www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 1045-1048

e-ISSN : 2583-1062
Impact Factor : 7.001

CHILD SAFETY IN THE DIGITAL WORLD: LEGAL AND TECHNOLOGICAL MEASURES AGAINST ONLINE EXPLOITATION AND ABUSE

Ms. Asma Jawed[1], Dr. Prem Chandra[2]

[1]Research Scholar, Sardar Patel Subharti Institute Of Law, Swami Vivekanand Subharti. University, Meerut, India.

[2]Associate Professor, Sardar Patel Subharti Institute Of Law, Swami Vivekanand Subharti, University, Meerut, India.

DOI: https://www.doi.org/10.58257/IJPREMS43921

ABSTRACT

Online exploitation and abuse targeting children have reached unprecedented levels globally. This research paper explores recent crime trends, legal responses, and technological countermeasures protecting minors in the digital space. It combines scholarly analysis and statistical data from the first half of 2025 to illustrate the urgent need for a multifaceted response. The rapid expansion of digital technologies has transformed the way children learn, communicate, and socialize, but it has also created new vulnerabilities that expose them to online exploitation and abuse. The digital environment presents risks such as grooming, cyberbullying, trafficking, and the circulation of child sexual abuse material (CSAM), which can have lasting psychological, social, and emotional consequences. Addressing these threats requires a comprehensive strategy that integrates legal frameworks with technological innovations.

From a legal perspective, international conventions such as the United Nations Convention on the Rights of the Child (CRC) and the Budapest Convention on Cybercrime provide a foundation for protecting children in cyberspace. National legislations, including India's Protection of Children from Sexual Offences (POCSO) Act, the United States' Children's Online Privacy Protection Act (COPPA), and the European Union's General Data Protection Regulation (GDPR), illustrate how different jurisdictions seek to safeguard children from digital harms. However, cross-border crimes, the anonymity of the dark web, and jurisdictional conflicts continue to challenge enforcement mechanisms.

Technological measures complement legal responses by providing preventive, detection, and intervention tools. Artificial intelligence and machine learning enable the monitoring of suspicious online behaviors and the identification of CSAM. Innovations such as Microsoft's PhotoDNA, content-filtering algorithms, and parental control systems strengthen efforts to protect children. At the same time, concerns over privacy, encryption, and digital rights necessitate a careful balance between safety and freedom.

This paper explores how coordinated legal and technological approaches can strengthen child protection in the digital world, highlighting both progress achieved and the challenges that remain.

1. INTRODUCTION

Modern children are more connected than any preceding generation, yet this access brings severe risks. As digital threats against minors multiply, safeguarding measures have become a priority for governments, international organizations, educators, and technology providers. Adapting legal frameworks and innovating new technological tools remain key strategies in the fight against online child exploitation and abuse. The digital revolution has redefined human interaction, learning, and communication, particularly for children and adolescents who are among the most active users of technology. With the increasing penetration of smartphones, social media platforms, gaming applications, and online learning environments, children are now more connected than ever before. While these digital advancements provide immense opportunities for education, creativity, and global networking, they also expose young users to significant risks such as online grooming, sexual exploitation, cyberbullying, trafficking, and exposure to harmful content (UNICEF, 2021). The anonymity and global reach of the internet amplify these risks, making children vulnerable to exploitation by individuals and organized networks operating across borders.

Online exploitation and abuse are not limited to isolated incidents; they constitute a growing global concern. Reports from organizations such as Interpol and the Internet Watch Foundation (IWF) indicate that the volume of child sexual abuse material (CSAM) has increased exponentially, with millions of images and videos circulating online each year. The psychological, emotional, and social consequences for victims are severe, often persisting into adulthood. Therefore, ensuring child safety in the digital environment requires urgent, coordinated, and multidimensional responses.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 1045-1048

e-ISSN : 2583-1062
Impact Factor : 7.001

Legal measures form the foundation of child protection. International instruments like the United Nations Convention on the Rights of the Child (CRC) and regional/national legislations—such as the Protection of Children from Sexual Offences (POCSO) Act in India, COPPA in the United States, and GDPR in the European Union—highlight global commitments to addressing online exploitation. However, gaps remain due to jurisdictional conflicts, technological sophistication of offenders, and enforcement limitations.

Complementing the legal framework, technological innovations are essential in preventing, detecting, and responding to online threats. Artificial intelligence (AI), machine learning, and digital forensics enable the identification of suspicious activities, the tracking of child sexual abuse material, and the development of parental control and monitoring systems. Tools such as Microsoft's Photo DNA and hash-matching databases provide crucial support to law enforcement agencies. Yet, the balance between child protection, privacy rights, and data security continues to pose ethical and legal challenges.

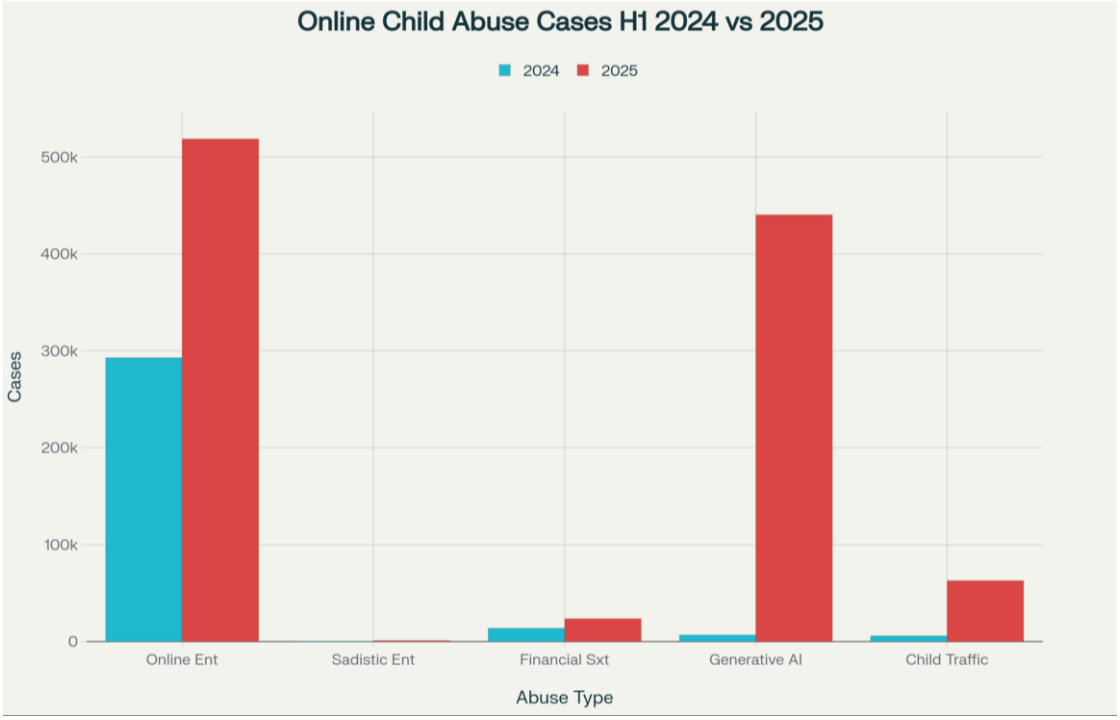
This study examines the intersection of legal and technological measures in combating online exploitation and abuse of children. It explores how laws, policies, and advanced technologies can be harmonized to strengthen child safety in the digital world while addressing the challenges of enforcement, privacy, and global cooperation.

2. THE SCOPE AND RECENT TRENDS OF ONLINE CHILD EXPLOITATION

A landmark global study found that 1 in 12 children—about 8.1%—have been subjected to online sexual exploitation or abuse. Specific subtypes, such as non-consensual sharing of images and online solicitation, occur at even higher rates, with over 12% of minors reporting unwanted sexual messages or exposure to explicit content.

An analysis of first-half 2025 statistics from the National Center for Missing & Exploited Children (NCMEC) demonstrates rapidly growing threats:

Type of Report	Jan-Jun 2024	Jan-Jun 2025
Online Enticement	292,951	518,720
Sadistic Online Enticement	508	1,093
Financial Sextortion	13,842	23,593
Generative AI Exploitation	6,835	440,419
Child Sex Trafficking	5,976	62,891



Reported Cases of Various Online Child Exploitation Crimes (Jan-Jun 2024 vs Jan-Jun 2025)

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 1045-1048

e-ISSN : 2583-1062
Impact Factor : 7.001

These figures underline how new forms of abuse—such as generative AI-facilitated exploitation—can cause enormous spikes in reporting and victimization.

3. LEGAL RESPONSES AND LEGISLATIVE DEVELOPMENTS

Recent legal developments have greatly strengthened the regulatory landscape for online child protection:

- The United Kingdom's Online Safety Act (2023, in force from July 2025) requires robust age verification for adult content, targeted risk assessments, swift removal of illegal material, and penalties up to £18 million or 10% of global turnover for noncompliance. The Act introduces new criminal offences focused on cyberflashing, deepfake abuse, and intimidation, as well as enhanced obligations for platforms to protect minors.
- In the United States, the Kids Online Safety Act establishes a duty of care by internet platforms, requiring them to implement parental controls, age-appropriate settings, default high privacy for minors, and mechanisms to easily report harmful content. Enforcement and transparency obligations have also increased, with federal and state oversight.
- The REPORT Act expands mandatory reporting for electronic service providers, including new online crimes like AI-powered offenses and sex trafficking.[1]

These changes illustrate a global movement toward enforcing platform responsibility and accountability for child online safety.

4. TECHNOLOGICAL SAFEGUARDS AGAINST EXPLOITATION

Technology plays a dual role: while it can facilitate abuse, it is also crucial to prevention and protection.

Key Digital Safeguards

- **AI and Machine Learning Detection**: Automated systems now screen for harmful keywords, detect potentially explicit imagery, and monitor suspicious online behaviors.
- **Age Verification Systems**: Privacy-centric methods (e.g., facial age estimation, ID scanning) help control access to age-restricted content.
- **Parental Controls**: Apps allow parents to monitor texts, calls, web browsing, and location, offering proactive protection for minors.
- **Content Filtering and Safe Modes**: Algorithms filter out explicit or harmful materials in children's feeds, while strict privacy settings limit interactions from unknown contacts.
- **Rapid Reporting Tools**: Enhanced mechanisms on social platforms and national CyberTipline resources facilitate faster responses and victim support.

Preventive and Educational Initiatives

- **Open Communication**: Encouraging ongoing dialog between parents, guardians, and children enables early identification of risks.
- **Education and Training**: Online safety is now part of school curricula, and staff are required to be trained in latest risks and reporting procedures.
- **International Coordination**: Policies emphasize cooperation across borders to prevent cross-platform and cross-jurisdiction abuse.

5. DISCUSSION: OPPORTUNITIES AND GAPS

While there has been major progress in both law and technology, child online protection often lags behind evolving threats. The sharp rise in generative AI-facilitated crimes demonstrates the pace at which offenders can exploit new technologies. Laws are catching up, but continuous review and international cooperation are essential. There are also privacy and implementation challenges, such as balancing robust child protection with minors' digital rights and freedom of expression.

6. CONCLUSION

Child safety in the digital world demands urgent, sustained efforts—both legal and technological. The scale and sophistication of threats will only increase, but robust regulations, innovative technical safeguards, and strong community awareness can protect minors and uphold their rights online. Regular measurement of abuse prevalence and offender tactics must inform policy, while ongoing education empowers children and their caretakers.

1. National Center for Missing & Exploited Children (NCMEC) reports, 2025.
2. Georgia State University Global Study, 2025.

3. UK Online Safety Act, 2023/2025.
4. Kids Online Safety Act, USA, 2025.
5. Technological and parental control innovations.
6. Better Internet for Kids policy workshop.

7. REFERENCES

[1] National Center for Missing & Exploited Children (NCMEC). (2025). Spike in online crimes against children a "wake-up call". Retrieved from https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call

[2] Georgia State University. (2025, January 21). Study estimates 1 in 12 children subjected to online sexual exploitation or abuse. Retrieved from https://news.gsu.edu/2025/01/22/study-estimates-1-in-12-children-subjected-to-online-sexual-exploitation-or-abuse/

[3] Wirral Safeguarding Children Partnership. (2025). The Online Safety Act 2023 in force from 25th July 2025. Retrieved from https://www.wirralsafeguarding.co.uk/news/stonger-protection-for-children-the-online-safety-act-2023-in-force-from-25th-july-2025/

[4] BBC News. (2024, February 9). What the Online Safety Act is - and how to keep children safe online. Retrieved from https://www.bbc.com/news/articles/c0epennv98lo

[5] U.S. Congress. (2025, May 13). S.1748 - Kids Online Safety Act 119th Congress (2025-2026). Retrieved from https://www.congress.gov/bill/119th-congress/senate-bill/1748

[6] Wikipedia. (2023, July 26). Kids Online Safety Act. Retrieved from https://en.wikipedia.org/wiki/Kids_Online_Safety_Act

[7] Better Internet for Kids. (2025, July 16). Protecting children online: a deep dive into technology, policy and prevention against child online exploitation. Retrieved from https://better-internet-for-kids.europa.eu/en/news/protecting-children-online-deep-dive-technology-policy-and-prevention-against-child-online

[8] NITI Aayog, Government of India. (2025, June). Online safety for children: protecting the next generation from harm. Retrieved from https://www.niti.gov.in/sites/default/files/2025-06/Online-safety-for-children-protecting-the-next-Generation-from-harm.pdf

[9] ECPAT International. (2024, January 24). Achieving child safety online through technology. Retrieved from https://ecpat.org/story/achieving-child-safety-online-through-technology/

[10] United Nations. (2023, January 31). Child and youth safety online. Retrieved from https://www.un.org/en/global-issues/child-and-youth-safety-online