INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

DIGITAL CHILDHOOD AND LEGAL PROTECTION: EVALUATING INDIA'S RESPONSE TO ONLINE CHILD ABUSE

AUTHORED BY - DR. POOJA SOOD & SHWETA SHARMA

ABSTRACT

In today's time we can see that the increased use of digital technologies has changed the way children are communicating, socializing and learning in this world. When in the past where children used to rely more on outdoor activities and books, today they are dependent more on digital media whether for entertainment, interaction or educational purposes. These digital technologies have not only provided them with increased number of opportunities but have also posed many risks such as cyber bullying, grooming, trafficking, digital addiction, cyber extremism, online sexual exploitation, hacking, sextortion, gaming addiction, infringement of privacy and exposure to harmful content etc. not only in India but in the entire world. This article is going to explore the current legal framework of India in dealing with this emerging problem and will also analyze the changes that can be brought in handling this issue more efficiently and effectively. This article will also determine as to how appropriately our agencies for the law enforcement and judiciary is responding towards online abuse of children and will compare India's current standing with best international practices and will also propose certain reforms and suggestions for strengthening the protection of children in the digital world.

Keywords: Child rights, cyber space, India, cybercrime, digital technology, children, child abuse

INTRODUCTION

The outlook of children has been transformed tremendously with the emergence of information -technology. With increased use of smartphones, online learning platforms, social media and uncontrolled internet access children are being born in an age where all these digital interactions have now become a part of daily life. This current digital environment has not only provided children with enormous opportunities for communication, learning, and showcasing their creativity but has also posed a risk for different cyber threats such as cyber bullying,

 ISSN: 2582-6433

grooming, trafficking, exposure to sexually explicit content, online sexual abuse etc. All these threats have increased manifolds in the recent times and India having one of the globe's biggest population of children needs to think more efficiently to confront these threats effectively.

In the current times abuse of children online has come across as a major concern across the world leaving India as no exception. Today children are spending more and more time on online platforms without any adult supervision and safeguards. Not only this, digital technology has also become more accessible among children since the coronavirus hit the globe in the year 2020 as due to lockdowns children had to shift to online platforms and digital interactions for conversing, exchanging information and academic learning. Whether we talk about laptops, smartphones, tablets or computers, all these technological devices are being used among children for communication, entertainment and educational purposes leading to online abuse and addiction among children due to lack of digital literacy. Children born in this digital age are not automatically possessed with digital skills nor can we say that their behavior will not be negatively affected due to such digital media but such dependence on digital media is posing a threat to the children of our country due to the drawbacks that emerge while using these technologies[1]. Increased instances of materials pertaining to sexual abuse of children being originated and watched over India is also rising which is upraising an alarm for the parents, law enforcement agencies, school authorities and the policy makers of this country.

Online child abuse is not very simple but a complex and multi-dimensional problem. There are many cyber crimes that are committed against children which are multinational, masked and enabled by the namelessness of the cyber space. Offenders make use of the gaps existing in the technology, inadequacies in the parental supervision or lack of awareness and lacunas in the enforcement of law targeting children. Contrary to the conventional forms of abuse, online exploitation can occur without any physical touch which eventually makes the discovery of the offence more tough and making its mental effects more deceitful and long lasting.

The Indian law-making bodies have taken serious cognizance of these offences occurring in the online environment by taking important lawful policy changes in response to these threats. The Protection of Children from Sexual Offences (POCSO) Act, 2012 has been amended in

[1] Valentina Presta et. al., "The impact of digital devices on Children's Health: A Systematic Literature Review" 9(4) Journal of Functional Morphology and Kinesiology 236 (2024).

 ISSN: 2582-6433

the year 2019 to address the issue of CSEAM (Child Sexual Exploitation and Abuse Material)[2] more clearly and even the IT, Act 2000 along with the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have introduced provisions for disclosing, reporting and removing of the harmful online content against children. India is also taking initiatives for protection of children online and organizing digital literacy programs which is showing India's growing concern over this burning issue. In spite of taking such measures India's response towards this situation still has some major gaps impacting the efficacy, application and attainability of the statutes safeguarding the children in the digital world. First of all, India's approach is often curative rather than preventive in nature. The law enforcement agencies which are there at the base level are not well equipped with the dealing of cyber crime matters especially involving children due to absence of proper training, resources and knowledge of the technical devices. Furthermore, when we are addressing the privileges of children such as their privacy rights, opportunity of being heard and the privilege of being protected from harm, is frequently being disregarded by the policy makers. Unlike nations such as the USA and UK which owns comprehensive child specific data protection laws, India lacks an extensive digital safety framework and child specific data protection laws for safeguarding the minors from online abuse.

Other than this there is also an absence of transparency regarding the responsibility of the social media platforms, lack of legal recognition to crimes such as cyber grooming and sextortion, and the lack of parental control due to which all these things are contributing to the systematic shortcomings in the protection of children online. In India there is also a social stigma, where talking about sex, sexuality and abuse are often met with silence. Victims of such abuse often show hesitance to report such incidents because of fear of humiliation and absence of faith in authorities due to which the victims are put up with loneliness. In addition to this there is also a digital divide in India between the urban and rural population which further worsens this problem because children in rural India are progressively using digital tools but the understanding of the risks involved online and the protection system remains deficient.

So, the role of education and digital literacy must not be overshadowed for safeguarding the minors from cyber abuse and even the empowerment of minors to report online abuse plus the

[2] Viewing, Storing Child Sexual Exploitation and Abuse Material (CSEAM) an offence: Supreme Court available at: https://visionias.in/current-affairs/news-today/2024-09-24/social-issues/viewing-storing-child-sexual-exploitation-and-abuse-material-cseam-an-offence-supreme-court (last visited on June 8, 2025).

 ISSN: 2582-6433

training of parents, teachers and guardians to identify the indications of exploitation is the need of the hour. All child right activists, tech companies and organizations should come up together to upgrade and promote ethical digital environment where rights of children are protected by law and design.

DIGITAL RISKS IN INDIA: UNDERSTANDING THE CYBER THREATS ON CHILDREN

Since the digital world has expanded so much in India that the children are on a continuous risk of facing threats emerging out of using digital technology. Since the technology has also advanced there are new cyber threats that have come up in the digital environment. There are many factors which are responsible for the increase of cyber-crimes such as absence of parental supervision, lack of digital literacy or insufficient enforcement. All these factors are making children in India, a vulnerable section online. The different threats that are being faced by children in India are cyber bullying, online sexual exploitation and abuse, exposure to inappropriate content, online gaming risks and addiction, phishing and identity theft, privacy violations and data misuse, misinformation and radicalization and many more.

If we talk about different cyber threats in detail then firstly, cyber bullying is an act where online innovations such as social media, gaming platforms, mobile devices, messaging platforms or emails are used for intentionally and continuously harassing, demeaning, intimidating or targeting a person[3]. Contrary to traditional bullying, cyber bullying can be done endlessly which can reach a person at any time making it more psychologically damaging and intrusive. India holds the largest count of cyberbullying cases in the entire world with over 85% children reporting it[4]. Indian children have reported almost double the cases of cyberbullying as compared to the children in the whole world[5]. In India mostly spreading rumors which is 39%, being kept out of chat groups which is 35% and calling out names which is 34% are the most commonly types of cyber bullying being reported by children in India[6].

Secondly, there are risks with online gaming which is leading children towards many harmful effects such as addiction, impact on their physical and mental well-being, their socializing skills

[3] Rufa Mitsu & Eman Dawood "Cyber Bullying: An overview" 4(1) Indonesian Journal of Global Health Research 195 (2022).
[4] Editorial, "Cyber bullying: A growing concern for parents and educators" The Times of India, May 21, 2023.
[5] Ibid.
[6] Ibid.

 ISSN: 2582-6433

and educational attainment. Not only this addiction towards gaming has also been recognized as a mental health condition by the World Health Organization called as the Internet Gaming Disorder (IGD). As per the report that has been declared by the Community Medicine and Public Health Journal of India in 2020, around 3.5% youngsters are suffering from Internet Gaming Disorder and this percentage in 0.5% higher than the global rate[7]. Indian studies have shown that 8% boys and 3% girls are addicted to gaming and are suffering from IGD[8].

Thirdly, there is also a problem of exposure of inappropriate content online to children. Children are being susceptible to online harmful content which includes pornographic content, brutal violence, inciting hatred and content which is advocating self-inflicted harm and detrimental behavior[9]. Not only this but content which is there on the websites and social media is also spreading misinformation and misleading children which can certainly cause ambiguity, terror and twisted views of themselves or the others around the world. This is also rising more because children are spending more and more time on social media, OTT platforms and gaming platforms online.

Fourthly, the problem of virtual sexual misconduct and abuse of minors is moreover on a rise because of rising internet invasion. This includes a lot of offences such as child grooming, sextortion and holding, disbursing and providing child sexual abuse material. The rate to these crimes has increased drastically in the recent times which has led to the need of legislative and social actions. According to the report of the Childline NGO there has been a 40-50% rise in the cases of virtual sexual abuse and exploitation of minors between the year 2020 and 2022[10]. Fifthly, there are rising cases of privacy violations and data misuse of children due to rapid digital transformation of teaching and social communications. There was a survey conducted in the year 2022 by the Association of India for Internet and Mobile (IAMAI) which showed that 67% children in India who are between the age group of 9 and 17 are found to be accessing the internet on a daily basis which are making them more exposed to data misuse and tracking[11].

[7] Experts warn of dangers of online gaming, India available at: https://www.deccanherald.com/india/experts-warn-of-dangers-of-addiction-to-online-gaming-1117242.html (last visited on June 25, 2025).
[8] Ibid.
[9] Sonia Livingstone & Peter K. Smith, 'Annual Research Review: Harms Experienced by Child Users of online and Mobile Technologies', 55(6) Journal of Child Psychology and Psychiatry 635-654 (2014), available at: https://doi.org/10.1111/cpp.12193 (last visited June 25,2025).
[10] Childline India, Annual Report 2022-2023, available at: https://www.childlineindia.org (last visited on June 25, 2025).
[11] Internet and Mobile Association of India (IAMAI), Internet in India Report 2022, available at: https://www.iamai.in (last visited on June 25, 2025).

 ISSN: 2582-6433

Not only this there was another study conducted in 2021 by the National Commission for Protection of Child Rights (NCPCR) which showcased that around 25-30% of mobile applications being used by children in India have gathered sensitive data beyond their said purpose and have shared it with third parties for interest based and audience-based advertising[12].

Then lastly there have also been increasing cases of phishing and identity theft of children in India as phishing attacks are usually happening when children are tricked into sharing their personal information through misleading messages, emails or websites or through gaming platforms, social media or mobile applications. In 2023, according to a record of the National Crime Records Bureau (NCRB) there were 65,000 cases of cybercrime registered in which a major portion includes phishing and online fraud, including cases that have attacked children[13]. Another survey which was organized in the year by the Internet and Mobile Association of India have revealed that 14-16% children who are using the net have been victims of phishing attacks and online frauds as many share their personal information unintentionally[14].

LEGAL SAFEGUARDS AND POLICY FRAMEWORK FOR SHIELDING CHILDREN AGAINST ONLINE ABUSE

Due to the growing dependence on digital platforms children have exposed themselves to various cyber risks which have been mentioned above. So, in response the Government of India has enforced a multi-faceted lawful and regulatory system for securing the children online which includes statutory laws and different policy actions for ensuring a safe digital environment for children.

The main law which talks about controlling of cyber-crime targeting children is the Information Technology Act, 2000. It enlists various sections dealing with safeguarding children online such as:

- **Section 66C** which talks about identity theft. It prescribes the punishment for a person who dishonestly or fraudulently uses someone else's identification features or their

[12] National Commission for Protection of Child Rights (NCPCR), Annual Report 2021, *available at*: https://ncpcr.gov.in (last visited on June 25, 2025).
[13] National Crime Records Bureau (NCRB), Crime in India 2022, Ministry of Home Affairs, Government of India, *available at:* https://ncrb.gov.in (last visited on June 25, 2025).
[14] Internet and Mobile Association of India (IAMAI), Internet in India Report 2022, *available at*: https://iamai.in (last visited on June 25, 2025)

 ISSN: 2582-6433

passwords with up to three years of imprisonment and a penalty of up to one lakh rupees[15].

- **Section 66E** talks about the punishment for privacy violation for whoever shares and captures the images of a person's private parts and not having his or her consent is liable for three years of imprisonment or a penalty of not more than two lakh rupees or both[16].
- **Section 67B** provides for the punishment for sharing and creating material which show minors being involved in obscene acts in digital form for which there is up to five years of imprisonment and a penalty which can go up to ten lakh rupees[17].

This Act was further altered in the year 2008 for incorporating the provisions referring to child pornography along with sexual exploitation through online platforms which strengthened this law more on online child protection.

Then another important statute is the Protection of Children from Sexual Offences (POCSO) Act 2012 which extensively deals in child exploitation along with sexual abuse by also including offences happening in the online world. Sections such as 13 which provides for that any person who uses children for sexual content or satisfaction through any form of media is guilty of that offence[18] and section 14 prescribes the punishment for the offence mentioned in section 13 which is imprisonment for a period of not less than 5 years and will also be liable for fine[19].

One more important statue is the Juvenile Justice (Care and Protection of Children) Act, 2015 which has been crucial in keeping the kids safe online. This Act has provided for procedures which are child friendly and has mechanisms for supporting the children who have experienced virtual mistreatment and exploitation by supporting their rehabilitation[20].

Since the online threats have evolved so much since their inception so the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have introduced strict responsibility of the digital platforms. According to these regulations, the intermediaries must remove or prevent access to CSAM within 24 hours of receiving a court

[15] The Information Technology Act, 2000 (Act 21 of 2000), s. 66C.
[16] The Information Technology Act, 2000 (Act 21 of 2000), s. 66E.
[17] The Information Technology Act, 2000 (Act 21 of 2000), s. 67B.
[18] The Protection of Children from Sexual Offences, 2012 (Act 32 of 2012), s. 13.
[19] The Protection of Children from Sexual Offences, 2012 (Act 32 of 2012), s. 14.
[20] The Juvenile Justice (Care and Protection of Children) Act, 2015 (Act 2 of 2016), s. 39.

 ISSN: 2582-6433

or official directive. Under these rules there is also appointment of grievance officer who ensure the accountability in dealing with complaints which are related to online child safety.

More recent is the Digital Personal Data Protection (DPDP) Act, 2023 which provided for a layer of protection for children's privacy. This Act imposed certain responsibility for the data fiduciaries while they are handling the minor's personal information. It includes provisions which require parental consent before processing child's data[21] and also restricting advertising which is targeting and profiling children[22] which would contribute to the development of a secure online environment.

All these legislative efforts have been complimented by some policy measures from the Indian Government such as the National Policy for Children, 2013 which has provided a regulating framework in order to safeguard the children by understanding the importance of protecting children from online exploitation and abuse[23]. Additionally the 'Indian Cyber Crime Coordination Centre (I4C)' was established by the Ministry of Home Affairs as an attached office for dealing with all types of cyber-crimes in a coordinated manner and as part of I4C the National Cyber Crime Reporting Portal has also been established which is being considered as a committed mechanism for the reporting of cyber crimes against children as well which is helping in prompting timely inquiry and legal action[24].

With these legislative and policy measures India has created a framework to safeguard children in the cyber space but they still lack its effective enforcement. There are still certain challenges that India is facing which is hampering the effective implementation and causing hurdles in the judicial process.

CHALLENGES FACED BY INDIA FOR SAFEGUARDING CHILDREN FROM ABUSE AND ONLINE MISTREATMENT

Though India has a strong lawful and policy framework governing the serious cyber crimes which children are exposed to due to the swift expansion of the digital technologies but still

[21] The Digital Personal and Data Protection (DPDP) Act, 2023 (Act 22 of 2023), s. 9.
[22] The Digital Personal and Data Protection (DPDP) Act, 2023 (Act 22 of 2023), s. 10.
[23] National Policy for Children, 2013, Ministry of Women and Child Development, available at: https://www.wcd.nic.in (last visited on June 20, 2025).
[24] Steps to curb cyber-crimes, India, *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112244 (last visited on June 25, 2025).

 ISSN: 2582-6433

India faces certain challenges in safeguarding the children from online abuse and exploitation. The following are the challenges enlisted below:

- Many children and their guardians in India particularly in the rural areas have very limited digital literacy and awareness about the different cyber threats. There is an absence of a proper structured online safety education in their course of study which disables them to figure out and react to situations where cyber abuse and exploitation happens.
- Although there are many legislations which deal with the problem of cyber abuse such as the IT, Act 2000 and the POCSO Act, 2012 but the enforcement of these laws remains a bit incompatible because of resource limitations, hindrance in the investigation process and very limited digital skills within the law enforcement agencies. Even the police are not well equipped to deal with complex cases of cyber-crimes which are involving children.
- There is lack of exclusive cyber units which are primarily just focusing on the crimes against children due to which there are unnecessary delays in addressing such incidents and also in providing support to such victims. Very child friendly practices are to be implemented so that it creates less trauma on the child victims.
- There is not proper coordination between the law enforcement agencies, NGO's, child protection authorities and the digital platforms which eventually leads to disintegrated responses. There is also deficiency in the regulated protocol to be followed for collecting evidence or sharing of information which causes delays in the investigation of the case and deteriorates the quality of outcome.
- Though laws have come up for regulating the social media like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, but still the execution and adherence by the social media platforms remains inconsistent. Gaming platforms and social media have evolved so much that they are becoming the hubs for grooming and exploitation of children which clearly shows the legislative and enforcement gaps.
- The child protection authorities and the enforcement agencies often lack the required technical infrastructure and skilled personnel for dealing with investigation of cyber-crimes. Very limited funds and resources are allocated which effect the efforts both at the national and state level.

 ISSN: 2582-6433

- The pace at which the online platforms are progressing and new technologies are being adopted such as artificial intelligence or end to end encryption, these things are complicating the enforcement procedures as the offenders are using complicated tools due to which their chances of getting caught gets reduced.
- The delays on part of the judiciary in dealing with cyber crime cases is also obstructing access to justice to these victims and there is also lack of psychological assistance and rehabilitation services to the child victims which eventually leads to difficulty in their recovery and the reconciliation of the society.
- The online platforms offer anonymity which helps the offenders to work across state, national and international borders. Not only this there is also lack of international cooperation in dealing with such cases which brings delay in the inquiry and prosecution of cyber- crime cases against children.
- Since a proper balance has to be achieved between privacy and protection of children, this complicates the policy making process which is for safeguarding the children online. All the recent cyber protection laws that are being passed have to be aligned both with data privacy rights and child protection initiatives.

INDIA'S COMMITMENT WITH INTERNATIONAL STANDARDS FOR SAFEGUARDING CHILDREN FROM CYBER ABUSE

India has taken up various international obligations that has shaped its legal and policy regulations for the security of minors from cyber abuse and exploitation. These commitments are resulting from the binding conventions and treaties which together explains the international standards which India seeks to coordinate with.

The first such convention was the United Nations Convention on the Rights of the Child (UNCRC), 1989 which India formally consented to in the year 1992 for having a detailed framework for child rights. Some of its provisions talk about safeguarding children against all types of exploitation and abuse[25], while some deal with the responsibility of the states to protect the children from such abuse and exploitation[26]. The General Comment No. 25 which was made in the year 2021 by the committee had interpreted these articles in such a way that it was the obligation of the state to shield children from virtual sexual assault and abuse, to ensure

[25] The United Nations Convention on the Rights of the Child (UNCRC), 1989, art. 19.
[26] The United Nations Convention on the Rights of the Child (UNCRC), 1989, art. 34.

 ISSN: 2582-6433

that the designs of digital services are age appropriate and to promote digital literacy of children[27]. India's ratification to this treaty showed its wanting to integrate such interpretation in its domestic laws so that the problem of online child abuse can be addressed.

Then India also recognized the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC), 2000 in the year 2005 which had straightway addressed different types of online sexual exploitation of children which usually happen with them. Giving recognition to this protocol this mandated that India needs to have a strong legislation and effective cross border cooperation[28] so that such crimes against children can be dealt with in the cyber space.

Then India is also the member of the International Telecommunication Union (ITU) Guidelines on Child Online Protection (CGP) which is not a binding treaty but it has developed Global Child Online Protection Guidelines[29]. These have prompted the states to adopt such strategies which have laws criminalizing online child abuse, to have such technological measures for finding and blocking CSAM and also to initiate awareness campaigns to educate the children, parents and teachers.

India is also pledged to the 2030 Agenda for Sustainable Development including the SDG target 16.2 which calls for the cessation of all forms of violence against children including trafficking, exploitation and abuse[30]. In this online sexual abuse against children is also considered as one of the exploitative practices for which India needs to adopt national plans for addressing these issues.

India is also a member at the regional level of the SAARC Convention on Regional Arrangements for the Promotion of Child Welfare in South Asia (2002) which has later on stated that there is a need to expand the cooperation to cyber related exploitation for protecting the children from online sexual abuse as this convention was adopted before the evolution of social media. So, India has also taken part in various discussions on cyber crime and child

[27] UN Committee on the Rights of the Child, General Comment No. 25 on Children's Rights in Relation to Digital Environment, 2021.
[28] The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC), 2000, arts. 4-10.
[29] ITU-Child Online Protection Guidelines, *available at*: https://www.itu.int (Last visited on June 18, 2025).
[30] United Nations- Sustainable Development Goals, Target 16.2, available at: https://sdgs.un.org/goals (Last visited on June 25, 2025).

 ISSN: 2582-6433

protection and has showed its willingness to adapt to the change's happenings in the digital age.

Then India is also an active member of the INTERPOL which provides for the initiative of crime Against Children and international CSAM databases[31]. With this framework India shares and also have access to the intelligence on the networks for online child exploitation and abuse. Not only this India also enables global investigation and the trial of such offenders.

Then lastly India is a non-member of the Budapest Convention and Cooperation on Cyber Crimes but it has taken part in the related deliberations and has regulated its domestic laws by criminalizing online sexual abuse and grooming against children in consonance with the provisions of the Budapest Convention.

JUDICIAL RESPONSE IN COMBATTING CHILD EXPLOITATION AND ONLINE ABUSE

Our Indian judiciary is playing a very important role in explaining, clarifying and enforcing the laws for safeguarding the kids from online exploitation and abuse as the technology has evolved so much that the digital threats against children are on a rise. Our courts have time and again emphasized the requirement for a strong procedure, victim centric techniques and the liability of the digital intermediaries. The judgements have served to interpret the already existing laws in such a way so that the dignity, safety, privacy and welfare of children is protected at all costs.

Some landmark judgments dealing with such cases are the case of Avnish Bajaj v. State of (NCT of Delhi)[32] in which ebay India's Managing Director was held responsible in accordance with section 67 of the IT Act 2000 for showing a pornographic MMS which involved a child. Though the court laid importance on mens rea in determining the liability of such intermediaries but the pronouncement stressed on the growing threat of child pornography and the requirement for proper verification and analysis by the digital platforms.

Then one major development happened in the case of Re: Prajwala Letters Case[33] in the year

[31] INTERPOL- Crimes Against Children, available at: https://www.interpol.int/en/Crimes/Crimes-against-children (Last visited at 24 June, 2025)
[32] *Avnish Bajaj v. State (NCT of Delhi),* 116 (2005) DLT 427.
[33] *Re: Prajwala Letter Dated 18.2.2015 Videos of Sexual Violence and Recommendations,* W.P. (Crl.) No. 3/2015, Supreme Court of India.

 ISSN: 2582-6433

2015 wherein a social activist sent a letter to India's Chief Justice on how there is unchecked increase in the circulation of videos relating to child abuse and rape on the social media platforms. This communication by way of a letter was treated as a petition for a writ and the apex court gave a series of directions to the Ministry of Home Affairs and the digital platforms such as Google, Facebook and Microsoft to evolve such tools and rules which helps in identifying, blocking and removing the material involving sexual abuse of children. This case strengthened the need of technological safeguards and the liability of internet network service providers.

Then another case of 2017 wherein the Supreme Court took suo moto cognizance and gave directions for strict monitoring of child care institutions and highlighted the mechanism of digital surveillance registration so that the trafficking and online abuse of the children living in these institutions could be controlled[34]. The court emphasized on the responsibility of the states to make sure that the children are not only protected in the offline world but also against the upcoming cyber threats and dangers.

Then in X v. State (2020)[35], the Delhi High Court was dealing with a case of online sexual grooming in which the court held that the digital harassment and luring of children online leads to serious breach of privacy and bodily freedom of children. In this the court took a victim centered approach and advised the psychological counselling of such minor victims and recommended the need of timely investigation of cyber crimes against children.

Then in the year 2024 the Apex Court gave a landmark verdict in which it held that even if a person just sees, have with him or stores material which shows minors in sexual acts will lead to the committing a crime under the POCSO Act, 2012[36]. The role of social media intermediaries was also established by the Court to communicate the publication and circulation of sexually explicit material involving children to the law enforcement officials and gave suggestion to the Parliament to replace the word "child pornography" with "CSAM (Child Sexual Exploitative and Abuse Material)".

[34] *Re: Exploitation of Children in Orphanages in the State of Tamil Nadu* (2017) 7 SCC 578.
[35] *X v. State (NCT Of Delhi),* 2020 SCC Online Del 1426.
[36] *Just Rights for Children Alliance v. S Harish* 2024 INSC 716.

 ISSN: 2582-6433

RECOMMENDATIONS FOR REFORMING THE ONLINE CHILD PROTECTION BASED ON COMPARATIVE ANALYSIS

Safeguarding the interests of minors in the virtual environment is the biggest concern globally. This digital technology has exposed children to a lot of risks and countries are dealing with, this situation through different strategies and legal framework. Though India has taken positive steps through various legislations but there are still many gaps that are existing either in enforcement, cross border cooperation and children friendly online designs. So, a comparative analysis is done with different countries such as UK, USA and Australia so that some things can be learnt from these countries to improve and strengthen our legal response in dealing with these situations.

In UK there is a dynamic approach that has been adopted for online child protection through its Online Safety Act, 2023[37] which puts a legal "duty of care" on the digital marketplace for the protection of its users especially minors from harmful material which includes grooming, sexual content involving minors and cyberbullying. This law also ensures that proper risk assessment is done, content moderation safeguards are followed and proper safety-by-design features are there on the online services which are used by the children. Also. there is provision for the Office of Communications who is empowered to look into and punish the platforms which are non-compliant. Whereas India on the other hand does not impose any binding duty of care on the intermediaries. The IT Rules, 2021 puts obligations for the taking down of content put on the platforms but lacks a proper child specific structure. If India adopts the UK style model, then India can shift to a preventive and platform liable model rather than having takedowns from such platforms mostly in dangerous surroundings such as the messaging and live streaming apps.

The United States has a dynamic model known as the National Center for Missing and Exploited Children (NCMEC) and the CyberTipline[38]. The federal law under title 18 U.S.C 2258A makes it necessary for all the internet service providers to disclose all the alleged CSAM and virtual inducement cases to the NCMEC which acts as unified clearing house for the national and international coordination, including with agencies from India through

[37] Online Safety Act 2023, UK, c. 46 *available at*: https://www.legislation.gov.uk/ukpga/2023/46/enacted (Last visited on June 20, 2025).
[38] National Centre for Missing & Exploited Children, USA, *available at*: https://www.missingkids.org (Last visited on June 20,2025).

 ISSN: 2582-6433

INTERPOL. Whereas India's implementation networks are disintegrated. Although the Ministry of Home Affairs has setup a Cyber Crime Reporting Portal[39], but there is no chief coordination body equal to that of the NCMEC. So, India should have a proper national unit which is legally recognized so that there can be proper reporting, inquiry, child support and international coordination so that there can be quick, harmonized, and child-centric responses. In Australia there is Online Safety Act, 2021 and Children Data Code under the privacy Act which provides for age-appropriate protection. Under this there is appointment of an independent eSafety Commissioner who can order the removal of any harmful material which involves minors and under these Acts the companies must showcase compliance with the intended standards of design which reduce data collection and behavioral baiting. On the other hand, India's Digital Personal and Data Protection Act of 2023 requires parental consent for moving ahead with the children's data but it does not have enough safeguards against profiling, compelling design or behavioral marketing. So, if the Australian model is adopted then there will child centric design code which would make sure that digital platforms adopt their interfaces and practices which would eventually give more importance to children's safety and privacy.

In UK and USA there are special prosecutors and judges which handle the cases of online child exploitation as they have devoted training in digital forensics and victim-sensitive plan of action. Such as the US Internet Crimes Against Children Task Forces work jointly with prosecutors and courts to speed up such cases. But in India though POCSO Courts are established but they are short of expertise in cyber law, electronic evidence and the upcoming cyber-crime threats. So, India should give preference to specialized training to the judges and prosecutors on digital enabled sexual offences on children and should consider having special dedicated cyber POCSO benches in big cities so that the merit and speed in adjudication of such cases in ensured.

India is a member of various multinational instruments like the UN Convention on the Rights of the Child and Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography. But it has not signed the Budapest Convention on Cybercrime which enables transnational sharing of evidence and unified criminalization of online offences. Considering the built-in international nature of the online sexual abuse of children, India should also

[39] Ministry of Home Affairs, Government of India, Cyber Crime Reporting Portal, *available at:* https://cybercrime.gov.in (Last visited on June 20, 2025)

 ISSN: 2582-6433

consider becoming a signatory to such framework and also to develop bilateral and multilateral treaties to make sure that there is proper cross border investigation and trial. India also needs to conform its domestic laws with the global legal regime which would eventually strengthen the collaboration with major tech companies having their headquarters outside India.

CONCLUSION

Safeguarding the children from virtual abuse and ill-treatment is an immediate and progressing concern of the world. While India has made major advancement in its legal regime still its current statutory framework requires strengthening so that it can meet with the intricacies of the emerging online threats against children. In India a child centric, technically informed along with globally aligned policy and legal structure is required so that the children can be protected from such virtual abuse and exploitation.