

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 6

2025

© 2025 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Guarding Innocence: A Comparative Analysis of International and National Child Protection Laws on Child Pornography.

AIMAN KHAN¹

ABSTRACT

This research presents a comparative analysis of the international child protection framework, highlighting India's statutory measures against child sexual abuse, particularly the Protection of Children from Sexual Offences Act (POCSO) Act, the Information Technology Act, and the Bharatiya Nyaya Sanhita. The researcher has attempted to understand various legal frameworks surrounding the offences against children, specifically, online child sexual abuse. This is a study of laws globally that aim to protect children from online abuse. While India's legal provisions reflect International standards in defining offences, prescribing stringent penalties, and promoting child-friendly judicial procedures, significant gaps persist in institutional mechanisms when compared with countries such as the United States, Australia, and Canada.

India's non-signatory status to critical international conventions, including the Budapest Convention on Cybercrime and the Lanzarote Convention on the Protection of Children Against Sexual Exploitation, limits cross-border cooperation, delays evidence-sharing in transnational cases, and hampers coordinated action against online child sexual abuse material (CSAM), particularly on encrypted or foreign-hosted platforms.

The study also attempts at making various suggestions to strengthen the present 'child sexual abuse' oriented laws with the help of international cooperation and amendments in present national laws. Key recommendations include aligning national cyber laws with international standards, establishing district-wise Child Advocacy Centers, developing a secure sex offender monitoring system, and enhancing digital forensic and cyber policing capacities. Intensified public awareness and preventive measures are also emphasized as critical components of a resilient protection system.

Ultimately, safeguarding our future generation is not just a legal obligation of a nation, it's our moral duty, a responsibility as a growing power. It's important to understand that children are the most vulnerable yet the most crucial part of a society, the security of which, directly effects the growth of a nation. In this era of cyber space where offences transcends boundaries, it's imperative for nations to come together, and combat these crimes, through

¹ Author is a PhD Scholar at Rabindranath Tagore University, Bhopal, M.P., India.

resilient legal framework and mutual cooperation that aligns with international conventions.

I. INTRODUCTION

Technological progress is undeniably one of humanity's greatest achievements. With the advent of the internet, the world has shrunk to the size of the screen- distance is no longer a barrier to personal and professional interactions. Businesses are managed remotely, relationships are maintained across continents, and information is accessible within seconds. Although this digital revolution has been a remarkable boon, its darker, more precarious side is also visible now. The same platform that connects people is also being weaponized by the perpetrators to target the young minds.

Among the gravest manifestations of this abuse is the alarming surge in the crimes against children, majorly; online child sexual exploitation and child pornography. Child pornography, more accurately termed as child Sexual Abuse Material (CSAM), involves the production, circulation, or possession of sexually explicit material that depicts minors. In the digital era, this offense has taken a more alarming form through creation, sharing, or possession of such content via electronic and internet-based platforms. With the rapid expansion of technology and proliferation of its use, the creation of CSAM has increased at an alarming pace. Both in India and across the globe, it is considered one of the most heinous crimes, as it directly fuels child sexual abuse and exploitation.

Recent research by the Child Light Global Safety Institute², hosted by the University of Edinburgh and supported by the Human Dignity Foundation, shows that over 300 million children every year, roughly one in eight (12.6%) of the world's children, have been victims of non-consensual image-based abuse, including the taking, sharing, and exposure to sexual images or videos. To put the crises into perspective, these offences occur at an alarming rate of 10 incidents every second, making this a truly global 'hidden pandemic'.

Between in 2020-2025, like many other countries, India also has experienced a steep surge in CSAM-related cybercrime. Reports indicate that cases rose from 842 incidents in 2020 to nearly 2 lakh cases by 2024, reflecting an unprecedented escalation

² Over300 million children are victims of technology- facilitated sexual exploitation and abuse, CHILDLIGHT Global Child Safety Institute (December 4th 2024) <https://www.childlight.org/newsroom/over-300-million-children-a-year-are-victims-of-online-sexual-exploitation-and-abuse>

II. GLOBAL FRAMEWORK AND STRATEGIES

The international community has recognized the urgency of this threat. Global efforts, like the 1999 Vienna Conference on Combating Child Pornography on the Internet, emphasize the need for criminalizing activities including production, distribution, export, import, transmission, possession, and advertisement of child pornography globally. The initiatives that highlight the importance of international cooperation, covering partnerships among governments, international organizations, and the technology sector, are -

1. Optional Protocol to the Child's Rights Convention, Concerning the Sale of Children, Child Prostitution and Child Pornography -

The protocol addresses child prostitution, sale of children, and child pornography, recognizing them as a grave violation of children's rights and making them an offence. It defines these offences and obliges the government:

- Criminalizes these acts under national laws with strict penalties.
- Investigate, prosecute, and punish offenders.
- Provide comprehensive support and rehabilitation for victims, including family reunification or alternative care when necessary.

2. Convention on Cybercrime (Budapest Convention) –

Adopted in 2001, the Budapest Convention was the first international treaty specifically aimed at addressing crimes committed through the internet and other computer networks. While it broadly covers offences such as unauthorized access, data interference, fraud, and copyright violations, it places strong emphasis on content-related crimes, and emphasized child pornography also.

The convention obliges member states to:

- Criminalize the production, distribution, dissemination, and possession of child pornography through digital means.
- Establish laws against the creation and use of computer systems for exploiting children sexually.
- Impose penalties not only on direct perpetrators but also on those aiding or abetting such offences.

Importantly, the treaties stress that enforcement measures must respect human rights and fundamental freedoms. It equips authorities with the power to secure or access computer data,

trace online activity in real time, and seize digital evidence, while ensuring safeguards against misuse of power.

On a global scale, the convention fosters international cooperation, requiring parties to assist one another in investigations, share evidence, and where applicable, extradite offenders. By harmonizing laws across borders, it strengthens the fight against online child sexual exploitation in an era where perpetrators often operate beyond national boundaries.

3. The Lanzarote Convention³ –

Adopted on 25 October 2007, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, also known as the Lanzarote Convention, stands as a significant global achievement in the effort for protecting children from sexual offences.

Ratified by all 47 Council of Europe member states, the convention urges countries to take a coordinated and proactive approach to tackling child sexual exploitation in every form, whether occurring online or offline. Its key aims include-

- Preventing and addressing exploitation of children and sexual abuse of a child.
- Safeguarding the dignity and rights of children who survives such atrocities.
- Strengthen cooperation between nations to fight such crimes.

The first legally binding international treaty to criminalize all forms of child sexual abuse, including those committed abroad is the Lanzarote Convention. It emphasizes prevention through measures such as screening and training professionals, monitoring offenders, and providing a support program for victims. Additionally, it requires the signing countries to criminalize the offenses related to online child sexual abuse, like sex tourism and child grooming, along with promoting accessible mechanisms like child helplines and online reporting systems⁴.

These international conventions play a crucial role in establishing a collective global response to CSAM. They create clear legal standards that make CSAM a punishable offense across multiple jurisdictions, ensuring that offenders cannot escape accountability by exploiting legal loopholes between countries. By defining what constitutes child pornography or CSAM, including the depiction of individuals who appear to be minors. These treaties eliminate

³ Hannah Marshall, Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, Bindmans(April 24th 2018);<https://www.bindmans.com/news-insights/blogs/lanzarote-convention-on-protection-of-children-against-sexual-exploitation/>

⁴ Elena Martellozzo, Online Child Sexual Abuse:Grooming Policing and Child Protection in a Multi-Media World, Sage Journals, Vol.15 Issue 8, Elena Martellozzo, Online Child Sexual Abuse: Grooming, Policing and Child Protection in a Multi-Media World - Daniel Nehring, 2012

ambiguity and strengthen enforcement. Importantly, they also address technology-driven crimes to acknowledge the evolving nature of exploitation in the digital era.

III. INDIA'S COMMITMENT

According to the NCRB⁵ statistics, 1 62,449 cases of child abuse were recorded in India in 2022. This translates to seven children every hour reporting an offence. While global conventions establish universal principles for child protection, India has built a strong national legal framework to address and prevent child sexual abuse and exploitation. The cornerstone of this effort is the Protection of Children from Sexual Offences Act, 2012, which provides a comprehensive legal structure for safeguarding children from all forms of sexual offences, ranging from harassment and assault to the use of children in pornographic content. Complementing POCSO, the Information Technology Act, 2000, criminalizes the publication, transmission, and storage of child sexual abuse material (CSAM) in electronic forms, addressing the digital dimensions of exploitation⁶.

Bharatiya Nyaya Sanhita 2023 – The Bharatiya Nyaya Sanhita marks a significant step in combating crimes against children, specifically those that utilize technology as a weapon, recognizing how rapidly cybercrime has aggravated in recent years. The need to tackle online abuse has been recognized in *Shreya Singhal v. Union of India* (2015)⁷, the Supreme Court highlighted the importance of protecting individuals from digital harm while upholding constitutional rights.

Section 95 of the act widens the scope of sexual crimes to include child pornography as well. The act takes a strong stand against online exploitation of children by explicitly including child pornography in its 'explanation' clause, which clearly states that using a child for sexual exploitation or for the purpose of creating pornography is a serious offence⁸. The law treats this kind of abuse as a serious threat to a child, as the child is being used for sexual content that they cannot understand or consent to. Crimes such as online grooming, circulation or creation of child sexual abuse material (CSAM), digital harassment, and exploitation on social media or messaging platforms now fall squarely within the definition of punishable sexual offences.

The Protection of Children from Sexual Offences Act (POCSO)⁹ – The POCSO Act, 2012

⁵ End Child Sexual Abuse, INDIAN CHILD PROTECTION (2024)<https://www.childprotection.org.in/end-child-sexual-abuse/>

⁶ Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, at ¶98 (India)

⁸ Bharatiya Nyaya Sanhita, 2025, § 95

⁹ Ritika Sharma, Protection of Childrean from Sexual Offences Act (POCSO) 2012, IPLEADERS (November 10th 2024) <https://blog.ipleaders.in/pocso-act-everything-you-need-to-know/>

serves as India's primary law for protecting children from sexual abuse, including offences committed online. It recognizes the growing risk children face in the online world, such as online grooming, child pornography, and exploitation through social media or gaming platforms. POCSO criminalizes all forms of technology-enabled sexual exploitation of children, including the creation, sharing, or possession of any material related to child sexual abuse (CSAM).

Upholding the child-centric image of the POCSO Act, the Supreme Court in *Sampurna Behura v. Union of India*¹⁰ (2018) prohibited electronic media from publishing or broadcasting the image of minor girls, even in morphed or blurred form. This ruling reinforced the principle that a child's privacy and dignity must remain fully protected in all circumstances.

The Act also prioritizes the child's dignity and safety through measures like in-camera trials and child-friendly procedures, reducing trauma during legal proceedings. In cyber-related offences, POCSO operates alongside the Information Technology Act 2000, creating a comprehensive framework to protect minors in the digital environment. It further places responsibility on digital platforms and intermediaries to prevent the circulation of abusive content and comply with child-protection obligations.

The Information Technology (IT) Act 2000 – India's key legislation for combating cyber-crimes against children is the IT Act 2000. Before 2008, India had no dedicated law addressing child pornography. This changed with the amendment to the Information Technology Act, in 2008; which introduced section 67B, which makes it a criminal offence to publish, share, transmit, or even possess child sexual abuse material (CSAM) in any electronic form¹¹. Another important section, section 69, permits the government, subject to specific safeguards, to intercept or monitor digital data when required to investigate serious crimes, including child exploitation.

IV. A COMPARATIVE ANALYSIS: UNITED STATES OF AMERICA, CANADA & AUSTRALIA

The true severity of this crime can be understood through an analogy: if cybercrime were considered a nation, its estimated global impact of USD 6 trillion in losses in 2021 would make it the third-largest economy in the world, behind only the United States and China. Forecasts

¹⁰ *Sampurna Behura v. Union of India & Ors.*, Writ Petition (C) No. 473 of 2005, [2018] 2 S.C.R. 940 (India)

¹¹ Daniel Manoj, Ranjit Immanuel James, Senthil Kumaran, Gerard Pradeep Devnath, Benjy Tom Varughese, Antony L. Arakkal, Latif Rajesh Johnson, Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation, *Child Protection and Practice*, Vol.4, 2025, <https://www.sciencedirect.com/science/article/pii/S2950193824000883>

indicate an even more alarming trajectory: global cybercrime damages are expected to rise by 15% annually, reaching USD 10.5 trillion by the end of this financial year, compared to USD 3 trillion in 2015, making a staggering surge within just a decade¹².

In this global landscape, crimes related to child sexual abuse material (CSAM) form one of the fastest-growing and most harmful categories. As the digital platforms expand, the threat to the security of children also increases, as the offenders have numerous opportunities to attack these young and innocent minds. This vulnerability affecting children is global; it transcends the borders of a nation, where every child, regardless of nationality, is in the epicenter of these heinous offences against them. No nation can combat these crimes in isolation; such threats demand a united, global approach.

Hence, this research aims to examine how legal frameworks, both national as well as international, tackle such technology-driven child sexual exploitation. A comparative analysis not only reveals the strengths and gaps within each system but also underscores the need for harmonized global action to protect children in an increasingly digital world.

Countries such as the United States¹³, Australia, and Canada have developed advanced frameworks that combine strong legislation, institutional support mechanism, and mandatory reporting systems. India, through its Protection of Children from Sexual Offences Act (POCSO) Act, the Information Technology (IT) Act, the Bharatiya Nyaya Sanhita (BNS) 2023, has also established a comprehensive legal foundation. However, comparative analysis reveals differences in scope, implementation, digital preparedness, and victim support systems that shed light on strengths and gaps within the Indian framework.

- Definition & Scope –

In the United States¹⁴, federal and state laws clearly criminalize the production, possession, distribution, and online solicitation of minors, offering comprehensive definitions that extend to both digital and non-digital forms of exploitation. Australia's criminal code goes even further by covering modern abuse methods such as live-streamed exploitation, online grooming, and child sex tourism, demonstrating a forward-looking legal approach¹⁵. Similarly, Canada's

¹² Sausalito & Calif, Cybercrime to Cost the World \$10.5 Trillion Annually by 2025, CYBERCRIME MAGZINE (November 13th 2020), <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

¹³ NCMEC The Report Act

¹⁴ Dr. Puspanjali Mallick, Comparative analysis of the POCSO Act with International child protection laws: Lessons and Suggestions, IJPSG, Vol. 6 Issue 2, Pg.no. 249 <https://www.journalofpoliticalscience.com/uploads/archives/6-2-63-543.pdf>

¹⁵ Nina Kerwin, Australia: Phase 2 Online Safety Codes registered by e Safety Commissioner ,BAKER MCKENZIE, (September 26th 2025), <https://insightplus.bakermckenzie.com/bm/data-technology/australia-phase-2-online-safety-codes-registered-by-esafety-commissioner>

Criminal Code explicitly includes accessing, viewing, transmitting, or facilitating access to online child pornography.

India's framework, primarily through the POCSO Act (2012), section 67B of the IT Act, and the Bharatiya Nyaya Sanhita 2023, provides a detailed definition of sexual assault, harassment, and exploitation. These laws criminalize the creation, storage, and transmission of CSAM, aligning India with International norms. However, unlike Australia or Canada, India still lacks explicit statutory coverage of newer digital harms such as livestreamed abuse and persistent online grooming.

- Investigative Framework and Enforcement Mechanism –

International investigative frameworks offer integrated, technologically advanced approaches to handling child abuse cases. The United States pioneered the Children's Advocacy Centers (CACs)¹⁶, which operate as single-window systems providing forensic interviews, medical examinations, counselling, and coordinated law-enforcement involvement, minimizing trauma to the child. Additionally, the AMBER alert system ensures a rapid, nationwide response to missing children. Australia's investigative mechanisms are equally advanced, with strong digital enforcement tools and mandatory content takedown obligations under the Online Safety Act¹⁷. Canada's special cybercrime units employ sophisticated digital forensics, enabling swift trafficking of offenders and dismantling of online networks.

In India, cybercrime cells and POCSO special courts form the backbone of the investigative system. While these institutions represent meaningful progress, their effectiveness varies across states due to infrastructure gaps, limited digital forensic capabilities, and the absence of a unified, CAC-like support model.

- Victim Protection and Courtroom Procedures-

Victim-centered procedures vary notably across jurisdictions. Canada stands out for its extensive use of testimony aids, including video deposition, screens, and the allowance of second persons, ensuring a less intimidating environment for child witnesses. The United States integrates victim protection through CAC operations, which ensures that forensic interviews and therapeutic interventions occur in a child-friendly setting. Australia has strengthened

¹⁶ Children's Advocacy Centers Literature Review: A product of the Model Programs Guide, OJJDP (march 2025), <https://ojjdp.ojp.gov/model-programs-guide/literature-reviews/childrens-advocacy-centers>

¹⁷ Current Legislation, Australian Government- Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts, <https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation>

institutional accountability through reforms initiated by the Royal Commission into institutional responses to Child Sexual Abuse.

India's POCSO Act mandates in-camera trials, child-friendly courtrooms, and strict confidentiality regarding the child's identity. While the law is progressive, disparities in infrastructure, training, and courtroom sensitivity undermine consistent implementation nationwide.

- Digital Platform's Responsibility –

The regulation of digital platforms forms a crucial aspect of combating online child exploitation. Australia maintains the world's strictest regime, compelling the websites to rapidly remove the CSAM and comply with proactive safety measures under the Online Safety Act. In the United States, federal law obligates platforms to report suspected CSAM to the Center for Missing and Exploited Children (NCMEC), creating a robust reporting system. Canada similarly mandates ISPs and digital providers to report and preserve evidence of CSAM activity.

India's Intermediaries Rules 2021, issued by the Government of India, under the IT Act 2000, significantly reshape the framework for intermediary liability in India. It requires digital platforms to promptly remove and report CSAM to law enforcement agencies. Despite this framework, enforcement remains inconsistent due to limited monitoring mechanisms and technological gaps.

- Penalties & Sentencing –

Penalties for offences involving Child Sexual Abuse Material (CSAM) are stringent across leading international jurisdictions. In the United States, federal and state laws impose lengthy prison terms for CSAM production, distribution, possession, and online grooming. Additionally, the US mandates lifetime registration of sexual offenders, ensuring continuous monitoring of individuals even after they have served their sentence¹⁸. This long-term surveillance acts as a deterrent and helps prevent repeat offences. Australia and Canada similarly enforce severe punishments for CSAM-related crimes, including extended imprisonment, mandatory reporting obligations, and restrictions on offender movement or online activity. These countries also supplement penal consequences with a structured post-release monitoring system to reduce recidivism.

¹⁸ Citizen's Guide to U.S. Federal Law on Child Exploitation Laws , Criminal Division U.S.Department of Justice(August 11th 2023)<https://www.justice.gov/criminal/criminal-ceos/citizens-guide-us-federal-law-child-pornography>

In contrast, India's POCSO Act and the Bharatiya Nyaya Sanhita (BNS) prescribe strong punitive measures, including rigorous imprisonment and life sentences for aggravated forms of child sexual abuse. However, India currently lacks a national sex-offenders registry, whether public or law enforcement exclusive, limiting its ability to track offenders after their release. This gap constrains long-term preventive strategies and surveillance mechanisms. India's legal penalties are robust and largely aligned with global standards. Yet, international systems demonstrate the additional preventive value of sex-offenders registries.

V. CONCLUSION & SUGGESTIONS

A comparative analysis of global child protection laws shows that India has developed a strong statutory framework to combat child sexual abuse, particularly through the POCSO Act, the Information Technology Act, and the Bharatiya Nyaya Sanhita 2023. These laws reflect international norms in defining offences, prescribing strict penalties, and promoting child-friendly judicial processes.

However, when compared with jurisdictions such as the United States, Australia, and Canada, important gaps emerge in India's institutional mechanisms. These countries illustrate the effectiveness of:

1. Integrated, multidisciplinary investigative centers,
2. Advanced digital forensic infrastructure,
3. Strict compliance mechanism for digital platforms, and
4. Long-term offender monitoring systems, including sex offender registries.

Such systems strengthen preventive capacities and ensure quicker, more coordinated responses to child sexual exploitation. A significant limitation in India's fight against technology-enabled child sexual abuse is that it is not a signatory to prominent conventions such as:

1. The Budapest Convention on Cybercrime, and
2. The Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

These conventions establish global standards for cross-border cooperation, information-sharing, and coordinated action against online sexual exploitation. India's non-participation restricts access to established international networks, delays evidence sharing in transnational cases, and limits collaboration with countries that play a central role in combating online CSAM. This becomes particularly critical as most CSAM offences involve cross-border

servers, foreign platforms, encrypted networks, and international offender groups.

Suggestions:

To build a more resilient and future-ready system, India may consider adopting global practices, enhancing technological capacity, improving inter-agency coordination, and ensuring long-term, sustainable mechanisms for safeguarding children from evolving forms of sexual exploitation. Based on the above observations, this research attempts to suggest the key measures to strengthen India's child-centered protection framework.

1. India must strengthen its cyber laws by aligning them with global standards. Additionally, it should also come forward and contribute to the international fight against online offences against children by becoming a signatory to the Relevant International Conventions.
2. We should also have Child Advocacy Centers nationwide to ensure that every district has a safe space where children can obtain forensic, medical, psychological, and legal support in a harmonized manner.
3. Like the U.S., our legal framework needs a secure and constitutionally sound system for monitoring sex offenders, which allows long-term tracking of potential sex offenders, but respects their legal and fundamental rights.
4. Considering the importance and proliferation of AI, our country should invest in a strong digital forensic system that would help detect CSAM, and should also have systems that could target the dark web as well.
5. Ensure consistent nationwide implementation of POCSO courts, child-friendly procedures, and rapid-reporting mechanisms.
6. Our country should also actively invest in the awareness campaigns against the various threats of the internet, especially offences against children, because an informed society is the first line of defense against child sexual exploitation.
7. Protecting children is not merely a legal obligation; it is a moral duty that defines the conscience of a nation. As technology evolves, so does a threat, but so does our capacity to respond with compassion, vigilance, and collective responsibility. Strengthening India's laws, institutions, and international cooperation is not just about compliance; it is about ensuring that every child grows up with dignity, safety, and the freedom to dream without fear.
