DIGITAL EXPLOITATION OF CHILDREN: ANALYSING ONLINE GROOMING, CYBERBULLYING, AND THE ROLE OF INDIAN LAW

Divyanshi Yadav, Lovely Professional University, Punjab

ABSTRACT

Children are becoming increasingly vulnerable to acts of exploitation in cyberspace, with exploitation manifesting in considerably more nuanced forms of crime than traditional forms of abuse. There are laws like the POCSO and the IT Act in place addressing online pornography and abuse, but there are several areas of untouched digital exploitation worthy of exploration. These include how the dark web facilitates the production, distribution, and consumption of child sexual abuse material (CSAM), AI-enhanced grooming and manipulation, deepfake exploitation relating to minors, psychological tricks and manipulations used by offenders, jurisdictional issues when engaged in enforcement mechanisms across borders, and the ways in which children's statutory protection laws are being misused. This paper examines these unique facets of the exploitation of children and analyses the readiness in India's legal framework, compares with the approaches taken by other jurisdictions, and ultimately makes recommendations for reforms of laws that could be made to expand the rapidly waning gaps between technology and law.

Introduction

Children are the most vulnerable members of society, and the digital age brings new opportunities for growth as well as the potential for new forms of exploitation. Children are gaining access to smartphones, social media, and online learning platforms that allow them entry into virtual spaces where definitions of privacy, safety and trust are changing. In addition, the technology that allows for new forms of education and exercise of creativity also provides unprecedented access to exploitation online including online grooming, cyberbullying, pornography, and sexual exploitation, as well as phenomena like deepfake technology and threats by artificial intelligence.[1]

The protection of children and their rights in digital spaces cannot be considered solely a legal issue but must include a social and ethical responsibility. International instruments such as the Convention on the Rights of the Child (1989)[2] and national laws such as the Protection of Children from Sexual Offences (POCSO) Act, 2012[3] specify the responsibility to ensure children have safe spaces. However, when faced with the unique aspects of cyberspace, the global nature of the internet, the anonymity of the offender, and limitations to domestic law enforcement become confounding.

This report investigates the many aspects of children's digital exploitation, specifically online grooming, cyberbullying, and the development of Indian law. It exposes less discussed topics such as the dark web, cross boarder enforcement obstacles, the psychological effects of victimisation and threats from AI. By examining these unusual aspects, we advocate for legal reform, more robust enforcement mechanisms, and comprehensive protection mechanisms so that children's rights can be protected in an increasingly digitalised world.

The Dark Web and Anonymous Networks

The dark web has become one of the darkest spheres for child exploitation. The dark web is distinct from the surface web, which is indexed and controlled. The dark web exists in encrypted networks like Tor (The Onion Router), where the identity of users is disguised.[4] This

[1] Sameer Hinduja and Justin W Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edn, Sage 2014).
[2] UN General Assembly, *Convention on the Rights of the Child* (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.
[3] Protection of Children from Sexual Offences Act 2012 (India).
[4] R. Moore and T. Rid, 'Cryptopolitik and the Darknet' (2016) 58 *Survival* 7.

makes it an extremely lucrative marketplace for offenders, because they can freely trade illegal content, which includes child sexual abuse materials (CSAM), with very little fear of being detected.[5]

From India's perspective, policing the dark web is problematic. Law enforcement lacks the forensic resources and trained cyber personnel to grapple with the challenges in cyberspace. Jurisdictional concerns complicate matters even further, given that most of these servers, and, by extension, offenders, are based abroad and cannot be acted upon by Indian law.[6] The Information Technology Act, 2000[7] allows for blocking of websites and punishment for hosting illegal content, but the mechanisms to enforce them are mostly impotent when it comes to anonymised networks.

This is a call for a two-fold response in relation to the dark web and anonymous networks, which is a general technology intervention led by an investment in AI-based digital forensics, and secondly, but no less significant, working together internationally. If this is not taken seriously, the dark web will continue to be a prevalent yet largely invisible source of destructive activity in relation to child abuse.

Online Grooming and Trust-Building

Online grooming is a psychological exploitation in which the offenders establish intimate connections with children to lower their defences and to convince children to engage in sexual behaviour.[8] In contrast to direct physical abuse, grooming is manipulative; it lessens the child's defences through repeated trust and fondness told by flattery, false identities, and/or other false promises for affection or gifts.[9]

In India, grooming is not an actual codified offence per se. Groomers have been charged under the more broader provisions of the POCSO Act, 2012 or the Information Technology Act, 2000[10]. However, both legal limitations only charge grooming as a trivial crime, or males

[5] Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Europol 2022)
[6] Sameer Hinduja and Justin W Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edn, Sage 2014)
[7] Information Technology Act 2000 (India), ss 66, 67, 69.
[8] C. Wurtele, 'Preventing the Sexual Exploitation of Minors Online: The Role of Grooming Awareness' (2014) 29 *Journal of Child Sexual Abuse* 1.
[9] R. Wolak, D. Finkelhor and K. Mitchell, *Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment* (American Psychological Association 2012).
[10] Protection of Children from Sexual Offences Act 2012 (India); Information Technology Act 2000 (India), ss 66, 67.

should not harm the body of a child when they were grooming; moreover, both will never be able to explain or understand processes like emotional manipulation or desensitisation because grooming does not start on that day or some days before when an offender has or has not done anything explicit sexual although the child has still experienced harm.

It is important to acknowledge grooming as a separate offence with appropriate support protocols for digital evidence and a child-sensitive investigative process. Greater clarity around the law, along with future public awareness campaigns, should help India protect children from a growing issue that remains obscured for the time being.

Cyberbullying and Digital Harassment

Cyberbullying is one of the most insidious forms of abuse in the digital era, which typically entails repeated harassment, humiliation, or threats targeted at children using electronic channels.

In India, without statutes specifically dealing with cyberbullying, victims must rely on the relevant provisions of the Indian Penal Code, 1860[11], the Information Technology Act, 2000, and the POCSO Act, 2012. These laws include provisions that refer to harassment and obscenity, but fail to address the psychological harm one experiences when subjected to ongoing and repeated abuse online.

In light of this, India needs to adopt relevant and cohesive framework for cyberbullying which employs punitive solutions balanced with prevention techniques such as school based programs for awareness, schools programs for digital literacy, and platforms for reporting complaints to social media.

Cross-Border Enforcement Issues

One of the most difficult challenges to fighting the digital exploitation of children is the borderless nature of cyberspace. Offenders often operate in multiple jurisdictions - hosting servers in one, attempting to lure children in another, and distributing the content globally.

Particular barriers are presented for India to get cooperation from foreign platforms. The

[11] Indian Penal Code 1860 (India), ss 354A, 499;

Mutual Legal Assistance Treaties (MLATs) or regional conventions may provide mechanisms for cooperation, but the possible bureaucratic delays in terms of timeliness makes it very easy for the evidence to languish and/or grow stale[12]. Moreover, even platforms like Telegram and dark web forums routinely use end-to-end encryption which makes it difficult for authorities in India to trace perpetrators.

Lastly, without reciprocity and fuller participation in instruments like the Budapest Convention on Cybercrime, 2001, India is unlikely to see integrated and synchronized efforts.

Psychological Dimensions of Child Victimisation in Digital Spaces

The psychological damage inflicted upon children in digital online spaces is both deep and long lasting. The process of online grooming, cyber bullying and sexual exploitation of children abuses the developing cognitive and emotional settings of children. The dimension of digital exploitation transcends physical abuse in ways that are irreversible, as images and videos will always exist—therefore children can never escape the emotional distress and trauma, even if they do not have to deal with the abuser.

Victims i.e. children who face online exploitation often struggle with developing trust issues, anxiety and depression. Cyber bullying in association with the children impacted may result in low self-esteem, suicidal ideation, and worsened academic performance. In scenarios related to CSAM, the constant forcing of their own content back into the world may deepen and intensify the feeling of helplessness, loss of control, and futility that children experience.

As a result, to respond to digital exploitation, not only do punitive legal measures need to be taken into consideration but also the supportive measures of employing psychological care, school-based awareness programs, and trauma integrated measures need to be implemented.[13]

AI, Deepfakes and the Next Generation of Technological Threats

The transformation of artificial intelligence (AI) is creating immediate threats to children online, particularly in the forms of deepfakes, generative AI and bots. Unlike traditional

[12] UNODC, *Manual on Mutual Legal Assistance Treaties for Cybercrime* (United Nations Office on Drugs and Crime 2013).
[13] UNICEF, *Child Online Protection: Global Guidance for Policymakers* (UNICEF 2020).

instances of exploitation that entail the potential for a physical interaction with the child, the tools allow perpetrators to create CSAM.

For India, this threat is compounded by the lack of specific legislation related to synthetic CSAM. Although the IT Act, 2000 and the POCSO Act, 2012 outlaw various elements of online sexual exploitation of children, these laws do not specify the nature of AI-generated abuse. Likewise, because enforcement agencies do not possess the technical infrastructure to decompose AI-based exploitation networks, this undoubtedly complicates the response.

A legal response which foresees this threat is necessary. The response must incorporate AI digital forensic tools, algorithmic detection tools and an active international dimension that ensures technology contributes towards an effective shield and not aggravated threats.

The Gaps in the Indian Legal Framework and Need for Reform

The battle against digital exploitation of children requires a multi-faceted approach that integrates legal reform, feeds into policy innovation, supports technical tools, and addresses social consciousness. India has made a start with laws like POCSO and the IT Act, and it is now time to look forward to proactively expected futures such as online grooming, synthetic CSAM, and artificial intelligence-inspired exploitation.[14]

- **Legal reform**

  India needs to amend the POCSO itself to include grooming practices online, and the possession, etc., of synthetic child sexual abuse material, and other forms of digital crimes against children should be written into a singular statute for clarity and to avoid duplication. [15]Extraterritorial provisions for access should also be expanded upon, and potentially India can join the Budapest Convention on Cybercrime.

- **Technical protections**

  Law enforcement will need access to and use of AI detection tools for decryption and scenario analysis, forensic software, and dark web monitoring to identify offenders and

[14] Protection of Children from Sexual Offences Act 2012 (India); Information Technology Act 2000 (India).
[15] Sameer Hinduja and Justin W Patchin, *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd edn, Sage 2014).

dismantle exploitation.[16] Engaging and disbanding levels of information at all times is key. Global tech companies must be engaged to ensure takedowns are in "real time," and indigenous cyber-forensic capacity discussed to lessen reliance on foreign platforms.

- **Institutional Building and Capacity Building**

  All states should create dedicated cybercrime units with child protection expertise. Regular training for police, prosecutors and judiciary on digital evidence will enable effective law enforcement and the best service to victims. Investment in digital literacy programmes for children, parents and educators will also build resilience to factors that put them at risk online.

- **Victim-Focused Support**

  As well as legal measures, victims will require mental health services, rehabilitation programs, and child friendly access to reporting. By removing shame and stigma around reporting and ensuring informed and confidential service for victims, they may begin to seek help.

Recommendations

Responding to the digital exploitation of children requires a thorough and multi-faceted response that closes gaps in law, technology and enforcement. This report provides recommendations of immediate reforms:

- **Legislative reform**

  The POCSO Act 2012 and the IT Act 2000 should be amended to distinguish and specify the criminality of on-line child pornography including deepfakes and AI-enabled grooming. The identification of synthetic CSAM and preparatory grooming in law will presently close loopholes that undermine prosecution – and conditions which are unacceptable in a civil society.

[16] Council of Europe, *Convention on Cybercrime* (Budapest, 23 November 2001).

- **Cyber forensic Pathways and Training**

  Law enforcement agencies need access to AI detection tools, dark web tracking capability and full forensic software capability. Dedicated cyber-forensics labs in every state will support uniform enforcement and provide forensic support to law enforcement agencies. Technology partnerships with platforms and organisations will assist in real-time preservation of any evidence for child protection.

- **Cyberbullying Child-Specific Law**

  A separate statute is warranted to protect minors from sustained online harassment, illegal sharing of images without consent, impersonation and cyber-stalkers. This law should stipulate punitive consequences while mandating counselling and restorative practices that acknowledge the psychological cost it takes on a child.

- **Digital literacy campaign**

  Cyber safety needs to be taught as a compulsory subject in schools. You could have a series of training modules set for children, parents and teachers, that will create resilience (Immune System) regarding on-line grooming, breaches of privacy and harassment or bulling. You would need to have a nationally followed campaign that normalises what safe practices are whilst being online.

- **Cross-Border Treaties**

  A key step for India will be to sign bilateral treaties and platform-level agreements to streamline their process for takedowns for harmful content and obtaining digital evidence. International cooperation would also be helped by India's accession to the Budapest Convention on Cybercrime.

- **Safeguards against misuse**

  To safeguard against misuse of child protection laws, especially in the case of POCSO with consensual teenage relationships, new judicial oversight mechanisms should be created to punish genuine cases of exploitation while preventing the criminalisation of youth.

Conclusion

The digital world has afforded children unprecedented opportunities for growth and development, but children are more exposed than ever to complex and evolving forms of exploitation. This research paper finds that the problem of child abuse is not as apparent as cases of children clearly being abused, but includes other aspects like the dark web, enforcement challenges with cross-border investigations, the maleficent effects of psychological trauma, and the new dangers posed by AI.

India has take steps forward with the POCSO Act, 2012 and the Information Technology Act, 2000, but they cannot safeguard children against these emerging technological dimensions of abuse. Not only do we need a revamped legal framework, we need a global disciplined cooperative response, and unified holistic strategies to safeguard children.

Above all, safeguarding children online is not only a legal fine, but a moral one.