

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIAL TEAM

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

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 IMoot 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.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS
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.

VIRTUAL VULNERABILITIES: THE RISE OF CYBER EXPLOITATION AGAINST CHILDREN POST- PANDEMIC

AUTHORED BY - ARUNDHUTI DESHMUKH
& SPARSH MANOCHA

ABSTRACT

The COVID-19 pandemic brought significant changes in the cyber world. There was a sudden transition from traditional offline workspaces to online platforms, which included schools, colleges, court proceedings, and other activities being conducted virtually. Additionally, there was a notable increase in the number of children gaining access to smartphones and laptops, leading to a rapid rise in the exploitation of minors in the cyber realm. In India, there have been long-standing concerns regarding the impact of technological advancements on the sexual exploitation of children, this has resulted in legislative changes in India specifically addressing abusive images of children (child pornography) and acts accompanying such violent content. This paper explores the various aspects of cyber exploitation against minors, particularly in the context of increased access to technology during the pandemic. It examines the rise in incidents of child pornography and online abuse, analyzing how these trends have evolved in the wake of COVID-19.

Furthermore, this paper argues that existing legal frameworks in India, notably the Information Technology Act, 2000, and the Protection of Children from Sexual Offenses Act, 2012, while crucial, require further refinement to effectively address the escalating nature of online offenses against minors. The authors emphasize the need for a comprehensive approach that not only strengthens legislative measures but also promotes awareness and preventive strategies. By identifying gaps in current laws and their enforcement, this research provides insights and future directions to mitigate the cyber exploitation of children in India.

KEYWORDS

Cyber Crime, Cyber Grooming, Cyber Security, Minors, Cyber Exploitation

INTRODUCTION

“Digital can’t be divorced from cyber security. Digital world without security is like a pyramid without foundation which can collapse like a house of cards”¹ - Pavan Duggal

It is an undeniable reality that the digital realm resembles a vast pyramid, with cybersecurity serving as its foundational cornerstone. In its absence, any form of cyber threat functions as an earthquake capable of precipitating the collapse of the entire structure within mere seconds. We are currently in an era dominated by technology where the digital world has become an integral part of our daily lives, offering opportunities for communication, education, mobile transactions, and entertainment amongst many other things. As the boundaries between the physical and virtual realms diminish, a new obstacle emerges, namely the cyber exploitation of children. According to the 1989 United Nations Convention on the Rights of the Child, a child is defined as an individual who has not attained the age of 18 years². In a more generalized sense, the meaning of a child is a young person between infancy and puberty. Cybercrime encompasses acts perpetrated through electronic means that target individuals or groups with the intent to damage their reputation or inflict physical or mental trauma. Children as compared to any other age group are more vulnerable to cyber-attacks due to their expanding digital presence. The rapid increase of internet-connected devices, coupled with younger individuals (below 18 years of age) accessing online platforms, creates an environment where minors may lack the experience and awareness to navigate potential threats. Inadequate parental controls, limited digital literacy, and a growing trend of online learning further expose children to risks such as cyberbullying, inappropriate content, pornography, cyber grooming, etc. Cybercriminals exploit these vulnerabilities, targeting children for identity theft, fraud, or harassment. As technology evolves, fostering digital knowledge through education and online safety measures becomes imperative to safeguard the well-being of the younger generations.

According to NCRB data, in 2022, child cybercrime surged, 32% compared to the previous year (2021). The NCRB data, reveals a total of 1823 cases of cybercrimes against children in 2022, up from 1376 the previous year³. These crimes mainly included cases of cyber pornography, cyberstalking, and bullying. These crimes result in harming a child’s mental and

¹ Sakshi Chand, *Delhi cops to get ‘one touch’ internet monitoring system*, DNA (20 Oct 2024, 5:30 PM), <https://www.dnaindia.com/delhi/reports-delhi-cops-to-get-one-touch-internet-monitoring-system-2278908>.

² Convention on the Rights of the Child, <https://www.unicef.org/child-rights-convention>, (last visited oct 26, 2024).

³ Mohua Das, *Child cybercrime surges 32% reveals NCRB data, Underlining vulnerability to online risks*, Times of India (Oct. 19 2024, 7:00 PM), <https://timesofindia.indiatimes.com/india/child-cyber-crimes-surges-32-reveals-ncrb-data-underlying-culnerabilty-to-online-risk/articleshow/107168056.cms>.

emotional health and the child may exhibit a range of personality traits that include social withdrawal, limited social connections, pessimistic attitudes, and a lack of awareness. They may experience challenges in gaining acceptance in social settings, educational institutions, and professional environments. Additionally, these children may encounter difficulties in forming meaningful relationships, face privacy concerns, and witness a decline in life and achievement expectations.

CRIME AGAINST CHILDREN IN CYBER WORLD

Online child sexual abuse and online child sexual exploitation involve the use of information and communication technology as a means to sexually abuse and/or sexually exploit children. Perpetrators of this crime commit abuse or attempt to abuse "a position of vulnerability, differential power, or trust for sexual purposes" for monetary or other benefit (e.g., sexual gratification). The most prevalent forms of cybercrime against children are given as follows:

- 1. Cyber Grooming:** Child grooming, also known as the enticement or solicitation of children for sexual purposes, involves an adult establishing a deceptive relationship with a child, both online and offline, with the ultimate intention of sexual exploitation⁴. Predominantly perpetrated by males, the process unfolds through stages, including victim selection based on attractiveness, ease of access, and vulnerabilities. Perpetrators manipulate online platforms to befriend children, making a show of common interests and building trust. The grooming process is dynamic and driven by the offender's motivation, capabilities, and control over the victim. The ultimate goal is sexual exploitation, either online (e.g., coercing explicit content) or offline (e.g., in-person abuse). The consequences of grooming affect various aspects of a child's life, leading to anxiety, depression, self-harm, and more. As online grooming poses a significant threat to children in today's digital age, understanding the existing legal framework on this issue is crucial for ensuring the safety and well-being of children. While international instruments like the Lanzarote Convention explicitly criminalize child grooming, In India we do not have specific legislations that criminalize cyber grooming.
- 2. Child Pornography:** Child pornography means any representation, through various means, depicting a child engaged in explicit sexual activities or showcasing

⁴ Ministry of Home Affairs https://www.mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf (last visited Oct 26, 2024).

the sexual parts of a child, with a predominant purpose of sexual gratification⁵. In recent years child pornography has rapidly increased due to the widespread availability of internet access and online content. This heinous crime has led to other consequences, such as sex tourism and the sexual abuse of children. Child pornography may include actual or simulated sexual intercourse involving minors and is considered to be the evidence of child abuse. The internet has exacerbated the issue of child pornography, The online environment facilitates anonymous and private access to such content, fostering direct communication and image sharing among users. The internet's cost-effectiveness, high digital quality, and diverse formats, including pictures, videos, and sound, contribute to the proliferation of this illicit material. Additionally, the potential for real-time and interactive experiences, coupled with the modification of digital images, such as morphing, further compounds the severity of the issue.

3. **Cyber Bullying:** Cyberbullying is emerging as a prominent cyber threat in the recent times, it basically means the use of offensive or abusive language to harass fellow children. This harmful conduct extends to the transmission of damaging content, posing a significant risk to a child's self-esteem. It is crucial to recognize that the repercussions of unaddressed cyberbullying can be profound, exerting detrimental effects on a child's mental and emotional well-being. Unchecked instances of cyberbullying can impede a child's holistic development, emphasizing the urgency of early intervention. Various digital platforms serve as conduits for this form of abuse, including text messages, emails, websites, blogs, polls, social media posts, instant messages, as well as gaming and virtual reality sites. Perpetrators employ these mediums to humiliate, denigrate, harass, spread false information, engage in gossip or rumors, issue threats, and isolate or marginalize their targets.
4. **Cyber Stalking:** Cyberstalking uses the Internet or other electronic means to stalk or harass another by misusing information uploaded on social networking sites⁶. It involves the persistent, unwarranted intrusion into a child's online space with the intent to instill fear, intimidation, or harassment. Cyberstalkers exploit various digital platforms, including social media, messaging apps, and online gaming, to

⁵ International Centre for missing & Exploited Children, Child Pornography: Model Legislation & Global Review, 7 Edition, (Koons Family Institute on int. law and policy 1, 4 (2024), <https://www.icmec.org/wp-content/uploads/2015/10/7th-Edition-EN.pdf>).

⁶ Wikipedia, <https://en.wikipedia.org/wiki/Cyberstalking> (last visited October 26, 2024).

relentlessly monitor, follow, and engage with their targets. This intrusive behavior can extend to the dissemination of personal information, often exacerbating the threat. The consequences of cyberstalking on children are profound, encompassing psychological distress, anxiety, and potential long-term trauma.

5. **Revenge Porn:** Children pose as potential victims to adults as well as to the children of their age group in the case of revenge porn. Revenge porn is a form of online mistreatment where private pictures or videos showing nudity or intimate moments are shared without the permission of the people in them⁷. It's also known as nonconsensual pornography and is connected to sexual abuse. Sometimes, a current or past partner might share these images as a way to get back at someone or threaten to spread them to force the person to do something. In the case of revenge porn, the victim may have sent these private images or videos themselves or A partner may have convinced them to take explicit pictures, or an abusive partner could even take sexual or nude photos without the knowledge of the victim. Mainly teenage girls aged 14-19 years fall victim to this crime, The effects of this crime do not end with posting pictures online the victim is further shamed by society or in some cases ultimately married off to the person who has circulated the photos in the first place or sometimes due to lack of knowledge and feeling of helplessness the victim commits suicide. Even though Image-based sexual abuse or revenge porn is considered sexual harassment under section 75 of The Bharatiya Nyaya Sanhita 2023⁸, due to a sheer lack of knowledge and public shame or embarrassment associated with these crimes, these cases are mostly not even reported let alone filed
6. **E-Transaction Fraud:** While a significant number of children do not possess individual bank accounts, they regularly leverage their parent's accounts for various online transactions, including shopping and gaming. This practice exposes them to potential risks as criminals employ deceptive tactics that capitalize on the desire for free or valuable offerings, and use fraudulent calls offering purported benefits often assuming false identities, creating a heightened risk of falling victim to fraudulent schemes that illegally drain funds from these accounts. A collective effort involving parents, guardians, and financial institutions is essential to fortify the digital defence

⁷ Miha Šepceff, Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence, Vol. 13(2) IJCC 418, 420 (2024), <https://www.cybercrimejournal.com/pdf/MihaSepecVol13Issue2IJCC2019.pdf>.

⁸ Bharatiya Nyaya Sanhita, 2023, § 75, No. 45, Acts of Parliament, 2023 (India).

surrounding family accounts and mitigate the risks associated with deceptive practices by cyber criminals.

LEGISLATIONS CONCERNING ONLINE OFFENCES

AGAINST CHILDREN

The main legislations for combating cybercrime in India are “The Information Technology Act”, of 2000, “The Protection of Children from Sexual Offences Act”, of 2012, and “The Bharatiya Nyaya Sanhita, 2023.

1. Information Technology Act 2000: The main goal of this act was to restrict cybercrime across E-Commerce sites that operate throughout the country. It made India the 12th country in the world to pass laws on e-commerce and cybercrimes⁹. This act in Chapter XI provides penalties for unauthorized data access and computer damage caused by cyber-attacks, including viruses, phishing, botnets, malware, etc. Section 67B of this Act includes a special provision for protecting children on online platforms.

Section 67B: Punishment for publishing or transmitting material depicting children in sexually explicit acts, etc. in electronic form-

Anyone who,

- (a) shares or spreads material online showing children involved in sexually explicit acts,
- (b) creates, collects, advertises, or distributes material depicting children in an obscene or sexually explicit manner,
- (c) lures or encourages children into online relationships for explicit acts, or in a way that may offend a reasonable adult,
- (d) aids in abusing children online, or
- (e) records their own or others' abuse of children in any electronic form, will face penalties. Upon the first conviction, the punishment includes either imprisonment for up to five years and a fine of up to INR 10,00,000. In the case of a second or subsequent conviction, the imprisonment term may extend to seven years, along with a fine of up to INR 10,00,000.

However, the provisions of Section 67, Section 67A, and this Sec do not apply to materials that serve the public good, like those related to science, literature, art, or learning. Similarly,

⁹ Monesh Mehndiratta, Information Technology Act, 2000, IPleaders (August 24 2022), <https://blog.ipleaders.in/information-technology-act-2000/>.

materials kept for genuine heritage or religious purposes are also exempt from these regulations. The law aims to protect children from explicit content and online exploitation while allowing for exceptions that serve legitimate public or cultural interests¹⁰.

Other Important Sections:

Section 66C: This section specifically talks about identity theft cybercrimes and prescribes punishment for cases where someone intentionally and dishonestly uses another person's electronic signature, password, or any unique identification feature, they can be punished with imprisonment for a term which may extend to three years and may also be fined up to one lakh rupees.

Section 66D: This section provides punishment for a person who commits cheating by impersonating another by using computer resource can be punished with imprisonment for up to three years and may also be fined up to INR 1,00,000.

Section 66E: This section explains that if someone intentionally takes, shares, or shows pictures of someone's private body parts without their consent, in a way that invades their privacy, they can be punished with imprisonment for up to three years, or fined up to INR 2,00,000, or both.

2. **Bhartiya Nyaya Sanhita 2023**

Section 303(1) deals specifically with theft and applies only to movable property, excluding intangible and immovable properties. The punishment for theft is outlined in Section 303(2) of the BNS¹¹.

Section 323 of the BNS addresses the act of dishonestly or fraudulently concealing, removing or assisting in the concealment or removal of the property, along with dishonestly releasing any entitled demand or claim. The penalty for this offense may include imprisonment for up to two years, a fine, or both¹².

Moving on to Section 324(1) of the act, covers mischief, stating that intentionally causing

¹⁰ The Information Technology Act, 2000, § 67 and § 67 A, No. 21, Acts of Parliament, 2000 (India).

¹¹ Bharatiya Nyaya Sanhita, 2023, § 303(1), No. 45, Acts of Parliament, 2023 (India).

¹² Bharatiya Nyaya Sanhita, supra note 11. At § 323.

wrongful loss or damage to the public or any person by destroying property or altering it in a way that diminishes its value or utility constitutes mischief¹³. Section 324(2) specifies that the maximum punishment for mischief is imprisonment for up to six months, a fine, or both.

3. Provisions of the Protection of Children from Sexual Offenses Act, 2012. (POCSO, Act)

The POCSO Act, 2012 was enacted on 19 June 2012. This act provides laws relating to the protection of children from the offenses of sexual harassment, pornography, and sexual assault¹⁴. It emphasizes that the best interests and welfare of the child are of utmost importance at all stages.

Section 13: This section makes it a criminal offense for anyone to use a child in any form of media, such as TV shows, internet content, or printed material, for sexual gratification. This includes showing the child's sexual organs, depicting real or simulated sexual acts, or presenting the child in an indecent or obscene manner¹⁵. In simpler terms, it's illegal to involve a child in any sexual content, whether in pictures, videos, or other media.

Section 14: Using a child for pornographic purposes can lead to a minimum of five years in prison and a fine, with a maximum penalty of seven years in prison and additional fines for repeat convictions. If the use of a child for pornographic purposes involves penetrative sexual assault, the minimum imprisonment is ten years. For cases involving a child below 16 years, the minimum imprisonment is not less than 20 years. In such instances, a 20-year prison sentence and a fine are imposed for using a child for pornographic purposes¹⁶.

Section 15:

- (a) If someone has pornographic material involving a child but doesn't delete, destroy, or report it to the designated authority, intending to share or transmit child pornography, they can be fined at least INR 5,000. For a second or subsequent offense, the fine increases to not less than INR 10,000.

¹³ Bharatiya Nyaya Sanhita, supra note 11. At § 324 (1).

¹⁴ Protection of Children from Sexual Offences Act, 2012, Preamble, No.32, Acts of Parliament, 2012 (India).

¹⁵ POCSO, supra note 14. At § 13.

¹⁶ POCSO, supra note 14. At § 14.

- (b) Storing or possessing child pornographic material for transmission, propagation, display, or distribution, except for reporting or for use as court evidence, can lead to imprisonment for up to three years, or a fine, or both.
- (c) Anyone possessing child pornographic material for commercial purposes faces imprisonment for a minimum of three years (up to five years), or a fine, or both, on the first conviction. For a second or subsequent conviction, the imprisonment increases to a minimum of five years (up to seven years), along with a fine¹⁷. In simpler terms, having child pornographic material can result in fines or imprisonment, with more severe consequences for commercial purposes and repeated offenses.

IMPACT OF COVID 19 ON CYBER CRIMES AGAINST MINORS

The COVID-19 pandemic has brought about unprecedented changes in our daily lives, While the virus has affected various aspects of our society, one area that has seen a significant impact is cybercrime against children. The pandemic has created new opportunities for online predators, as children spend more time online due to school closures, social distancing measures, and remote learning. According to an article published by The Economic Times on 14 November 2021, there was a more than 400 percent increase in cyber-crimes cases committed against children reported in 2020 as compared to 2019 with most of them relating to publishing or transmitting of materials depicting children in sexually explicit acts¹⁸. According to the NCRB data, Uttar Pradesh (170), Karnataka (144), Maharashtra (137), Kerala (107), and Odisha (71) are among the top five states related to cybercrimes against children¹⁹. Parents, educators, and policymakers must prioritize cyber safety and digital literacy as a part of the new normal. This includes educating children about online safety, monitoring their online activities, and implementing strict measures against cybercrime. The pandemic has highlighted the urgent need for a collective effort to address the growing threat of cybercrime against children, and we must take proactive measures to ensure the safety and well-being of our children in the digital age.

¹⁷ POCSO, supra note 14. At § 15.

¹⁸ Public Trust of India, over 400% rise in cyber crime cases against children in 2020: NCRB data, Business Standard (Nov. 14 2021, 2:59 PM), https://www.business-standard.com/article/current-affairs/over-400-rise-in-cyber-crime-cases-against-children-in-2020-ncrb-data-121111400320_1.html.

¹⁹ NCRB data, supra note 18.

CASE STUDY: BOIS LOCKER-ROOM

In the case of "Bois Locker-Room," a group chat consisting of teenagers aged 16 to 18 years engaged in discussions regarding sexual assault against minor girls and circulated their pictures without consent. The group's chat, which was exposed through screenshots posted on social media platforms, revealed a series of disturbing conversations. The screenshots depicted the group's members sharing photos of underage women and teenage girls, guessing their ages, and then engaging in lewd discussions about their bodies and objectifying their classmates and other women, some as young as 14 years old. The group also allegedly shared nude or morphed photographs of the women and their personal information. Following the dissemination of screenshots from the "Bois Locker-Room" group chat, several members deactivated their accounts and made threats to leak explicit photos and hack the accounts of the women who exposed the group." In response, an Instagram page named "Bois Locker Room 2.0" was created to continue the crude discussions. The Delhi Commission for Women has taken cognizance of the matter and issued a notice demanding immediate arrests of the members, registration of an FIR against them, and directions for further investigation into the case²⁰. This case exemplifies juvenile delinquency, as the members of the group chat engaged in discussions that promoted sexual assault against minor girls. The participants' sexist mindset, which has normalized rape culture, is evident in the explicit content shared and the threats made against the women who exposed the group. This case highlights the urgent need for greater awareness and education about consent, online safety, and the consequences of engaging in such depraved behaviours.

FUTURE DIRECTIONS IN PREVENTING CYBERCRIMES

AGAINST CHILDREN

1. Integrating Digital Literacy in School: Digital literacy programs that deal with recognizing potential threats, understanding privacy settings, and having responsible online behaviour should be well incorporated in school in a child-friendly way so that children have knowledge about all the potential threats in cyberspace and have a basic understanding of how to deal with it.
2. Collaboration With Tech Companies: Government agencies should take the initiative to collaborate with tech companies to make easy-to-use apps as a one-stop

²⁰ Bismee Taskin, Remember 'Bois Locker Room'? Trial in 2020 case yet to start, forensic report on mobiles awaited, The Print (Oct. 16, 2023, 09:42 am IST), <https://theprint.in/india/remember-bois-locker-room-trial-in-2020-case-yet-to-start-forensic-report-on-mobiles-awaited/1804635/>.

solution for registering or reporting these crimes and for providing proper counselling and support services for child victims and their families. They can also use the online presence of these companies to create awareness about cybercrimes against minors.

3. **Specific Law Addressing Cybercrimes:** The government can make a specific law addressing all the types of cybercrimes against children and include strict penalties for the same. This will help in bringing clarity and consistency among the general public and will result in efficient law enforcement.
4. **Parental Control and Education:** Awareness campaigns and educational programs for parents to guide them in setting up effective parental controls on devices used by their children should be conducted in a large scale in vernacular languages for better understanding among the masses.
5. **Technological Innovation:** The government should invest in research and development of advanced technologies such as artificial intelligence and machine learning to proactively identify and prevent online threats. This can include developing tools to detect grooming behaviours and automatically filter inappropriate content.

CONCLUSION

Currently, we are living in an era which is dominated by technology, everyone is dependent on technology and it has become an integral part of our lives. Efforts to combat the cyber exploitation of minors must be approached through a collaborative and dynamic strategy. This includes bringing specific laws for these crimes, enhancing online platforms' security measures to prevent such incidents, and providing digital literacy and education among parents, guardians, and children. As technology continues to advance, so must our efforts to safeguard the vulnerable population of minors from online threats. A global commitment is required from government agencies, law enforcement agencies, technology companies, educators, and parents to create a safer digital environment for children.