Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

Digital Safety and Child Protection: Reassessing the POCSO Act, 2012 in light of Online Abuse

Bhupinder
Research Scholar
Sushant University (School of Law)
apbk789@gmail.com

Prof. (Dr.) Priya A Sondhi
Sushant University (School of Law)
Priyasondhi03@gmail.com

Dr. Deepak Miglani
Associate Professor
Sushant University (School of Law)
miglani786@gmail.com

Abstract:

Globally, children's experiences have been significantly transformed by the introduction of digital technologies. Children in today's world have limitless access to education, creativity, and international communication through online and digital means, since they are growing up surrounded by smartphones, social media, and online content. Beyond geographical boundaries, digital platforms offer chances for self-expression, education, and interaction. But there are also complicated concerns associated with these technical advancements. Threats to children nowadays include cyberbullying, online grooming, and the extensive dissemination of content involving child sexual abuse, which is made worse by the anonymity and accessibility of the internet. Because of their scope and global reach, these online threats are frequently more challenging to identify, track, and prosecute than more traditional kinds of abuse. The question of whether current legislative frameworks adequately protect children in so a rapidly evolving digital environment thus becomes essential. In our technologically advanced society, achieving a balance between the benefits of digital access and effective, child-focused safeguards has become an important issue.

This study thoroughly explores the Protection of Children from Sexual Offences (POCSO) Act, 2012 which was first passed with an emphasis on traditional forms of abuse and is the main

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

piece of legislation in India intended to protect children from sexual offences. The Act now has to deal with crimes that are being committed more frequently online. This paper assesses whether India's legal system is sufficiently strong to address challenges to children's rights aided by technology through a critical analysis. It evaluates the POCSO Act's scope, strengths as well as limitations in light of emerging digital world and emphasises the need for changes that take into account the complexities of online abuse. In order to ensure that children's rights and well-being are truly protected in a world driven by technology, the study concludes by recommending a comprehensive policy response that includes legal updates, enhanced enforcement, digital literacy initiatives, and improved cooperation among the public, private, and civil society sectors.

Keywords:

Child Rights, Digital Safety, POCSO Act, Online Abuse, Child-focused safeguards

1. Introduction

In the digital age, the context of children's rights has undergone significant evolution, presenting both opportunities and challenges. With the rapid expansion of internet access, smartphones, and social media platforms, children are increasingly engaging with digital technologies for education, communication, and entertainment. While this digital engagement promotes access to information and learning, it also exposes children to various risks such as cyberbullying, online grooming, exposure to harmful content, invasion of privacy, and digital exploitation. The United Nations Convention on the Rights of the Child (UNCRC) affirms that children’s rights, including the right to protection, participation, privacy, and access to information, must be upheld in all settings, including digital environments. As children become active participants in the online world, states, societies, and institutions have an urgent responsibility to ensure that digital platforms are safe, inclusive, and respectful of children’s dignity and developmental needs. This growing intersection of technology and child rights necessitates robust legal frameworks, ethical digital governance, and increased awareness to safeguard children’s well-being in the virtual sphere.

The United Nations Convention on the Rights of the Child (UNCRC) establishes comprehensive rights for children, including to privacy, freedom of expression, protection from harm, access to information, and participation in decisions affecting them, which uniformly

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

apply both offline and online.[1] Digital technology, from the internet and smartphones to artificial intelligence, has fundamentally changed childhood experiences.[2] Today, roughly one in three internet users globally is a child.[3] Digital connectivity shapes how children learn, play, communicate, and engage with society on an unprecedented scale.[4] The digital environment brings significant benefits such as increased access to educational resources, opportunities for self-expression, social connections, and even participation in civic life.[5] However, these gains coexist with a new spectrum of risks, including cyberbullying, online grooming, exposure to harmful content, manipulation of personal data, surveillance, and technology-facilitated sexual exploitation.

The UNCRC's General Comment No. 25 (2021) explicitly articulates how children's rights must be realised in the digital environment, emphasising that all rights under the Convention apply fully online.[6] This means that, as children navigate digital spaces, their rights to non-discrimination, best interests, life, development, and being heard must be respected just as in the physical world.[7] Governments have a duty not only to ensure safe and age-appropriate digital spaces by enforcing privacy, safety, and security by design, but also to bridge the digital divide and enable the full participation of all children, regardless of background or ability.[8] A rights-based approach is essential: children's digital rights should not be sacrificed for security, nor should access be restricted such that children are excluded from the benefits of technology.[9] Instead, children need digital literacy and empowerment, robust protection from exploitation

[1] United Nations Convention on the Rights of the Child. March 02, 2021. General comment No. 25 (2021) on children's rights in relation to the digital environment. UNICEF. https://www.unicef.org/bulgaria/en/media/10596/file

[2] OECD. (2025). How's Life for Children in the Digital Age?. https://www.oecd.org/en/publications/2025/05/how-s-life-for-children-in-the-digital-age_c4a22655.html

[3] Eurochild. (2025). The rights of children in the digital environment. https://eurochild.org/resource/the-rights-of-children-in-the-digital-environment/

[4] Ibid 2

[5] DigWatch. (n.d.). Children Rights. https://dig.watch/topics/childrens-rights

[6] eSafety Commissioner. (2021). UNCRC General Comment: Children's rights in the digital world. https://www.esafety.gov.au/newsroom/blogs/uncrc-general-comment-childrens-rights-in-the-digital-world#:~:text=eSafety's%20work%20is%20heavily%20influenced,abuse%20material%20from%20the%20internet.

[7] Office of the High Commissioner for Human Rights. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[8] Child Rights Connect et al. (2023). Overarching Principles for the Global Digital Compact. https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_Child_Rights_Connect_Taskforce.pdf

[9] Eurochild. (2025). The rights of children in the digital environment. https://eurochild.org/resource/the-rights-of-children-in-the-digital-environment/

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

and abuse, and meaningful opportunities to participate in shaping the online world.[10] These responsibilities extend to states, businesses, families, and communities, all of whom must work collaboratively to ensure digital environments promote children's well-being, development, and agency in consonance with global child rights standards.[11]

2. Opportunities and Risks to Children's Rights in the Digital Era

Children's rights are fundamentally protected and recognised under both the Indian Constitution and international legal instruments, forming a robust framework that guides child protection policies and laws, including digital safety.[12] Under the Indian Constitution, several provisions explicitly safeguard children's rights. Article 15(3) allows the state to make special provisions for children[13], Article 21 guarantees the right to life and personal liberty, which has been judicially interpreted to include the right to a safe and healthy environment[14]. Article 24 prohibits child labour and exploitation.[15] Article 21A ensures the right to free and compulsory education for children aged 6 to 14 years.[16] Collectively, these constitutional articles guarantee the establishment of children's right to survival, development, education, and protection from exploitation and abuse. At the international level, the cornerstone is the United Nations Convention on the Rights of the Child (UNCRC), ratified by India in 1992.[17] The UNCRC enshrines a comprehensive set of rights, including survival, development, protection, and participation rights. Crucially, General Comment No. 25 (2021) by the UN Committee on the Rights of the Child extends these rights explicitly into the digital environment[18], underscoring that all protections and freedoms applicable offline equally apply online. This includes the

[10] Office of the High Commissioner for Human Rights. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.
[11] Child Rights International Network. (2019). Briefing: Children's rights in the digital age. https://home.crin.org/issues/digital-rights/childrens-right-digital-age#:~:text=Maximise%20children's%20enjoyment%20of%20all,what%20to%20do%20about%20them.
[12] Child Rights International Network. (2019). *Briefing: Children's rights in the digital age*. https://home.crin.org/issues/digital-rights/childrens-right-digital-age#:~:text=Maximise%20children's%20enjoyment%20of%20all,what%20to%20do%20about%20them.
[13] The Constitution of India, Article 15(3).
[14] M.C. Mehta v. State of Tamil Nadu, AIR 1997 SC 699.
[15] The Constitution of India, Article 24.
[16] The Constitution of India, Article 21A.
[17] United Nations Treaty Series. (1992). *Convention on the Rights of the Child – India Ratification*.
[18] UN Committee on the Rights of the Child. (2021). *General Comment No. 25 on children's rights in relation to the digital environment*.

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

rights to privacy, freedom of expression, protection from exploitation, and the right to have one's best interests prioritised in decisions affecting children in digital spaces.[19]

Technological advancements have significantly improved children's education, access to information, and participation in local and global communities. Digital tools have enabled individualised instruction through e-learning platforms, interactive applications, and virtual classrooms. These innovations bridge geographic barriers and provide inclusive literacy and skill development for children in rural or marginalised communities. Technology also provides access to vast information reservoirs, enabling children to explore subjects, nurture curiosity, and develop critical thinking.[20] Accessible information supports children's rights to discover, seek, and receive knowledge, as recognised by international standards like the Convention on the Rights of the Child. Digital platforms like social media, age-appropriate forums, and online communities enable children to interact, share opinions, and contribute to societal discourse, encouraging them to consume information, generate content, and participate in decision-making processes.[21] For vulnerable and marginalised groups, technology can facilitate social inclusion by breaking down physical and social barriers, allowing voices that might otherwise remain unheard in traditional settings to be amplified and represented.

Children are one of the vulnerable sections of our society that exacerbate their risk of harm when they are online. Due to their developmental stages and relative lack of experience, children are more susceptible to manipulation, exploitation, and privacy violations within digital environments.[22] Risks include exposure to cyberbullying, online grooming, trafficking, sextortion, and access to harmful or inappropriate content, all facilitated by the anonymity and reach of the internet. Moreover, marginalised groups such as children with disabilities, gender minorities, or economically disadvantaged children face increased vulnerabilities due to

[19] eSafety Commissioner. (2021). UNCRC General Comment: Children's rights in the digital world. https://www.esafety.gov.au/newsroom/blogs/uncrc-general-comment-childrens-rights-in-the-digital-world#:~:text=eSafety's%20work%20is%20heavily%20influenced,abuse%20material%20from%20the%20internet.

[20] OECD. (2025). How's Life for Children in the Digital Age?. https://www.oecd.org/en/publications/2025/05/how-s-life-for-children-in-the-digital-age_c4a22655.html

[21] UN Committee on the Rights of the Child. (2021). *General Comment No. 25 on children's rights in relation to the digital environment*.

[22] Livingstone, S., & Third, A. (2017). *Children and young people's rights in the digital age*. New Media & Society, 19(5), 657–670.

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

limited digital literacy, lack of access to protective resources, and discrimination.[23] The intersection of childhood dependency and the pervasive reach of technology necessitates tailored legal protections and supportive measures to ensure their rights and well-being are upheld comprehensively in the digital world. This framework demands that states and stakeholders prioritise children's rights in all digital governance, ensuring safe, inclusive, and empowering online environments for children consistent with constitutional mandates and international standards.

3. Kinds of risks and harms in Digital Spaces

In the context of safeguarding children's rights in digital spaces under the Protection of Children from Sexual Offences (POCSO) Act, 2012, it is critical to recognise the diverse spectrum of online risks and harms amplified by technological advances. Cyberbullying involves persistent targeting of children online, resulting in psychological distress, reduced self-esteem, and, in extreme cases, self-harm[24]. The anonymity and reach of digital platforms exacerbate the intensity of such abuse.

Online grooming involves using technology or the internet to establish relationships with minors, with the intent of deceiving them into participating in sexual activity. This can involve pretending to be another individual, or even assuming a separate identity and establishing trust.[25] The POCSO Act criminalises such acts. However, due to encrypted content and non-jurisdiction of online activities, the offenders often escape.

Trafficking has also evolved digitally. Human traffickers use various internet platforms, such as social media and online marketplace sites, to recruit victims and attract clients, either actively hunting vulnerable individuals or passively fishing for potential victims through advertisements.[26]

[23] Eurochild. (2025). The rights of children in the digital environment. https://eurochild.org/resource/the-rights-of-children-in-the-digital-environment/

[24] OECD. (2025). How's Life for Children in the Digital Age?. https://www.oecd.org/en/publications/2025/05/how-s-life-for-children-in-the-digital-age_c4a22655.html

[25] CEOP. (n.d.). Online grooming. https://www.ceopeducation.co.uk/11_18/lets-talk-about/sexual-abuse/online-grooming/

[26] United Nations. (n.d.). Technology and Human Trafficking: Avoid the Trap!. https://www.unodc.org/unodc/en/endht/2022/internet-safety-tips.html

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

Generative AI technologies are being used to produce *child sexual abuse material (CSAM),* which includes images, videos, or synthetic depictions of abuse, which remains one of the gravest threats, allowing for fantasy, extortion, and peer-based bullying. Although still in its early stages, these AI models are being manipulated to create material of historical survivors and specific kids, enabling abuse and manipulation of children in schools and communities.[27] Section 13 of the POCSO Act penalises the use of children for pornographic purposes, but the rapid production and circulation of CSAM online through AI tools often outpace law enforcement capacity.

Sextortion takes place when perpetrators manipulate or deceive their victims into disclosing explicit photographs or films, which are then used for extortion. A significant increase in sextortion reports has been noted globally in recent years.[28] This digital crime calls for applying and interpreting POCSO provisions in ways that address coercion conducted entirely in virtual spaces.

Privacy violations, including the unauthorised sharing of a child's personal details, images, or location, constitute serious risks. Gaps in India's broader data protection regime leave children's online privacy insufficiently safeguarded. The challenges to children's privacy are dynamic, growing with prevailing technology and emerging circumstances.[29]

Emerging AI-based abuses, such as deepfake CSAM, represent a new legal frontier. These synthetic materials can be created without the child's awareness or physical presence, yet can cause real, ongoing harm. POCSO's current language does not specifically address synthetic or manipulated depictions, underscoring the need for legislative updates.[30]

Children from low-income backgrounds, rural areas, those with disabilities, gender or sexual minority youth, and those lacking digital literacy (*Marginalised groups)* are disproportionately

[27] Thorn. (n.d.). Child sexual abuse material (CSAM). https://www.thorn.org/research/child-sexual-abuse-material-csam/#:~:text=Regardless%20of%20how%20these%20materials,to%20groom%20other%20potential%20victims.

[28] Interpol. (2022, September 5). Asia: Sextortion ring dismantled by police. https://www.interpol.int/en/News-and-Events/News/2022/Asia-Sextortion-ring-dismantled-by-police

[29] Goyal, T. Safeguarding Children's Informational Privacy in India: An Assessment of the Framework under the PDP Bill, 2019. *Vidhi Centre for Legal Policy.* P, 1-84

[30] UN Office of the High Commissioner for Human Rights. (2021, March 02). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

exposed to these risks. Socioeconomic vulnerability, stigma, and limited access to legal or psychosocial support hinder reporting and justice.[31] Strengthening POCSO's implementation must therefore go hand-in-hand with targeted outreach, capacity building, and inclusive digital literacy initiatives.

4. The Protection of Children from Sexual Offences (POCSO) Act, 2012

India's legal framework for safeguarding children online is primarily governed by the Protection of Children from Sexual Offences (POCSO) Act, 2012. This law provides a comprehensive structure to combat various forms of child sexual abuse, including those enabled by technology. It defines crimes such as child pornography, sexual harassment, and online grooming, and establishes specific procedures for reporting, investigating, and prosecuting these offences. Importantly, sections 13 to 15 of POCSO criminalise using children for pornographic purposes, whether through traditional or electronic media.[32]

Salient Provisions Relevant to Digital Offences under the POCSO Act

1. Section 13 *(Use of Children for Pornographic Purposes)* criminalises using a child for producing or distributing sexually explicit material, including images, videos, or other digital content. It explicitly applies to material in electronic form as well as traditional media, covering offences via computers, smartphones, and internet platforms.
2. Sections 14 & 15 (*Punishments for CSAM-related Offences)* prescribe enhanced penalties when CSAM is created, distributed, or used for commercial purposes and penalise possession or browsing of CSAM with intent, even without production or distribution, respectively.
3. Section 11 *(Sexual Harassment via Technology)* includes digital acts such as indecent messages, online stalking, coercion, and harassment through electronic communication and recognises online grooming and exploitation via social media, messaging platforms, and online games.

[31] Eurochild. (2025). The rights of children in the digital environment. https://eurochild.org/resource/the-rights-of-children-in-the-digital-environment/
[32] Section 13 & 15 of the POCSO Act, 2012

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

4. Section 19 *(Mandatory Reporting Obligations)* requires any person with knowledge or suspicion of an offence to report it immediately. Non-reporting of which is a punishable offence, ensuring accountability and cooperation from intermediaries and the public.

5. Information Technology (IT) Act, 2000,

The Information Technology (IT) Act of 2000 contains provisions that specifically address online child abuse, particularly in relation to child sexual abuse material (CSAM), even though its primary objectives are to legalise electronic transactions and prevent cybercrimes. Besides POCSO, this act supplements protections by criminalising the publication, transmission, and browsing of child sexual abuse material online.[33]

1. *Section 66 E*- It deals with the capturing, publishing, or transmitting of private images of any person without consent. It is relevant in cases where children's private images are misused online.
2. *Section 67*- This section prescribes punishment for the publication, transmission, or causing of transmission of obscene material in electronic form. The offence covers any electronic content that is lascivious, appeals to the prurient interest, or tends to deprave and corrupt individuals exposed to it. This section forms the general legal basis for curbing obscenity online. The punishment for first conviction is 3 years imprisonment and a fine of up to five lakh rupees. While subsequent convictions can lead to up to five years imprisonment and a fine of up to ten lakh rupees.
3. *Section 67A*- It criminalises the electronic publication or transmission of sexually explicit material, addressing the more aggravated form of obscenity. For the first offence, imprisonment up to five years and a fine of ten lakh rupees is prescribed, while repeat offenders may face up to seven years of imprisonment and a similar fine. This section reflects the legislature's intent to impose enhanced responsibility in regulating sexually explicit digital content.
4. *Section 67B*- It criminalises the publishing, transmitting, browsing, collecting, or advertising of material depicting children in sexually explicit acts. It not only penalises those who directly disseminate child sexual abuse material (CSAM) but also those who merely seek or download such content, thereby addressing both supply and demand

[33] Section 67(B) of the Information Technology Act, 2000

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

aspects of online abuse. The punishment under this section ranges from five years of imprisonment and a fine of up to ten lakh rupees for the first conviction, extending to seven years for subsequent offences. It applies to online platforms such as social media and other digital platforms. It complements the POCSO Act by addressing intermediary liability and digital evidence.

6. Digital Personal Data Protection Act, 2023

Recent legislative developments, such as the Digital Personal Data Protection Act, 2023, seek to further provide privacy safeguards for children. The Act regulates the processing of digital personal data, acknowledging individuals' rights to safeguard their personal information while permitting the processing of such data for legitimate reasons and related matters.[34] Yet implementation gaps persist in ensuring the safe handling and protection of children's digital footprints.[35]

This act mandates explicit parental consent for collecting and processing personal data of children under 18. It is necessary to process a child's personal data, and explicitly prohibits processing that may impair a child's well-being, including behavioural tracking, profiling, and targeted advertising. It prohibits tracking, targeting, and profiling of children online. It encourages child-safety-by-design in digital platforms and aims to reduce online exploitation risks, identity theft, and privacy violations.[36] Although the Act was approved on August 11, 2023, it remains non-operational until the final rules, including those outlining mechanisms for gaining verifiable parental consent.[37]

7. Critical Appraisal: Effectiveness of the POCSO Act in Digital Spaces

The Protection of Children from Sexual Offences (POCSO) Act plays a crucial role in safeguarding children from sexual abuse, including in digital spaces where technology has

[34] Vikaspedia. (2025, February 27). Digital Personal Data Protection Act, 2023. https://en.vikaspedia.in/viewcontent/e-governance/digital-india/digital-personal-data-protection-act-2023

[35] Express Computer. (2025, July 4). Enforcement Gaps in India's DPDP Act and the case for decentralized data protection boards. https://www.expresscomputer.in/guest-blogs/enforcement-gaps-in-indias-dpdp-act-and-the-case-for-decentralized-data-protection-boards/126140/

[36] Section 9 of the Digital Personal Data Protection Act, 2023

[37] Suraksha, P. (2025, August 11). India's long wait for data protection law. *The Economic Times.* https://economictimes.indiatimes.com/tech/technology/indias-long-wait-for-data-protection-law/articleshow/123223043.cms

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

created new avenues for exploitation and harm. While the Act provides a broad legislative framework criminalising online sexual offences such as grooming, child pornography, child sexual abuse material (CSAM), and harassment, its effectiveness in the rapidly evolving digital environment is mixed and requires ongoing evaluation. The Act mandates mandatory reporting of suspected offences and establishes child-friendly procedures to reduce victim trauma during prosecution.

Strengths of the POCSO Act

The Protection of Children from Sexual Offences (POCSO) Act, 2012, possesses several key strengths that establish it as a progressive and comprehensive legal instrument for safeguarding children's rights, including in the digital realm.

Firstly, the Act incorporates broad and inclusive definitions of sexual offences that cover a wide array of abusive acts against children, both physical and non-physical. Its clear categorisation of offences, such as penetrative sexual assault, sexual harassment, and using children for pornographic purposes, allows law enforcement and the judiciary to address diverse forms of abuse without ambiguity, including those perpetrated via digital platforms.

Secondly, the POCSO Act emphasises child-friendly processes and procedures to minimise trauma for victims. It mandates the establishment of special courts for speedy trials, provides for in-camera proceedings to protect the privacy of child victims, and requires the presence of support persons or counsellors during investigations and trials. These provisions help children participate in the justice process with dignity and reduce re-victimisation, which is critical in sensitive online abuse cases where emotional well-being is particularly vulnerable.[38]

Thirdly, the Act features explicit coverage of certain online crimes. For instance, Section 13 criminalises the use of children for pornographic purposes across all media forms, including electronic and digital platforms. Section 11 defines sexual harassment to include acts perpetrated via electronic communication, addressing behaviours such as indecent messages, online stalking, and online grooming. These provisions concretely acknowledge digital risks

[38] LegalKart. (2025, July 11). Understanding the POCSO Act, 2012: Safeguarding Children's Rights and Dignity. https://www.legalkart.com/legal-blog/understanding-the-pocso-act-2012-safeguarding-children%E2%80%99s-rights-and-dignity#:~:text=The%20Protection%20of%20Children%20from%20Sexual%20Offences%20Act%2C%202012%2C%20is,to%20unreported%20or%20unresolved%20cases.

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

and ensure that offences committed via the internet and digital devices are prosecutable under POCSO, bridging the gap between traditional protections and cyber threats.

Together, these strengths position the POCSO Act as a cornerstone of child protection in India, responding effectively to the complex realities of both offline and online sexual offences. However, the true potential of the Act depends on dynamic interpretation and responsive implementation to keep pace with evolving digital threats and technological innovations.[39]

Key gaps and challenges

The National Crime Records Bureau (NCRB) 2022 data showed that convictions in POCSO cases occurred in only 29.6% of cases. While the Protection of Children from Sexual Offences (POCSO) Act, 2012 was a landmark development in addressing child sexual abuse in India, its ability to tackle digital-age crimes remains limited. The Act was primarily drafted with traditional forms of abuse in mind and does not comprehensively cover the complexities of online offences such as cyber grooming, sextortion, child sexual abuse material (CSAM), and exploitation through social media or gaming platforms.[40] Although Sections 13–15 of the Act address the use of children in pornography, the definitions are broad and lack detailed procedural mechanisms to combat offences facilitated by evolving technologies.

A major challenge lies in the absence of clear integration between POCSO and the Information Technology Act, 2000. While the IT Act criminalises online abuse, the lack of harmonised procedures often leads to jurisdictional confusion and delays in investigation.[41] Moreover, law enforcement agencies frequently lack the technical capacity and digital forensic tools to identify, trace, and prosecute online offenders, especially in cases involving encrypted communication or cross-border servers.[42]

[39] Riya. (2025, July29). Beyond the Textbook: Understanding the POCSO Act Through Real-World Impact. Nomeansno. https://www.nomeansno.in/understanding-pocso-act-in-2025-through-real-world-impact/

[40] UNICEF. (2019). *Child Online Protection in India: A review of policies and practices*. United Nations Children's Fund. https://www.unicef.org/india/media/3401/file/Child-Online-Protection-in-India.pdf

[41] Internet and Mobile Association of India (IAMAI) & Nishith Desai Associates. (2018). *Internet Intermediary Liability in India*. https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Internet_Intermediary_Liability.pdf

[42] Human Rights Watch. (2017). *India: Broken System Fails Abused Children*. https://www.hrw.org/report/2017/02/07/broken-system/failures-indias-child-protection

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

Additionally, there is a paucity of child-specific cyber awareness programs, and many children and parents are unaware of the legal remedies available under POCSO and allied laws.[43] The Act also lacks explicit provisions for the mandatory takedown of online abusive content or mechanisms for collaboration with social media intermediaries, which are critical for timely redressal.[44] As digital spaces become more integral to children's lives, updating the POCSO framework to address technology-facilitated abuse is both urgent and essential for comprehensive child protection.[45]

Implementation Challenges:

1. Underreporting of cases remains a pronounced barrier, attributed to stigma, lack of awareness, and social pressures facing victims and families.[46]
2. Judicial delays result from overburdened courts, insufficient infrastructure, and lack of specialised training for law enforcement and the judiciary, causing extended trauma for victims and undermining deterrence.[47]
3. Inadequate protection mechanisms mean child victims and witnesses may encounter intimidation or harassment, further hindering justice delivery.[48]

[43] Bajpai, A. (2017). *Child Rights in India: Law, Policy, and Practice* (2nd ed.). Oxford University Press.
[44] IAMAI & Nishith Desai Associates. (2018). *Internet Intermediary Liability in India*. https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Internet_Intermediary_Liability.pdf
[45] United Nations Committee on the Rights of the Child. (2021). *General Comment No. 25 on Children's Rights in Relation to the Digital Environment*. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights
[46] Samantha. (n.d.). Why Children Don't Tell. Alliance for Children. https://www.allianceforchildren.org/blog/2018/08/why-children-dont-tell#:~:text=Oftentimes%20victims%20still%20care%20for,also%20make%20immediate%20disclosure%20difficult.
[47] Trivedi, P. (2025, August 11). *Delayed Justice in Rape Cases: Examining Systemic and Legal Barriers.* Chintan. https://chintan.indiafoundation.in/articles/delayed-justice-in-rape-cases-examining-systemic-and-legal-barriers/#:~:text=According%20to%20the%20National%20Crime,in%20the%20criminal%20justice%20system.&text=India%20has%20over%205%20crore,redundancies%2C%20nullifying%20their%20intended%20speed.&text=Investigations%20by%20police%20often%20lack,medical%20and%20DNA%20evidence%20submission.&text=Victims%20often%20retract%20statements%20under,of%20hostile%20witnesses%20during%20trials.
[48] United Nations Office on Drugs and Crime. (n.d.). *Justice in Matters involving Child Victims and Witnesses of Crime.* Unicef. https://www.unodc.org/documents/justice-and-prison-reform/Justice_in_matters...pdf

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

4. Technological challenges include difficulties in gathering digital evidence, lack of digital forensic expertise, and delays in investigations for cyber-enabled offences.[49]

In summary, while the POCSO Act provides a robust legal framework for prosecuting digital sexual offences against children, landmark judicial clarifications and enforcement efforts have not been matched by improvements in reporting, infrastructure, and conviction rates. Systemic reforms, training, and technological upgrades are urgently needed for the Act to deliver meaningful child protection in the digital age.

9. Differentiated Impact of online abuse on vulnerable populations

Digital sexual offences impact children unevenly, with those in rural areas, gender minorities, and children with disabilities facing distinct and heightened vulnerabilities in India's evolving digital landscape:

1) Rural Children:

Children in rural regions often have lower digital literacy, while parental awareness regarding online risks is similarly limited. These factors, combined with less internet infrastructure and cultural constraints, make detecting and reporting online child sexual exploitation challenging.[50] Many rural children are unaware of online risks such as unsolicited friend requests or risky content-sharing, leading to underreporting and delayed interventions even as smartphone penetration in these communities increases.[51] Cultural norms may also reduce girls' access to devices but increase the likelihood of punitive action if abuse is suspected.[52]

2) Gender Minorities:

Studies indicate that harassment rates in these groups can be up to four times higher than for their cisgender peers. Children identifying as transgender, non-binary,

[49] GeeksforGeeks. (2023, January 27). *Challenges in Digital Forensics*. https://www.geeksforgeeks.org/ethical-hacking/challenges-in-digital-forensics/

[50] Maji, S. & Abhiram, A.H. "Mental health cost of internet": A mixed-method study of cyberbullying among Indian sexual minorities. *Telematics and Informatics Reports*. Vol. 10. (2023).

[51] Digital Readiness of India's Youth. ASER. (2024). https://asercentre.org/wp-content/uploads/2022/12/EB_Digital-Readiness-of-Indias-Youth_11.03.2024.pdf

[52] Tiwari, A. & Aggarwal, P. (2025, January 31). Rural parents prefer private schools, but digital literacy lags. India Today. https://www.indiatoday.in/diu/story/rural-education-private-schools-digital-literacy-issues-2672701-2025-01-31

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

or LGBTQI+ often face higher exposure to cyberbullying and identity-based harassment.[53] Persistent stigma and discrimination create barriers to reporting offences and reduce access to supportive services. In addition, legal frameworks like the POCSO Act lack explicit recognition of gender-diverse children, limiting tailored protections.

3) Children with Disabilities:

Disabled children are at an increased risk of online grooming and abuse due to social isolation, dependence on caregivers, and communication barriers. These factors often limit their ability to recognise or report abuse. Research shows they face poorer mental health outcomes, reduced literacy levels, and fewer specialised support networks. Accessibility issues, both in digital safety education and reporting mechanisms, further hinder their capacity to seek justice.[54]

10. Comparative and Policy Analysis

Internationally, several countries have developed robust legal frameworks and policy initiatives to address online child sexual abuse, digital exploitation, and child safety in technology-driven environments. Comparing these with India's POCSO Act reveals areas for improvement.[55]

1) International approaches

In the European Union (EU), the EU Digital Services Act (DSA) sets stringent requirements for digital platforms to tackle illegal content, including child sexual abuse material (CSAM). The DSA mandates proactive content moderation, crisis response pathways, age-appropriate safety controls, and transparency reports for handling child abuse online.[56] Additionally, EU member states enforce the General Data Protection Regulation (GDPR), which embeds special protections for children's personal data in the digital environment. The proposed EU

[53] Kosciw, J. G., Clark, C. M. & Menard, L. (2022). The 2021 National School Climate Survey: The experiences of LGBTQ+ youth in our nation's schools. New York: GLSEN. https://www.glsen.org/sites/default/files/2022-10/NSCS-2021-Full-Report.pdf

[54] Flynn, S., Maher, R. D., & Byrne, J. Child protection and welfare risks and opportunities related to disability and internet use: Broadening current conceptualisations through critical literature review. *Children and Youth Services Review*. Vol. 157. (2024).

[55] Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation. *Child Protection and Practice.* Vol. 4. (2025).

[56] General Data Protection Regulation (EU), 2018

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

Regulation to Prevent and Combat Child Sexual Abuse will, if adopted, compel service providers to detect, report, and remove CSAM using cutting-edge technology, while ensuring privacy and fundamental rights.[57]

The United Kingdom's Online Safety Act (2023) is considered a global benchmark for balancing digital freedom with children's rights and protection. The Act imposes a 'duty of care' on online platforms, requiring companies such as social networks, gaming sites, and messaging apps to identify, mitigate, and report online harms affecting minors. It contains specific provisions to curb cyberbullying, online grooming, and exposure to harmful content, while Ofcom (the UK's digital regulator) oversees enforcement and can levy heavy penalties.[58] Notably, the UK also employs the Age-appropriate Design Code (Children's Code), which compels platforms to provide data minimisation, default privacy, and developmental safeguards tailored for children.[59]

Australia's Online Safety Act (2021) grants its eSafety Commissioner powers to investigate and require the rapid removal of CSAM, cyberbullying, and non-consensual sexual material. This legislation centralises reporting mechanisms, offers victim support, and mandates industry codes for digital platforms resulting in high regulatory compliance and prompt action against offenders and harmful content. Australia's approach includes specific features for children with disabilities and marginalised groups, promoting inclusive eSafety outreach.[60]

India's POCSO Act, while pioneering in its protection of children from sexual offences, can be updated to integrate these comparative best practices, thereby strengthening its legal, technical, and victim-support capacities in the digital era.[61]

[57] European Commission. (2022). Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209

[58] UK Government. (2023). Online Safety Act 2023. https://www.gov.uk/government/collections/online-safety-act

[59] Information Commissioner's Office. (2020). Age Appropriate Design Code (Children's Code). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[60] eSafety Commissioner Australia. (2021). Online Safety Act 2021. https://www.esafety.gov.au/newsroom/whats-on/online-safety-act

[61] Ibid 45

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

2) Role of Technology Companies

Technology companies globally are increasingly recognised as co-regulators in the space of child online protection. Under EU and UK regimes, significant intermediary liability attaches to platforms that fail to prevent, detect, or remove illegal content, including CSAM or grooming behaviour. Companies are incentivised to develop and deploy advanced AI-based monitoring, robust age-verification, default privacy, and user-reporting tools.[62]

3) Civil Society and Multi-Stakeholder Initiatives

Civil society, child protection NGOs, and academic actors play an indispensable role in both advocacy and frontline support. Internationally, initiatives such as the WePROTECT Global Alliance, ECPAT International, and the UK's Internet Watch Foundation have demonstrated the power of cross-sector coalitions combining technical expertise, research, survivor advocacy, and direct reporting mechanisms.[63] Meaningful capacity-building for educators, law enforcement, and judiciary—as seen in the Australian eSafety grants program or the EU INHOPE hotlines—raises the bar for digital safety expertise.[64]

Public-private partnerships, like the Australian Tech Council's collaboration with government for innovation in age-assurance technology, showcase how knowledge exchange and technology transfers can be streamlined.[65] Notably, civil society actors remain vital in raising digital literacy, running awareness campaigns, pushing for legislative reform, and holding government and industry to account.

11. Conclusion and suggestions

Safeguarding children's rights in digital spaces demands urgent, decisive action from lawmakers, society, and technology platforms. As online risks evolve, India's child protection framework must embrace clear, enforceable legal standards, inclusive and survivor-centric

[62] Sonia Livingstone & John Carr, "One in Three: Internet Governance and Children's Rights," 3 Global Commission on Internet Governance Paper Series 22–25 (2015).
[63] Internet Watch Foundation. IWF Annual Report 2023. https://www.iwf.org.uk/annual-report-2023/
[64] INHOPE. (n.d.). We are INHOPE. https://www.inhope.org/EN/articles/about-inhope
[65] Tech Council of Australia. (2024). *TCA statement on Online Safety Amendment (Social Media Minimum Age) Bill 2024 [Provisions]*. https://techcouncil.com.au/newsroom/tca-statement-on-online-safety-amendment-social-media-minimum-age-bill-2024-provisions/

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

support, and robust, multi-stakeholder collaboration. A holistic, dynamic, and rights-based approach adaptive to future technologies and conscious of vulnerability is essential to ensure every child experiences safety, dignity, and empowerment online. Strengthening digital literacy, regulatory enforcement, and international cooperation will not only address present threats but also build a resilient foundation for protecting children in tomorrow's technology-driven world. The rise of new technologies like encrypted messaging, AI-generated imagery, and deepfake content in India is outpacing legislative responses, causing enforcement agencies to struggle with digital evidence collection and cross-border jurisdiction issues. Despite the POCSO Act providing a strong legal foundation, ongoing reforms and capacity-building are needed to safeguard children's rights in the digital world.

Here are some suggestions to bridge the shortcomings and gaps in our legal framework and to strengthen it in order to effectively protect the children:

1) Legal reform:

The POCSO Act should be modified to clearly define technology-facilitated offences, such as digital grooming, live streaming of abuse, and artificial intelligence-generated child sexual abuse content, in order to confront the growing threats posed by the internet. To increase conviction rates and prosecutions, the Act must create improved procedures for the gathering, preserving, and sharing of digital evidence across international borders. To ensure that laws are flexible as technology develops, specific measures should be included to address new offences including deepfakes, virtual reality, artificial intelligence, and encrypted platforms.

2) Stronger regulatory mechanisms:

Stronger rules are needed to make sure that internet platforms actually follow child safety rules. This means that there should be strong reporting mechanisms for abuse, automated detection and quick removal of child sexual abuse material (CSAM), and thorough age verification methods to keep children from getting into unsafe or inappropriate online environments. Platforms must be legally responsible for failures in these areas, and there must be independent regulatory supervision and regular reports on transparency to make sure they follow the rules. These kinds of preventive steps will significantly reduce the risk of exploitation and make the digital world safer for children.

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

3) Capacity Building and Digital Literacy

To protect children online, there must be dedicated training, seminars and digital literacy programs for children, parents, educators and the concerned people. Authorities and judges need to know how to use technology to investigate and punish digital crimes. Teachers and parents need to be aware of hazards in order to spot and stop them. Children should be taught about internet safety and responsible behaviour in a way that is right for their age. In a world where the internet is evolving quickly, it is important to have a strong culture of digital literacy to keep children safe.

4) Victim-Centric and Inclusive Justice

Justice systems should emphasise child victims by making reporting processes user-friendly, confidential, and accessible to all, particularly to disadvantaged and vulnerable populations. Rehabilitation programs must provide holistic support to the victims. To remove barriers to support for disabled children, linguistic minorities, and rural people, inclusive justice requires modification of procedures. Institutional sensitivity, survivor-centric approaches, and multi-disciplinary support teams should be the norm to make every child feel secure, heard, and empowered during judicial procedures.

5) International and Cross-sectoral Collaboration

Governments should cooperate across borders to quickly share evidence, intelligence and best practices. They can do this through mutual legal aid treaties and cooperative investigation frameworks. Working with IT businesses, NGOs, and schools can help create capacity, find technical solutions, and raise public awareness. To fight transnational risks like cyber trafficking and CSAM, countries need to work together to curb this problem.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 3
December 2025
Impact Factor: 11.9
Subject: Law

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Bhupinder
Prof. (Dr.) Priya A Sondhi
Dr. Deepak Miglani

******