

PSYCHOLOGICAL MANIPULATION AND ONLINE ABUSE OF CHILDREN THROUGH SOCIAL MEDIA PLATFORMS: A LEGAL AND BEHAVIORAL STUDY

Urwashi Nirmalkar, Assistant Professor, Faculty of Law, SAM Global University, Raisen, Madhya Pradesh

Abstract

In a world where the use of social media has exploded, the ways in which children develop and interact with each other have completely changed, while also providing new avenues for psychological manipulation and abuse. This paper examines the psychological mechanisms involved in the experience of online child abuse; the behavioural manifestations of perpetrators and victims; and the changing laws aimed at addressing online child abuse. The study draws on the theories and concepts of clinical psychology, criminology, developmental neuroscience and international law to examine the concept of grooming practices, coercive control, the nature of cyberbullying, and the long-term psychological effects on the child victim. A comparative study of legislative action at various levels of government (including the EU, the UK, India and the USA) shows that there are large gaps between what is technologically feasible and what is legally protected. Additionally, the paper will explore the concept of platform accountability, algorithmic complicity, and parental/educational interventions. Results show that effective child protection is achieved through a multi-layered strategy that combines strong policy-making, technology measures at the platform level, trauma-informed clinical practices, and general digital literacy training. Finally, the paper offers recommendations for policy makers, mental health providers, teachers and tech companies.

Key-words: online child abuse, psychological manipulation, grooming, cyberbullying, digital predation, child protection law, social media regulation, trauma, platform accountability, online safety, developmental psychology.

1. INTRODUCTION

Social environment of children and adolescents is no exception to the digital revolution impacting almost all aspects of human life. Today, social media giants Instagram, TikTok, Snapchat, Discord, Facebook, YouTube, and the ever-growing list of new apps have become the new social space for hundreds of millions of minors across the globe. Pew Research Center (2023) found that 95% of U.S. teens say they use social media, and 46% say they are 'almost constantly online'. These figures are similar in developed and developing countries.

Digital connectivity has clear benefits for children, such as the ability to connect with peers, to create, to learn, and to participate in society, but these spaces have also been the breeding ground for a variety of damaging behaviours that are directed at children. This intimacy and anonymity of communication online can be used for systematic psychological manipulation, grooming, exploitation and abuse. At the same time, peer-to-peer harms, such as cyberbullying, image-based abuse and online harassment have become major concerns for child mental health and wellbeing.

The psychological and legal aspects of this are complicated and pressing. Online manipulation strategies exploit well-documented developmental vulnerabilities in adolescents' brains, such as increased reward sensitivity, immature impulse control, sensitivity to social influence and the innate developmental need for belonging to others. The digital technologies have been continually evolving and outpacing legislative and regulatory measures, leading to systemic child protection gaps.

This paper makes a detailed interdisciplinary study of these phenomena. It brings together empirical findings from clinical psychology, developmental neuroscience, criminology, sociology and legal research to provide a full and integrated understanding of how children are psychologically manipulated in online environments, by whom, who is most vulnerable, what harms arise, and how the law and policy have sought sometimes unsuccessfully to respond. The analysis considers the psychological processes at the micro level, moves to the legal and institutional dimensions at the macro level, and concludes that child protection must be achieved at all levels at the same time.

2. CONCEPTUAL FRAMEWORK AND DEFINITIONS

Establishing clear definitional parameters of the concepts for which substantive analysis is to be conducted. Any precision in this field is a prerequisite for a thorough analysis that is both contested and jurisdiction specific.

2.1 Online Child Abuse

Online child abuse is the type of child abuse that involves any type of abuse sexual, psychological, physical or financial and is committed, facilitated, or mediated by digital technologies. The Internet Watch Foundation (IWF, 2023) defines it as a part of any abuse that involves a digital element, either as a primary way of committing the offence, as an additional tool or as a way of documentation and distribution of the abuse. This is a very general term to describe a range of behaviours from online sexual solicitation to cyberbullying, financial exploitation and distribution of intimate images without consent.

While the psychological nature of online child abuse is similar to that of offline child abuse, the characteristics of online offending are distinct from offline offending:

- geographical disinhibition
- permanency and replicability of digital evidence and material
- scalability of offending through technology
- intimacy and anonymity of digital communication.

2.2 Psychological Manipulation

Within the field of clinical and forensic psychology, psychological manipulation is the application of indirect, covert, or coercive influence strategies to influence another person's thinking, feeling, or behavior in a manner that is inconsistent with the target's free will and welfare (Simon, 2010). Manipulation can take many forms in the context of online child abuse, such as deceptive, flattering, developmentally inappropriate dependency, fear creation, normalization of inappropriate behavior, and cognitive and emotional vulnerability exploitation. The concept is different from legitimate social influence, because it is intentional, exploits the vulnerability and disregards the interests of the target.

2.3 Grooming

Perhaps the most thoroughly researched type of psychological manipulation in the child protection literature is grooming. It is a process and not one act in which a perpetrator systematically gains trust, breaks boundaries and habituates a child (often family, community) to inappropriate contact, making it easier to sexually or otherwise exploit them (Craven, Brown, & Gilchrist, 2006). Grooming is offline and online, but it is much easier to groom in the online space, in terms of anonymity, speed, and extent.

Lanning (2010) states that there are three main grooming targets: the child victim directly, child's caretakers to gain a proximal connection, and child's community to create social legitimacy. The first pathway is especially exacerbated through online grooming where the offender is able to establish an intimate one-on-one relationship with the victim without the supervision of the caregiver.

2.4 Cyberbullying

Cyberbullying is defined as "Digitally orchestrated, intentional, repeated aggressive behavior against another person with the intent to harm, distress, or humiliate". Unlike offline bullying, it has four characteristics described by Kowalski:

- may reach the victim at any time (24 hours a day);
- the perpetrator may remain anonymous;
- the humiliating content may be viewed by many individuals;
- the victim may not be able to withdraw from the situation.

Examples of cyberbullying are online harassment, doxxing, impersonation, exclusion campaigns, and the sharing of embarrassing photos or images.

2.5 Child Sexual Abuse Material (CSAM)

Any visual representation of sexually explicit conduct of a minor is considered to be Child Sexual Abuse Material (CSAM) (previously and now referred to as 'child pornography'). The change

from the term 'pornography' to 'abuse material' illustrates the changing attitude to the categorisation as pornography is now seen to be a record of abuse, not an abstract label for sexual material. In 2022, the National Center for Missing and Exploited Children (NCMEC, 2023) received 32.1 million reports of apparent CSAM, a 12-fold increase from 2010, with the vast majority of these reports made via major social media and messaging platforms.

3. BEHAVIORAL TYPOLOGY OF ONLINE PREDATORS

To better comprehend online child abuse, it is necessary to understand the individuals who perpetrate it. There is a considerable amount of literature in forensic psychology and criminology concerning typologies of offenders, but it is worth noting that there is no one-to-one relationship between typologies and distinct categories. Individual offenders often portray several characteristics of more than one offender type, and typologies are not a method of prediction and exclusion of the risk.

3.1 Typological Classifications

In the literature there are several typological frameworks. The Finkelhor Precondition Model, though not as recent as the internet, is still very basic. Finkelhor has defined four conditions under which child sexual abuse can happen:

- (1) a motivation to abuse;
- (2) overcoming of internal inhibitors;
- (3) overcoming of external inhibitors; and
- (4) overcoming of child resistance.

Digital technology changes conditions (3) and (4) in a radical way, eliminating many of the external obstacles to organized behavior such as geographic closeness, parental control, social witness and offering tools specifically designed to challenge and defeat child resisters through manipulation.

More recently, Briggs, Simon, and Simonsen (2011) suggested a typology between 'contact-driven offenders' and 'fantasy-driven offenders' online. Offenders who contact their victims on the internet predominantly target them for identification, grooming and physical access, and communication online is a precursor to planned offline abuse. Fantasy-driven offenders, on the other hand, are offenders whose primary mode of online sex communication and CSAM collection is with no immediate desire for physical contact. In practice, however, this gradation is often not clearly defined: empirical research by Wolak et al. (2004) indicates that offenders who start out with fantasy may progress toward contact offenses over the course of grooming.

3.2 The Fixated vs. Regressed Distinction

Both the 'fixated' and 'regressed' offender type (Groth, Hobson, & Gary, 1982) have relevance to online predation. Fixated offenders are those who have a primary and exclusive sexual attraction to children that begins at a young age, lasts for a long time, and has complex operational patterns. They are overrepresented in premeditated online grooming as they know many details about child psychology and have invested in the selection of their victims for a long period of time. By contrast, regressed offenders may have primary adult sexual orientations but undergo situational regression to child directed behaviors, and this may be triggered by psychosocial stressors. They may not be as systematic in their offences, but the reduced barriers to accessing the internet increases their opportunities.

3.3 Cyberbullying Perpetrators

Cyberbullies are a different, but not mutually exclusive, type of perpetrators. Kowalski et al. (2014) describe a number of different types of cyberbully perpetrators, such as: the 'vengeful angel' who acts out in a supposed 'retaliation'; the 'power-hungry' bully who is seeking dominance and control; the 'mean girl' who is motivated by social exclusion and reputation management; and the 'inadvertent cyberbully' who does not initially realize their behavior is harmful. The results of Hinduja and Patchin (2021) research show a strong association between offline and cyberbullying: some 64% of cyberbully perpetrators were also involved in offline bullying, reflecting similar psychological traits such as callous-unemotional personality features, lack of empathy, and norms that favor aggression.

No matter the typology, online predators have some common characteristics in how they operate, which are ingrained in the medium. Online predators, no matter their typology, have some common characteristics of how they work, brought to the digital medium. Research by Wolak, Finkelhor, Mitchell, and Ybarra (2010) shows that there are consistent patterns of exploitation, such as: initial contact via gaming platforms, social media, or chat applications where children are already present; adoption of false identities, often as “peers” or young adults; systematic information gathering to identify vulnerabilities; gradual escalation of intimacy; introduction of sexual topics via gradual desensitization; maintaining the secret through flattery, gifts, threats, or appeals to shared identity; and exploiting the specific affordances of individual platforms.

Table 1: Comparative Typology of Online Child Abuse Perpetrators

Type	Primary Motivation	Platform Preference	Key Behavioral Indicators
Fixated Offender	Exclusive sexual attraction to children	Gaming, social media, private messaging	Systematic grooming, sophisticated deception, long-term victim investment
Regressed Offender	Situational, stress-precipitated	Adult social media platforms	Impulsive contact, less elaborate grooming, prior adult relationships
Contact-Driven	Physical access to victim	Platforms with location features	Rapid escalation toward offline meeting
Fantasy-Driven	Sexual gratification through digital interaction	Private messaging, dark web	CSAM collection, role-play solicitation, lower contact-seeking behavior
Cyberbully	Power, social dominance, revenge	Public social media, gaming platforms	Repeated targeting, peer coordination, anonymous harassment

4. VICTIM PSYCHOLOGY AND VULNERABILITY FACTORS

This is because knowledge of the factors that make some children more susceptible to online manipulation and abuse are vital to clinical interventions as well as the development of prevention programs. The first point to remember is that the word "vulnerability" does not mean "victim," and the victim is never blamed for the violence committed and the consequences it entails. Vulnerability analysis is only used for informing protective interventions.

4.1 Developmental Vulnerabilities

Adolescent cognitive and emotional development leaves them vulnerable to exploitation by predators. Steinberg's (2008) dual-systems model suggests that there are two partially independent neurological systems that mature at different times in development: the socioemotional system, which matures quickly during early adolescence, characterized by increased sensitivity to rewards, and sensitivity to the peer group; and the cognitive control system, which matures more slowly and extends through the mid-twenties, involving greater control of impulses, long-term planning, and resisting social pressure. This developmental gap between these systems (adolescents have strong social and emotional needs that are rapidly developing before they have the cognitive process to manage them) generates a window of opportunity for being manipulated.

This neurological system has been thoroughly researched and supported by a significant body of empirical evidence indicating that adolescents are more vulnerable to: peer pressure and social influence; risky decision-making in emotionally charged situations; impulsive decision making in light

of immediate rewards versus future consequences; and poor judgment regarding the trustworthiness of online contacts (Steinberg, 2010).

4.2 Psychosocial Risk Factors

In addition to normative developmental vulnerabilities, individuals are at increased risk due to a variety of psychosocial factors. In a nationally representative study of online victimization, the following were found: Prior sexual or physical abuse; family conflict and instability; low parental monitoring; social isolation or peer rejection; LGBTQ+ identity (increased online identity exploration and decreased access to supportive offline relationships); depression, anxiety, and low self-esteem; and high online social risk-taking behaviors. These factors often occur together and interrelate, and there are often no easy profiles of vulnerability.

The link between childhood trauma and being a victim of online victimization is especially well established. Children with a previous history of trauma had different stress response systems that impaired their ability to evaluate threat in new social contexts, as found by Jonzon and Lindblom (2004). Online, it can become harder to identify that care is sincere versus insincere, that the relationship is truly intimate instead of being one that is being manipulated, and that it is not too much or too soon to be skeptical of the relationship.

4.3 Media Literacy Skills & Strategies

There are a number of online behaviours that have been linked to high victimisation risk. We found the tendency to disclose more information about oneself and engage in riskier behaviors online than offline, or 'online disinhibition,' to be a notable risk. This phenomenon was first described by Suler (2004) and is the result of four different factors that online environments provide: anonymity, invisibility, asynchronous communication, and 'minimized authority'. Online disinhibition is a general phenomenon, but it is especially strong in adolescents, and could be exacerbated by past trauma or social anxiety.

Table 2: Developmental Vulnerability Profiles by Age Group

Age Group	Platform Usage Patterns	Primary Vulnerabilities	Typical Abuse Forms
6-9 years	Gaming, child-directed apps (Roblox, Minecraft)	Trust, naivety, authority compliance, lack of digital literacy	Gaming grooming, in-app solicitation, in-game gifts for personal information
10-12 years	TikTok, YouTube, early social media	Identity formation, peer approval seeking, limited impulse control	Social media grooming, peer cyberbullying, image solicitation
13-15 years	Instagram, Snapchat, Discord, online gaming	Romantic attachment, body image concerns, risk-taking, independence seeking	Sextortion, grooming, sexting coercion, peer sexual harassment
16-17 years	Full social media spectrum, dating apps	Emotional intimacy seeking, adult identity exploration, financial naivety	Financial exploitation, intimate partner cyberstalking, CSAM production coercion

5. TYPES OF ONLINE ABUSE OF CHILDREN

Online abuse of children can take many forms and is an ever-changing form of abuse. This section reviews systematically the main categories found in the empirical and clinical literature.

5.1 Online Sexual Grooming and Exploitation

Online child abuse, specifically online sexual grooming has been the subject of the most in-depth research and is the most focused upon in most legislations. As outlined in Section 4, it's a

deliberate process of trust-building, the erosion of boundaries, and sexual desensitization targeting sexual abuse. The Internet Watch Foundation (2023) states that 92% of all CSAM identified on the internet was self-generated - that is, most of it is produced by adults, often as a result of grooming.

This definition reflects what is referred to as 'online facilitated child sexual abuse' whereby children have been groomed online and subsequently sexually abused offline. The association of digital and physical sex offending is reflected in a study of convicted internet sex offenders in the UK which confirmed that 43% had been convicted of an online contact offence with a child. In contrast, Wolak contest the dominant 'stranger danger' discourse: in contrast to the popular image of an online predator, most such predators do not deceive their victims about their age or intent, but instead are characterized by using 'straightforward methods' of flattery and romantic relationship development, taking advantage of adolescents' developmental vulnerabilities for enacting romantic attachments.

5.2 Sextortion

One of the fastest growing types of online child abuse is sextortion, the demand for a child to provide images of himself or herself in sexually explicit positions or other images, financial compensation or sexual activity, or whatever, in exchange for refraining from sharing similar photos or photos of other minors with others. The Public Safety Alert from the FBI in 2023 reported an increase in financially motivated sexually exploitative activity targeting adolescent boys, where offenders are typically trying to pass off as a female peer, and successfully getting one image before using that image for financial extortion. Sextortion differs from traditional sexual grooming because it doesn't involve developing a relationship with the victim before moving from contact to extortion, but rather from hours to days.

Sextortion is a serious and immediate psychological issue. The victims feel a deep sense of shame, fear and powerlessness, and a study by Wittes. has found that victims of sexting were more likely to experience suicidal ideation, especially adolescent boys who are subject to an extra stigma of being a womanizer. Multiple jurisdictions have been subject to significant policy attention for several high-profile cases of adolescent suicide that have followed a sextortion campaign.

5.3 Cyberbullying

Cyberbullying is the most common form of online peer-to-peer victimization experienced by children, and there is a wide range of estimates for prevalence from 15% to 45% based on the definition or measurement tool used. Cyberbullying is the intentional use of digital technology by peers to harass, bully, embarrass, threaten or harm others. Forms of this harassment include direct harassment (threats or abusive messages), relational aggression (deliberate exclusion from online social groups), public humiliation (embarrassing pictures or content), impersonation (creating fake profiles), outing (sharing private information without permission), and stalking (persistent unwanted contact).

Cyberbullying on social media is exacerbated by its public nature. There are no limits on who can see the bullying when it happens online: limitless viewers, unlimitable storage, round-the-clock targeting into the victim's home environment. However, in adolescent social situations, the 'audience effect' the presence of bystanders is especially detrimental in the developmentally salient arena of reputation management.

5.4 Non-Consensual Intimate Image Sharing

Non-consensual sharing of intimate images (NCII) takes place in a variety of contexts, such as when a peer sends a consensual sexting image with the understanding that it will not be shared beyond the intended recipient; and when an adult distributes an intimate image produced as a part of grooming practices; and when an intimate image is created and distributed via a process that constitutes CSAM. The production, possession, and distribution of sexual images are serious criminal offences for minors whether the image appears to be consensual or not,

The research conducted by Ringrose with adolescents in the UK highlighted high levels of gendered power differentials; boys reported high social rewards to receiving and sharing intimate images of girls, and girls reported high levels of social sanctions for not complying and/or for refusing to share intimate images with boys. This imbalance is due, in part, to a more general power imbalance between women and men, which is exacerbated in online environments where the consequences of distributing images are particularly severe for girls.

5.5 Online Radicalization and Cult Recruitment

Another intriguing and little-known type of psychological manipulation affecting children on the Internet is radicalization and cult-like recruitment. Vulnerable youth have been targeted by extremist groups in many ways from both sides of the political and religious spectrum over the past few years using manipulation strategies that have structural similarities to sexual grooming: identity exploration and exploitation, false sense of belonging, incremental ideological escalation, and the development of an "us vs. them" mentality that separates the target from others' relationships.

Moonshot CVE has found that 42% of those who have been identified as extremist content consumers online were aged between 13 and 24, with the highest vulnerability period being middle adolescence, when identity formation is most intense. Developmental vulnerability and advanced digital recruitment present a daunting challenge to child protection and counter-terrorism mechanisms.

5.6 Financial Exploitation

Online financial exploitation of children includes a spectrum of activities from financial fraud and scams involving children and exploitation of children through financial manipulation. This involves tactics used in games (loot box abuse, scarcity manipulation), romance scams (on older adolescents) and outright financial requests (in sextortion). The in-game economies are a vector that presents itself as a particularly significant loss: the Federal Trade Commission (2022) reported that more than \$200 million in fraud was reported in gaming and social media platforms against people under 20.

6. LEGAL FRAMEWORKS: DOMESTIC AND INTERNATIONAL

The legal framework for online child protection is multilevel, complex, fragmented, and also has significant gaps between the legal framework and the technological reality. This section compares the legislative and regulatory responses to the crisis in key jurisdictions and internationally.

6.1 International Legal Framework

The basic international document dealing with children's rights is the United Nations Convention on the Rights of the Child (UNCRC, 1989) which was ratified by 196 states and is the most widely ratified human rights treaty in history. Article 34 clearly requires States to protect children from all types of sexual exploitation and abuse, and Article 19 requires States to ensure children are not subjected to any form of violence, injury or exploitation. The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000) puts these duties into effect and explicitly includes online exploitation, and requires the criminalisation of CSAM production, distribution and possession.

More specific and operationally detailed are the frameworks of the Budapest Convention on Cybercrime (2001) and of the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) adopted by the Council of Europe. The Lanzarote Convention is especially relevant in the definition of 'grooming' as an independent offence (Article 23), the criminalisation of 'corruption of children' in exposure to sexual content and the minimum age of protection standards. To date, 47 countries are party to the Lanzarote Convention (2023).

The Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography (2011/93/EU) sets minimum standards for the criminalisation of certain offences and protection of victims in EU member states at the European Union level. The most recent major development in European platform regulation is the landmark Digital Services Act (DSA, 2022), which represents not only one of the most significant pieces of legislation ever passed to regulate platforms but also places a number of far-reaching due diligence obligations on 'very large online platforms,' including a duty to carry out a risk assessment for child safety and a duty to proactively detect and remove content.

6.2 International Legal Framework

The U.S. has one of the most comprehensive U.S. child protection laws addressing online protection, which also has significant jurisdictional complexity and is subject to continuing debates over constitutionality. Federal laws relating to Internet child protection include: the PROTECT Act (2003) which criminalized computer-facilitated sexual exploitation and enhanced sentencing for

CSAM offenses; the CIPA (Children's Internet Protection Act, 2000), which requires that federally funded libraries and schools implement Internet filtering; COPPA (Children's Online Privacy Protection Act, 1998), which provides data privacy protections for children under 13 years of age and requires verifiable parental consent for data collection; and SESTA/FOSTA (2018), which amended Section 230 immunity to allow for civil and criminal liability for platforms that facilitate sex trafficking.

The Sexual Exploitation of Minors Statute is the primary federal criminal law pertaining to CSAM offenses, with a sentence of 15 to 30 years for production and distribution offenses. The PROTECT Act amendments to the Mann Act introduce extraterritoriality and make interstate transportation of minors for sexual exploitation a crime. Federal laws against grooming make it a crime to coerce or entice a minor into sexual activity through any means of interstate or foreign commerce. One controversial aspect of 230 of the Communications Decency Act (1996) that has remained a point of discussion in the child protection arena is that it shields platforms from liability for third party content. Those who oppose Section 230 immunity say it allows platforms to reap profits from problematic content without being held accountable for the harms caused by that content, while those who support it say that liability would stifle free speech and free the internet. The EARN IT Act has been introduced multiple times on the floor of Congress and suggested that Section 230 immunity be contingent on the platforms' adherence to child safety standards, but as yet it has not been passed as of this writing.

6.3 United Kingdom Legal Framework

The United Kingdom has put into place a comprehensive legal framework for online child protection, including the Sexual Offences Act 2003 criminalising child grooming (under Section 15) and online sexual solicitation. The Online Safety Act 2023 is the most recent piece of legislation, imposing a duty of care on online platforms, mandating a proactive approach to risk assessment and mitigation for children and young people and granting Ofcom substantial powers to regulate and enforce, such as fines of up to £18 million or 10% of global annual revenue. Age assurance technology is one of the child safety measures mandated by the Act, as is the default privacy settings to safeguard children and the filtering of content. The UK has also created a public-private partnership for the detection and removal of CSAM called the Internet Watch Foundation.

6.4 Adolescent Sexting: Legal Complexity

One of the most legally contentious issues in the field is the criminalization of adolescent consensual exchange of intimate images between adolescents of similar age (peer sexting). Existing CSAM laws define any photograph of a child being intimate, no matter how the image was taken, as child pornography, essentially holding teenagers who have created their own images responsible for committing serious felonies. The prosecutor's decision in these cases has been inconsistent and there has been a lot of public debate surrounding several "sexting teens" prosecutions for consensual sexual images.

More legal experts and child welfare groups agree that the implementation of 'Romeo and Juliet laws' is essential to prevent CSAM from being exploited by adults and ensure there are clear penalties for those who distribute such content without the consent of the sender. In 2023, there were about 27 states in the United States that have implemented some version of a modified sexting law that ranges in scope and effectiveness.

6.5 Adolescent Sexting: Legal Complexity

The criminalization of adolescent peer sexting, defined as the consensual sharing of intimate images between young (age 12-17) individuals, is one of the most legally contentious issues in the field. Most current CSAM laws define intimate pictures of minors as child pornography, even if there is an apparent understanding of consent, thus technically putting adolescents who willingly share self-generated images in a precarious position of committing serious felonies. Such prosecutorial discretion has been inconsistent, and there have been several seminal cases of criminal charges against teenagers for consensual peer sexting for which there has been much public controversy.

6.6 India Legal Framework

The government's legal framework for addressing child sexual abuse on the internet is based largely on the Protection of Children from Sexual Offences Act (POCSO) 2012 that was amended in 2019 to substantially improve the punishment for offenses and expand coverage to online crimes. The amendments to POCSO have introduced electronic media as a new category for grooming, solicitation or creation of CSAM and punishable with life imprisonment. The IT (Amendment) Act 2008 has added to provisions of the Information Technology Act 2000 relating to electronic publishing of obscene material involving children. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 puts obligations on the social media intermediaries such as the requirement of proactive content filtering, report of CSAM etc.

There are a number of common areas of disconnect between the law and technology across jurisdictions. Although there are international cooperation frameworks, the first issue is jurisdictional fragmentation and the extraterritorial enforcement limitations, which often results in the fact that cross-border online abuse can fall through the cracks of national legal systems. Second, there are definitional problems in various jurisdictions which make evidence collection and prosecution more difficult across multiple jurisdictions. Third, platform accountability mechanisms (apart from the EU DSA) are mostly reactive, rather than proactive, and do not create obligations to make platforms more accountable. Fourth, legal ramifications of AI-generated CSAM are not settled in most jurisdictions, leaving new loopholes. Fifth, civil remedies for children are still poorly developed, and access to justice is restricted for victims who are not and/or are not willing to participate in the criminal justice system.

7. CONCLUSION

Online abuse and psychological manipulation of children using social media is one of today's greatest child welfare issues of the 21st century. It is widespread and increasing; it is complex and profoundly targeted to the developmental vulnerabilities of children and young people; it causes serious and lasting harm; and the laws and institutions aimed at combating it are structurally weak. This paper calls for an interdisciplinary perspective which does not limit the problem to its psychological, legal or technological aspects. Children affected by such manipulation are often further victimized by poorly designed institutional response; platforms on which online grooming takes place make ethical decisions; legal systems that should respond are fragmented and lacking in definition; and online grooming exploits neurobiological vulnerabilities.

Solutions should be as multi-dimensional. What they need are legal frameworks that make child safety a central tenet of platforms, and not an add-on; a clinical and educational infrastructure that is able to recognize, support, and treat affected children; and a cultural shift that helps to break the cycle of secondary victimization and stigma that permeates the entire child protection response. The right to safe participation in digital life is a fundamental right of children. Realizing that it is not enough to criminalize abuse when it has happened, but creating digital environments where abuse is structurally more difficult to commit, more easily identifiable, more reliably prosecuted, and more robustly responded to in a manner commensurate with the clinical sophistication and human dignity that every child victim deserves. Research evidence for each of the components of this response framework is available. Collective will is all that is needed now to make it happen.

REFERENCES

Statutes and International Instruments

1. Council of Europe, Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), ETS No. 201 (2007).
2. European Union, Directive 2011/93/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography (2011).
3. European Union, Regulation (EU) 2022/2065 – Digital Services Act (2022).
4. United Nations, Convention on the Rights of the Child, GA Res 44/25, UN Doc A/RES/44/25 (1989).
5. United Nations, Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000).

Reports and Official Publications

1. Federal Bureau of Investigation, Sextortion Public Safety Alert: Financial Sextortion Targeting Minor Males (FBI, 2023).
2. Federal Trade Commission, Consumer Sentinel Network Data Book 2021 (FTC, 2022).
3. Internet Watch Foundation, Annual Report 2022 (IWF, 2023).
4. Moonshot CVE, Online Radicalisation of Young People: Patterns and Trends (Moonshot CVE, 2023).
5. National Center for Missing and Exploited Children, 2022 CyberTipline Report (NCMEC, 2023).
6. Pew Research Center, Teens, Social Media and Technology 2023 (Pew Research Center, 2023).
7. Stanford Internet Observatory, Algorithmic Amplification of Child Exploitation Material: A Study of Instagram's Recommendation System (Stanford University, 2023).

Books

1. Beckett, H., Holmes, D., and Walker, J., Child Sexual Exploitation: Definition and Scope (The Contextual Safeguarding Network, 2017).
2. Bronfenbrenner, U., The Ecology of Human Development: Experiments by Nature and Design (Harvard University Press, 1979).
3. Cohen, J.A., Mannarino, A.P., and Deblinger, E., Treating Trauma and Traumatic Grief in Children and Adolescents (Guilford Press, 2006).
4. Finkelhor, D., Child Sexual Abuse: New Theory and Research (Free Press, 1984).
5. Herman, J.L., Trauma and Recovery: The Aftermath of Violence—from Domestic Abuse to Political Terror (Basic Books, 1992).
6. Hinduja, S. and Patchin, J.W., Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying (3rd edn, Corwin Press, 2021).
7. Lanning, K.V., Child Molesters: A Behavioral Analysis (5th edn, National Center for Missing and Exploited Children, 2010).
8. Sageman, M., Misunderstanding Terrorism (University of Pennsylvania Press, 2017).
9. Simon, G.K., In Sheep's Clothing: Understanding and Dealing with Manipulative People (Parkhurst Brothers, 2010).

Journal Articles

1. Berson, I.R., Berson, M.J., and Ferron, J.M., 'Emerging Risks of Violence in the Digital Age: Lessons for Educators from an Online Study of Adolescent Girls in the United States' (2002) 1(2) Journal of School Violence 51.
2. Briggs, P., Simon, W.T., and Simonsen, S., 'An Exploratory Study of Internet-Initiated Sexual Offenses and the Chat Room Sex Offender' (2011) 23(1) Sexual Abuse: A Journal of Research and Treatment 72.
3. Cooper, A., McLoughlin, I.P., and Campbell, K.M., 'Sexuality in Cyberspace: Update for the 21st Century' (2000) 3(4) CyberPsychology & Behavior 521.
4. Craven, S., Brown, S., and Gilchrist, E., 'Sexual Grooming of Children: Review of Literature and Theoretical Considerations' (2006) 12(3) Journal of Sexual Aggression 287.
5. Hinduja, S. and Patchin, J.W., 'Sextortion among Teenagers: A Comparative Study of the Nature and Dynamics of Online Sexual Coercion' (2020) 45(3) Criminal Justice Review 321.
6. Kowalski, R.M., Giumetti, G.W., Schroeder, A.N., and Lattanner, M.R., 'Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research among Youth' (2014) 140(4) Psychological Bulletin 1073.
7. Mitchell, K.J., Finkelhor, D., and Wolak, J., 'Youth Internet Users at Risk for the Most Serious Online Sexual Solicitations' (2007) 32(6) American Journal of Preventive Medicine 532.
8. Quayle, E. and Taylor, M., 'Social Networking as a Nexus for Engagement and Exploitation of Young People' (2011) 16(2) Information Security Technical Report 44.
9. Suler, J., 'The Online Disinhibition Effect' (2004) 7(3) CyberPsychology & Behavior 321.
10. Wolak, J., Finkelhor, D., Mitchell, K.J., and Ybarra, M.L., 'Online "Predators" and Their Victims' (2010) 1(S) Psychology of Violence 13.

11. Ybarra, M.L. and Mitchell, K.J., 'Online Aggressor/Targets, Aggressors, and Targets: A Comparison of Associated Youth Characteristics' (2004) 45(7) Journal of Child Psychology and Psychiatry 1308.
12. Zych, I., Ortega-Ruiz, R., and Del Rey, R., 'Systematic Review of Theoretical Studies on Bullying and Cyberbullying: Facts, Knowledge, Prevention, and Intervention' (2015) 23 Aggression and Violent Behavior 1.