacy of legal protections for children against online exploitation in India. (challenges in terms of enforcement)
- What are all effective legal and policy reforms in strengthening the protection of children from online exploitation in India, and how can be closely related to exploring the solutions for effectively implementation.

Research hypothesis :

The urgent need for a specific and agile legal architecture ensures comprehensive protection of children in the digital world is keenly felt as India's legal frameworks, such as the POCSO Act and the Information Technology Act, are woefully deficient in responding to the changing formats of online child exploitation, therefore leaving enormous policy gaps as an impediment in the efficient conduct of prevention, detection, and enforcement measures.

Research methodology:

The study employs a doctrinal research methodology, emphasizing the promotion of constructive modifications to the legal system. It also uses an analytical approach, which makes it possible to do a thorough investigation of the body of existing literature. The study makes use of both deductive and inductive reasoning, which makes it easier to generate fresh ideas based on previously published research. Through the application of both qualitative and quantitative methodologies, the research depends upon pre-existing academic literature for its conclusions rather than obtaining original data from people or organizations.

Research method:

The current study uses the secondary data collection method, which comprises reading, analyzing and examining over previously published materials, like journals and other written works related to the topic. The production of this work, which is fully reference based involved secondary research method. The legal framework and legal issues covered in the paper are explained using primary data.

Understanding Online Exploitation of Children

Child exploitation through cyberspace has become a major concern for India as the increasing penetration of the internet exposes vulnerable children to a variety of online threats. Child pornography, cyberbullying, online grooming, and trafficking are a few of the grave threats. Social media sites, games, and other messaging apps have predators lurking around, taking advantage of children for their gainful illegal purposes. Along with the Prevention of Children from Sexual Offences (POCSO) Act and the IT Act, there exists a dearth of appropriate digital literacy amongst children and, particularly the parents. The government, together with civil society organizations, is working to heighten awareness and reporting mechanisms. Yet, to make the internet safer and serve as deterrents to the exploitation of children in cyberspace, coordination among schools, parents, law enforcers, and tech companies must be established. Definition and Forms of Online Exploitation: Online exploitation of children refers to harmful activities wherein the internet is used to abuse or take advantage of children. This may include inciting children to send inappropriate images or videos, grooming them online through their winning of trust to later exploit them, and cyberbullying or other harassment or threats forwarded through the internet. It also addresses concerns such as child trafficking, forcing children into labor, and exposing them to harmful content. All these could be on social media platforms or the gaming and messaging apps without the children realizing the full risks of these activities. The protection of children online will require awareness and strict security measures.

IMPACT ON CHILDREN: Online exploitation to a child can be very severe and long-term. Children are characterized by emotional and psychological upset when they encounter abuse or harmful activities on the internet. They fear, worry, become depressed, and suffering from shame or guilt. Some children face trust issues when they interact either online or offline and feel unsafe online. That affects their academic performance and their social relationships. Trauma also leads to mental problems such as low self-esteem and, in extreme cases, self-harm. Children may become reclusive or withdrawn, losing the confidence to play with others. Such experiences can be curbed early by intervention and support from parents, schools, and professionals.

Legal Structures to Protect the Child in India

The POCSO Act and the IT Act of India protect their children from exploitation, which could be targeted either online or offline. POCSO aims to punish the abusers and safeguard their rights in making children safe from sexual abuses, traffics, and cyber-related crimes.

Constitutional Provisions: The Indian Constitution, in its provisions, promises a few significant things that would keep the child safe, healthy, and develop. Article 15(3) gives the power to the government to enact special laws for the protection and welfare of children, which always remain at the vulnerable end of society. This is the legal provision that empowers the government to bring child-friendly legislation and policies. Article 21(A) ensures that every child between six and fourteen years of age has a right to compulsory free education. This provision aims at eliminating child labor and increasing literacy, where every child is provided with an education. Article 24 prohibits human trafficking and forced labor. It protects children from being exploited for illegal work or other ill practices. Article 24 clearly states children below the age of 14 must not be employed in hazardous industries that may be dangerous for child labor. Article 39(e) and (f) requires that the government ensures that children should not be abused or employed in harmful work and grow up in sound, clean, and healthily conditions. It calls for well-being of children and presents a challenge to the government to protect them and create a conducive environment

to raise and develop the children 3.2. NATIONAL LEGISLATIONS: There exists a high profile set of rules in India where children are protected from the acts of exploitation and abuse.

The main laws among these include the Protection of Children from Sexual Offences (POCSO) Act. It relates to any kind of sexual abuse, harassment, or pornography involving children. It ensures an exemplary punishment for culprits and guides child-friendly procedures for trials. The Juvenile Justice (Care and Protection of Children) Act mainly looked towards the care, protection, and rehabilitation of children in conflict with the law or those who are in need of care. It ensures a child-friendly approach in dealing with children involved in legal matters. The Child Labour (Prohibition and Regulation) Act banned the employment of children below 14 years in hazardous occupations, as a way of ensuring their safety and education. Apart from this, RTE Act has a special place in the Constitution by incorporating Article 21 (A) which provides free and compulsory education to children between 6 and 14 years to enhance their education and overcome child labor. These laws complement each other to safeguard children against wide ranges of abuse, exploitation, and neglect. Thus, the rights of the child are protected, and they are cared for to become better citizens in India. a) India is a signatory to various international instruments and treaties regarding the protection of children's rights. Notably significant is the United Nations Convention on the Rights of the Child, which India has adopted and ratified in the year 1992. The principles in the treaty ensure that every child, irrespective of which country he is from, has the right towards his survival, development, protection, and participation. In addition to these, the treaty ensures that children are not violated, abused, neglected, or exploited. b) India is also signatory to the Optional Protocols of the UNCRC, including protection from the involvement of children in armed conflict and the sale of children, child prostitution, and child pornography.

c) Country has ratified other international conventions, for example, ILO Convention on the Worst Forms of Child Labour No. 182; prohibits work that exploits children in dangerous conditions; and sets the minimum age for employment (ILO Minimum Age Convention-No. 138).

d) India is obligated to adhere to and implement laws that would safeguard children from the multifaceted exploitation and adverse consequences by ratifying such international treaties. The aforementioned conventions generally facilitate the striving of India towards the protection of children's rights as well as promoting welfare of children at both domestic and international levels.

Role of law enforcement agencies and internet service providers: Lack of Technical Expertise: A large number of Indian law enforcement organizations are devoid of the technology know-how required to efficiently monitor, look into, and prosecute incidents of online child exploitation. Many organizations lack the specialized training and equipment needed to combat cybercrimes, particularly those employing encryption, anonymous browsing, and the dark web. Jurisdictional Issues: Because online exploitation frequently transcends national boundaries due to the worldwide nature of the internet, it can be challenging for local law enforcement organizations to handle such instances. Enforcement operations are made more difficult by the lack of recognized structures for international collaboration. Resource Limitations: A growing number of cybercrimes has left many Indian law enforcement organizations underfunded. Timely and effective responses to allegations of online child exploitation are hampered by a shortage of personnel and state-of-the-art investigation technologies.

Internet Service Providers (ISPs): Inadequate Content Filtering: ISPs frequently lack robust systems to filter offensive information, such as child sexual abuse material (CSAM). Although some ISPs actively work to restrict unlawful content, others are either unwilling to invest in these technologies or lack the necessary technical infrastructure. Encryption and Data Privacy: As encrypted communications become

more common, it becomes more challenging for ISPs to identify or stop detrimental child exploitation-related actions. This has grown to be a major problem because encryption systems safeguard consumers' privacy while simultaneously making it difficult to catch criminals.

Policy gaps and challenges: The absence of a thorough, specialized legal framework that particularly addresses the various and changing forms of online child abuse, such as cyberbullying, grooming, and the distribution of child sexual abuse material (CSAM), is a significant policy gap impeding India's ability to effectively protect children from online exploitation. Although some parts of online exploitation are illegal under laws like the Protection of Children from Sexual Offences (POCSO) Act and the Information Technology (IT) Act, these rules were not created to completely address the special difficulties presented by the digital realm.

Internet anonymity: Because of the anonymity offered by the internet, it is challenging for law enforcement to find, trace, and capture criminals. The internet's worldwide reach and anonymity make it more difficult to implement current laws and handle jurisdictional concerns.

Lack of Digital Literacy: Parents, kids, and even law enforcement officers are not well-informed on the dangers of online exploitation and the resources available to prevent it. Both underreporting of occurrences and insufficient supervision of children's online activities are caused by low levels of digital literacy.

Lack of Digital Literacy: Parents, kids, and even law enforcement officers are not well-informed on the dangers of online exploitation and the resources available to prevent it. Both underreporting of occurrences and insufficient supervision of children's online activities are caused by low levels of digital literacy.

Insufficient Law Enforcement Training: Many law enforcement organizations lack the technological know-how and specific training necessary to address online crimes against children. This makes it challenging to properly look into and prosecute incidents of online abuse, especially when cutting-edge methods like encryption or complex anonymization technologies are employed.

A lack of coordination amongst agencies: The issue is made worse by a lack of collaboration between government offices, tech firms, and civil society groups. Without strong alliances, the prompt action and cooperation required to stop online child exploitation would not be possible.

IMPLEMENTATION MECHANISMS:

India has very clear laws against child exploitation online that make it uncomplicated to protect children from more nefarious clicks on the internet, such as the POCSO Act and the Information Technology Act. However, there lies an implementation gap. There is less digital literacy within these children and parents. This makes it that much more challenging to spot these dangers and report them. More often, monitoring and arresting the culprits in the cyber space becomes challenging for the law enforcers due to the anonymity of the internet. Mostly, there are under-resource units such as cybercrime units equipped neither with the most recent tools neither trained adequately to deal with all crimes committed online involving children. The reporting mechanisms are mostly inaccessible or inconvenient, thus becoming hard for the victims to come out. Thirdly, there is a lack of trained personnel to carry out child-friendly investigations and court procedures that delay justice. Lastly, the awareness and coordination between the stakeholders, including the social media, law enforcement agencies, and the government departments, are still evolving. Lack of coordination stands to dilute the strength that these laws intend to give children when being protected from online exploitation. More focused efforts must be made to better implement the already legislated laws.

Interagency Coordination: Successful protection of Indian children from online exploitation would require effective interagency coordination. It is only when different types of organizations and government bodies come together that the issue can be seriously addressed. Important players are police, cybercrime units, social media platforms, education departments, and child protection agencies.

Each one of these agencies has a part to play in the task:

- The police have to start investigations and prosecute offenders in the virtual world.
- Content service providers and social media organizations monitor and report inappropriate content and provide support for their victims.
- Education departments can offer digital literacy programs for children in addition to their parents, to recognize the dangers of the Internet.
- Agencies responsible for protecting children may even offer counseling and support for the victims.

Better coordination would translate into the right flow and distribution of information as well as resources to ensure concerted efforts in combating online exploitation. Such improvements could be hastened through constant meetings, shared training with the members of the agencies, and more defined lines of communication. Together, such agencies can prevent the internet from giving a way to harmful exploitation of children as well as respond speedily to such incidents.

Technological development: (A COMPARATIVE ANALYSIS OF INTERNATIONAL STANDARDS AND INDIAN LEGAL PROVISIONS ON CHILDREN'S PRIVACY, Journal of Fundamental & Comparative Research Vol. IX, Issue-II, Book No.07, July – December: 2023 ISSN: 2277-7067)

The revolutionary development of technology has enhanced the style of children's socialization, learning, and communicating. Technological advancement, in itself, has brought a multitude of unimagined opportunities, but it also exposed the minors to multifaceted risks of privacy. Consequently, social media sites, online games, educational applications, and Internet of Things-related tools became a part of the children's lifeworld while fueling several concerns over privacy and data security, illegal online crimes, and inappropriate age-related content exposure. Moreover, the prevalence of smart devices along with social networking apps also raises the likelihood of cyberbullying, online grooming, as well as unauthorized access to personal information all of which is indicators of the vulnerabilities of minors in the digital world.

New threats: (Child Online Safety: A Select Study in Indian Context Thesis submitted in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY by DITTIN ANDREWS, SCHOOL OF MANAGEMENT, NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA, SURATHKAL, MANGALORE – 575025, DECEMBER, 202) The types of internet threats are mainly categorized as: i) harmful advice, ii) harmful content or age-inappropriate, and iii) illegal content. The threats that occur from the internet are narrowly segmented and vary according to the level of risks and other factors, including the age of the child and their resilience.

Harmful advice: Generally, it is more challenging to manage this kind of content with harmful advice. As it can be spread on Web 2.0 applications by anyone, including children and minors, besides it is challenging to differentiate between helpful or harmless advice and harmful advice because data related to this concept can mix wellintentioned with potentially harmful advice.

Age-Inappropriate Content and Effect on Children: Millions of internet sites harbor age-inappropriate contents like pornography, hate speech, and violence that affect the growth of children. Even though such contents may be legal in most countries, they can negatively impact the minds of young people. Children often access such material inadvertently in their internet search or recommendations by friends. Online

video games that constitute interactive media are some of the ways violence can be portrayed; hence accessible to minors. While the internet is not always regulated for child audiences, unlike traditional media, children can access harmful content-including misleading domain names. Research shows that exposure to pornographic and violent content does harm children and an immense amount of research has already been conducted concerning risks for children worldwide. Stronger regulations and public awareness should be the first steps toward this end.

Illicit content: Content whose publishing is illegal and different country by country within administrative borders. In most countries, promoting hate speech, racism, bestiality and other issues of inequality are unlawful. However, in most countries the content on children sexual exploitation is illegal though the frequency of the content associated with children's sexual exploitation is not known or significantly less.

Cyber-grooming: In most countries, such activities as the use of the internet by an adult to achieve a desirable relationship with a child through the use of the internet, including sexual contact, are generally considered a crime. Cyber-grooming seems to be somewhat problematic in terms of legitimacy. It would possibly start with the falsification of the real age of the adults to win the affections of the child. Moreover, in many cases, it has been noted that there is no deception of any kind in the online or offline relationship at any stage; sometimes, it comprises legal minors or young adults (Dooley et al., 2009). Noticeably, it does not lessen the adult's accountability who thinks about the benefit of childhood innocence. It is a call for a very difficult-level understanding of prevention or how to handle this kind of condition.

Cyberbullying and online harassment: Cyberbullying is a new risk for children, starting from humiliation and intimidation, which increases the chances of cyberbullying. Cyberbullying is understood as the repeated, wilful harm through digital communication such as messages or posts, in which both children and adults can be involved. This type of harassment is based on the anonymity of the internet. Victims as well as perpetrators, children may engage in behaviors like "flaming" or "cyberstalking," hostile arguments that are persistent and harmful. As more and more children use smartphones, cyberbullying is becoming increasingly prevalent, particularly for older children. "Sexting"-exchanging explicit nude or semi-nude images-involves significant risks, as photographs might be published, creating lifelong privacy violations. These bring the call for stricter measures to be implemented in the safety of children while online.

Role of Technology in Protecting Children

Technological Solutions: Technology will largely protect the child from the dangers of the net since he or she gains access to it at various stages in life, which may be through study or entertainment among others. Solutions for parents, including good parental control software, content filtering tools, and monitoring apps, are imperative to ensure that this online experience is safe for them. The tools enable provision of boundaries to harmful content, monitor children's activities as well as block inappropriate content. The social media platforms and gaming apps have built in-safety measures, including age verification systems ensuring reporting of inappropriate behavior. AI-driven moderation tools ensure all forms of harmful content are removed before it reaches children. Online educational technology platforms provide an online safe and school-friendly learning environment. However, such solutions can only work effectively if upgraded regularly to meet the changing times of the digital landscape.

Ethical Considerations: Technological solutions are crucial for online safety, but they also raise ethical concerns. Parental control and monitoring apps can potentially infringe on a child's privacy, making it difficult to balance protection with respect for their autonomy. Data privacy is another concern, as tools

designed to protect children collect large amounts of data about their online activities. AI-based systems can be overly restrictive or too lenient, and their transparency makes it difficult to assess their fairness and effectiveness. The digital divide also poses a challenge, as children from disadvantaged backgrounds may not have access to the latest technology, making them more vulnerable to online risks. Ensuring equitable access to protective tools is essential in the larger ethical debate surrounding child safety online.

Awareness: With rapid internet access and smartphone use, India stands at both opportunity and risk for children, particularly in education, entertainment, and social communications. This calls for the need for pressing the issue to enhance online child safety awareness. Government and other public campaigns are conducted to educate parents, teachers, and children about the risks of cyberspace. The Cyber Swachhta Kendra advocates guidelines for safe and improved usage of the internet. Schools' digital literacy programs have also been promoted, which equip students with necessary knowledge on cybersecurity as well as responsible behavior in online activities. NGOs and advocacy groups like Save the Children and Cyber Peace Foundation run awareness programs that serve as resources to avoid such unsafe online behavior. However, India has a broad digital divide so that most children browse the web without proper education or supervision, as internet illiteracy among parents and guardians is rampant in the country.

Recommendations and Policy Implications:

Legislative Reforms: as the web continues to grow and develop, threats and risks become more apparent in the digital world for children. On these grounds, most of the current legislation offers a degree of protection, but they are just not sufficient enough to address the important questions raised in the digital arena, especially as was followed in the Information Technology Act of 2000 and POCSO Act. Cyberbullying has advanced rapidly while the cases of online grooming and exposure to harmful content as well as data privacy violations require, therefore, a renewed push for an overarching child-specific legal regime specifically designed for securing children online.

A standalone statute outlining crimes that are committed against children in the digital space is better to address this issue. Digital exploitation, which includes child offenses online, should be recognized and considered while deciding the case. This law should govern digital platforms while establishing clear boundaries of liability among the stakeholders, including the technology companies, parents, and educators, and delineate clear expectations with regard to dealing with digital exploitation. A proper statute should also respect the rights of children concerning privacy and independence while meting out severe punishment to the perpetrators.

The most important thing for the government to achieve proactive and effective child protection online is a very specialized legal framework that can evolve with technology. International cooperation will feature in it in consideration of international cooperation against such crimes as online child abuse and exploitation, it will augment knowledge and enhancement of enforcement, thereby strengthening protection mechanisms for children.

Capacity Building Initiatives

Thus, capacity building programs are therefore very important to empower people and communities to protect the young user from the increasing dangers of this digital world. They are helpful for parents, educators, law enforcement, and children in developing knowledge, skills, and resources, which establish safer online environments. School is expected to play a significant role in the education of the net world, and all initiatives now focus on including modules in their curriculum that cover cyber safety. Training

programs for parents form another significant capacity-building area wherein parents are educated about digital tools, parental control software, and how to speak to their children about internet safety. Training law enforcement and child protection agencies on recognition and response to cases of online child abuse, cyber grooming, and exploitation. Capacity-building for NGOs and community-based organizations occurs through grassroots activities with outreach programs and workshops in local communities to create awareness about the safety of children online. Initiatives like Google's Be Internet Awesome or DigiSafe in India are usually child centered, teaching children basic digital skills, training them to be responsible digital citizens.

Conclusion:

The increasing prevalence of online exploitation of children in India necessitates a comprehensive reevaluation and enhancement of existing legal frameworks to effectively address the evolving digital threats. Strengthening these laws, alongside fostering public-private partnerships and raising awareness among parents and educators, is essential for creating a safer online environment for children. The phenomenal growth of Internet access in India has proved to be a double-edged sword for children. As the internet offers unprecedented opportunities for learning and socialization, it also throws open dangers like cyberbullying, grooming, and online sexual exploitation. The present laws on the issue are very important-law like the Information Technology Act and the Protection of Children from Sexual Offenses (POCSO) Act-which have yet to do justice to the issue. Online child exploitation is a challenging issue, and the fact that digital threats keep changing implies that these laws should be reviewed and widened to conform to new technologies and criminal techniques. These threats need a holistic approach to counter them. It is not only a question of law enforcement but also requires cooperation from private companies, schools, parents, and civil society. Providing training to law enforcement in the most updated investigative techniques as well as public-private partnerships will strengthen the power of the law and enhance their ability to uncover and prevent crimes of this nature. In a way, parents and guardians too, should be very proactive and educate them rightly about online safety while maintaining proper balance with their privacy. Strict punishment of the offenders along with better reporting mechanisms, such as national helplines, would act as deterrents. Therefore, in the scenario of this increasingly global electronic world, child protection in India should be equivalent to international norms and best practices. Drafting an independent statute that comprehensively addresses the issue of online child exploitation would be the most forward step in the protection of children in these times of digital revolution. By making people aware, strengthening actions, and developing with the times, new technological trends, India can make her cyberspace even safer for its youngest, most vulnerable citizens.

REFERENCES:

1. Research Note on Online Child Pornography Law in India Rahul¹² :
2. Child Protection in India: Issues and Policies Nidhi Marothiya, Shraddha Kapoor and Vinita Bhargava PhD Scholar, Department of Human Development and Childhood Studies, Lady Irwin College, Delhi University, India.¹³
3. Challenges in Child Rights and Child Protection in India Dr. Dakshina Saraswathy, Associate Professor, Kerala Law Academy, Thiruvananthapuram¹⁴
4. CHILD PROTECTION IN INDIA , NICOLE RANGEL MENEZES¹⁵
5. Children's online activities, risks and safety A literature review by the UKCCIS Evidence Group

Professor Sonia Livingstone ▪ LSE Professor Julia Davidson ▪ Middlesex University Dr Joanne Bryce
▪ University of Central Lancashire With Saqba Batool, Ciaran Haughton and Anulekha Nandi
October 2017.

6. Child Online Safety: A Select Study in Indian Context, Thesis submitted in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY by DITTIN ANDREWS