
UNVEILING CHALLENGES IN VICTIM IDENTITY PROTECTION FOR CHILD PORNOGRAPHY AMID DIGITAL EXPLORATION

Pishati Pranava, Alliance University

ABSTRACT

The problem of child sexual abuse is a global problem and present throughout the world. A child is immature, weak, and dependent on others¹. The POCSO Act was enacted in response to the need for laws that specifically addressed sexual offences against children. The heinous crime of child pornography is one of several types of sexual abuse recognised by the POCSO Act of 2012. Section 14 of the Act, in particular, imposes severe penalties on individuals involved in child pornography violations, such as fines and imprisonment for up to five years. Given the backlash such incidents receive from society, and the possibility that disclosing their identity will expose them to further hostile discrimination or harassment in the future, it is critical to keep the victim's identity private, especially when it involves minors who may be unaware of their legal rights.

The act aims to protect children's privacy and reputation while also prohibiting the direct or indirect publication of their identity. Nonetheless, this protection applies only to media publications, not the internet, where reporting or disclosure is more difficult due to anonymity. India currently does not have an online mechanism in place for closely monitoring, reporting, and removing content connected to child sexual abuse. As a result, CSAM reporting and removal statistics are not available, monitored, or analysed, and there is a lack of awareness about how to report CSAM-related content. This paper attempts to critically assesses the limitations of current legal provisions, particularly under the POCSO Act, in adequately safeguarding the identities of victims and this paper also emphasises the need for re-evaluation of the treatment of child pornography offenses, advocating for distinct legal measures that acknowledge the digital nature of this form of exploitation and prioritize the protection of victims' rights and well-being.

Keywords: POSCO, IPC, Child Pornography, victim identity protection, rights of children, ministry of women and children, cybercrime, Child sexual abuse material.

¹ Khushboo R. Hotchandani, *every child is special- a study of child sexual abuse and the law (POCSO) in India*, International Journal of Creative Research Thoughts (IJCRT) Volume 6, Issue I (2018) <www.ijpub.org>

CHAPTER 1

INTRODUCTION

The use of children as subjects in pornographic materials is extremely detrimental to both the children and society as whole. Sexually abused children are unable to form healthy emotional relationships later in life, have sexual dysfunctions, and are more likely to become sexual abusers as adults. The United States Supreme Court² has recognised that child pornography can be a more dangerous threat to a young victim than sexual assault or prostitution. Because the child's acts are reduced to a recording, the pornography may haunt her in the years following the original misdeed.

Child pornography is generally created with the goal of gaining money from it. The exploiters often publish the videos for sale on websites, which then distribute the recordings to the end users. In addition to the fact that specific child pornography depicts physical and sexual abuse of children, the fact that such abuse has been documented, spread, and watched adds to the victimisation and mistreatment of the young victims. Knowing that the abuse that has been documented and depicted is still happening and being enjoyed by others adds to the anguish.

Any sexual abuse survivor will face hostile prejudice and social marginalisation in their community. Such a victim will have difficulty finding work, getting married, and integrating into society as a normal person. Although our criminal law lacks adequate means for protecting witnesses, it is critical to protect the victim and their identity, particularly the identity of a child, in order to protect them from future harassment or prejudice.

The Calcutta High Court in Bijoy case³ has also given other directions to ensure that the provisions of the law are followed in letter and spirit, and the fundamental rights of a child victim and other basic human rights are protected.

In the case of *Nipun Saxena and another vs. Union of India and others*, (2019) 2 SCC 703⁴ the court stated that “We are clearly of the view that the phrase “matter which may make known the identity of the person” does not solely mean that only the name of the victim should not be disclosed but it also means that the identity of the victim should not be discernible from any

² *Ferber*, 458 U.S. at 759-60

³ *Bijoy case* 2017 SCC OnLine Cal 417

⁴ *Nipun Saxena and another vs. Union of India and others*, (2019) 2 SCC 703

matter published in the media. The intention of the law makers was that the victim of such offences should not be identifiable so that they do not face any hostile discrimination or harassment in the future.”

Following numerous regulations requiring the confidentiality of victims' identities and repeatedly stating that no one may print or publish the victim's name in print, electronic, social media, or any other manner that could lead to the victim being identified and making her identity known to the general public.

But still in cases such as In *Re: Prajwala Letter (2017)*, it was observed the videos and information being circulated online. The judiciary has regularly ruled that media comprises press, electronic, and social media outlets. However, the laws could only safeguard the victim's identity to the extent that they were published by the press, and since internet transfers and sharing are anonymous, it is exceedingly difficult to identify the individual who is publishing such CSAM. The decision of *Gambhirsinh R Dekare*⁵ the court clarified that sub-section (3) of Section 23 of the POCSO Act do not limit on the application of penal provisions of Section 23 of the Act only to the editor, owner or publisher of the media or studio or photographic facilities, rather the provision makes them jointly and severally liable with all other persons who contravene the provisions of Section 23 of the Act.

The detection and prosecution of child pornography requires technological expertise, such as the ability to examine temporary Internet files and find secondary storage devices, as well as the continual training in the handling of electronic evidence⁶. The evidence that prosecutors need to establish their cases must be regularly updated and can be hidden or stored on mobile, easily replaceable microchips. Legal concerns with the seizure of evidence in child pornography cases may occur as a result of rapid technological advancements, including how photos are created and stored, as well as the possibility that computer crime laws will alter.

This was also emphasised in the case of *Avnish Bajaj v. State (2005)*⁷ Court noted that "India may wish to develop a different kind of legislative model to regulate the use of the internet with a view to prohibiting its use for disseminating child pornographic materials; this task

⁵ *Gambhirsinh R. Dekare v. Fhalgunbhai Chimanbhai Patel* AIR 2013 SC 1590.

⁶ Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, BERKELEY TECH. pp-1227-1239 (2004).

⁷ *Avnish Bajaj v. State* (2005) 116 DLT 427

deserves the utmost priority,"

Literature Review –

Courtney Fraser, *From "Ladies First" to "Asking for It": Benevolent Sexism in the Maintenance of Rape Culture*, California Law Review, (2015)

This study suggests that direct legal reforms alone are insufficient to address sexual harassment and rape. It evaluates legislative suggestions in this area, some of which have been enacted. It claims that in order to reduce the rates of rape and acquittal, gender norms and the inflexible binary separation of gender must be broken. The researcher intends to employ this study to make claims about victim blaming and gender norms and how these directly affect the need for improved victim identity protection.

Nipun Saxena and another vs. Union of India and others, (2019) 2 SCC 703

This landmark judgment gave a set of well-established guidelines for victim identity protection be it under POCSO, IPC, JJ Act and the researcher intends to rely on these guidelines further in the study. In this case it was also established that law enforcement authorities who are aware of the victim's identity are required to maintain all information confidential and to only share it in reports that are given to the investigating authorities or the court under sealed cover. even under the Right to Information Act, 2005, no one should get the reports contained in sealed covers.

Wendy Walsh, Melissa Wells, Janis Wolak, *Challenges in Investigations and Prosecutions of Child Pornography Crimes*, Refining Child Pornography Law: Crime, Language, and Social Consequences, (2016)

The purpose of the study was to analyse the investigations for prosecutors and law enforcement officials and to add data from previous studies to increase the understanding of these crimes' investigation and prosecution. They specifically look at how law enforcement responded to these crimes, what methods they employed to investigate them, and how much of a focus dual offender who commit both child sexual assault and pornography are found in these investigations. The author emphasised on the challenges investigating child pornography crimes and difficulties in computer forensics like Timeliness of the forensic exam, Lack of equipment or training of officers and Search warrant issues, the researcher employs these

challenges as the basis in their paper.

Audrey Rogers, *The Dignitary Harm of Child Pornography—From Producers to Possessors, Refining Child Pornography Law: Crime, Language, and Social Consequences*, (2016)

This study discusses the harm that child pornographers bring to their victims. Discussing the various and comparable harms caused by their acts, it covers both the producers and nonproducers, as well as downstream users, of pornographic images. Given that present legislation associates harm and punishment with these groups, the study discusses the categorization of the numerous actors involved in child pornography and the researcher tends to employ it in their research.

Reporting abuse, Reporting abusers- reflections from survivors on mandatory reporting, Arpan organisation (2018)

These reports provided the interviews with survivors on guidelines on mandatory reporting. Their narratives put forth by them were Guilt and shame, they were two very common determinants that were obstructions to disclosure. While one could sense the feelings of guilt and shame in almost all the narratives, eight of the respondents explicitly stated that they were sure the abuse was their fault. The researcher intends to rely on these narratives to establish the importance of victim identity protection.

Kenneth J. Herrmann, *Children Sexually Exploited for Profit: A Plea for a New Social Work Priority, Social Work*, (1987)

The researcher intends to rely on the chapter named as ‘effects on children and society’ where the author mentioned that fighting child sexual and commercial abuse is not just another social issue or an isolated cultural anomaly. Social workers' professional ideals and ethics will be put to the test by how they handle this issue. These kids are in severe need of whatever assistance the profession may offer.

Research Problem-

Section 23 of the Protection of Children from Sexual Offences (POCSO) Act strictly protects the identity of child victims and forbids any kind of disclosure. Despite the fact that this clause covers all crimes, including child pornography, its application frequently concentrates on

traditional media sources rather than the internet, which is where child sexual abuse material (CSAM) is most prevalent. Given that anyone with internet access can access and spread CSAM, this leaves a large gap in the response to the special difficulties presented by online exploitation and the anonymity in the case of internet inclusion makes it difficult to report it. As a result, there is an evident lack of thorough information regarding CSAM reporting and removal initiatives, which is made worse by insufficient monitoring and analysis of such content. Furthermore, there is still a lack of awareness on giving complaint or to report the matters to for content relevant to CSAM, which makes intervention less effective.

Research Questions-

1. What recent legal developments have occurred in India addressing sexual abuse of the child?
2. Are the current legal provisions under POCSO and IPC adequate to protect victim's identity?
3. Should child pornography be treated the same as all the other sexual offences against a child?
4. What approaches can be employed to safeguard the identity of victims in cases of child pornography, especially when their images are already circulating online?
5. Should Indian lawmakers consider amending Information Technology Act to expedite the detection of child pornography and ensure prompt protection of victims' identities?

Objectives-

- To understand recent legal developments that have occurred in India addressing the sexual abuse of a child
- To evaluate the current legal provisions under POCSO and IPC that ensure identity protection.
- To assess the difference between child pornography and other sexual offences against a child under POCSO

- To critically analyze the approach taken by the Indian legislators.
- To provide recommendations and suggestions that are appropriate and effective for Indian context.

Hypothesis-

Due to the digital nature involved victim identity protection for child pornography should not be treated at par with other sexual offences against a child.

Scope of the study

This study focuses on victim identity protection in cases of child pornography, it delves into the aspects of victim identity protection against child sexual abuse in India. The study is limited to the evaluation related to the role of existing laws and the need to treat child pornography differently and advocates for amendment.

Limitation of the study-

The study mostly analyses existing laws, regulations, court decisions, and legal principles. As a result, it may lack reliable information on the real experiences, views, and decision-making processes of people undergoing as there are strict laws against publication. As a result, researchers faced challenges due to the limited availability of prior research on this subject and constrained access to pertinent data sources.

Methodology-

The researcher will use a doctrinal methodology to examine the legal implications of child pornography in terms of their identity protection. The researcher gathered primary data from legal databases such as JSTOR, HeinOnline, google scholar, Scconline and Manupatra, as well as material published on the websites of ministry of women and children, India child protection fund, and related documents. In addition, secondary data was incorporated from a number of official sources, such as books, websites, codes, and existing surveys. The researcher will attempt to explore children rights under international standards, identifying structures, differences, and possibilities for legal reform.

CHAPTERIZATION

CHAPTER -2 CURRENT LEGAL PROVISIONS

There are three major international legal instruments that address child pornography: the Optional Protocol to the United Nations Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography, the Council of Europe Convention on Cybercrime, and the Council of Europe Convention on the Protection of Children from Sexual Exploitation and Sexual Abuse.

In the UN Convention on the Rights of the Child. According to the convention, all state parties that have signed it must seek to prevent sexual exploitation of children, as well as the exploitation of minors for pornographic reasons⁸.

However, how this work should be carried out is not prescribed, and numerous factors influence how each state approaches the problem. Because it is not specifically specified that possession of child pornography should be criminalised, states may decide whether or not possession is a crime.

In India, the Protection of Children from Sexual Offences (POCSO) Act of 2012⁹ was adopted, which limits the subject matter to offences against children. The POCSO Act was modified in 2019. The updated POCSO contains stringent provisions such as the death penalty for serious sexual abuse on children. The Protection of Children from Sexual Offences (Amendment) Act, 2019, includes multiple sections that target child pornography in India. According to the amended act, anyone who uses a child or children for pornographic purposes shall be punished with imprisonment for a term of not less than five years and a fine, and in the event of a second or subsequent conviction with imprisonment for a term of not less than seven years and a fine. The Act is gender neutral, defining a child as anybody under the age of eighteen. It considers the child's best interests and welfare to be the most important consideration at all stages, in order to ensure the child's healthy physical, emotional, intellectual, and social development. The Act also requires mandatory reporting of the offence by anybody who is aware of it, in order to combat the culture of silence that is typically associated with such crimes.

⁸ Convention on the Rights of the Child, 1989

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

Since The growth of the Internet and advanced digital technology corresponds to the explosion of the child pornography market. Child pornography photos are easily accessible via almost any Internet technology, including social networking websites, file-sharing sites, photo-sharing sites, gaming gadgets, and even mobile apps. Child pornography offenders can also join on Internet forums and networks to discuss their interests, wants, and experiences abusing children, as well as sell, share, and trade photographs.

The information technology Act of 2000 criminalises the publication or transmission of any obscene material in electronic form. The former Act had no specialist provisions for child pornography; all occurrences of pornography were dealt with under Section 67 of the earlier Act. It is worth noting, however, that the IT Act of 2000 represented a significant improvement over previous legislation.

Previously, all cases of pornography, whether online or offline, were prosecuted under the Indian Penal Code 1860 and the Indecent Representation of Women (Prohibition) Act 1986. The transmission or publication of obscene content is punishable by imprisonment for two years and five months, with a fine of up to five lakh rupees, and any subsequent conviction by five years in prison and a fine of up to 10 lakh rupees. The later revision to the 2000 Act in 2008 specifically criminalises child pornography.

The act of publishing or transferring anything depicting children in sexually explicit situations is criminal. Furthermore, it criminalises the viewing, gathering, distribution, and manufacture of any sexually explicit content featuring children. Inducing internet relationships with children, enabling child abuse online, and filming sexual abuse of children on electronic devices are all serious offences¹⁰. The Act punishes a first conviction with five years in prison and a fine of up to five lakh rupees, while a second conviction is punishable by seven years in prison and a fine of up to 10 lakh rupees. The crime under the Act is both non-bailable and cognisable¹¹. Section 67C holds intermediaries responsible for the retention and production of information.

¹⁰ Belur Jyoti, Singh Brijesh Bahadur, *Child Sexual Abuse and Law in India, Crime Science – An Interdisciplinary Journal*, (2015).

¹¹ *Ibid*.

Section 67B¹²: Punishment for electronic publication or transmission of material depicting children in sexually explicit acts, etc. The following actions are prohibited:

- (a) publishing or causing to be published or transmitted material in any electronic form depicting children engaging in sexually explicit acts or conduct;
- (b) creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging, or distributing material in any electronic form depicting children in an obscene, indecent, or sexually explicit manner; or
- (c) cultivates, entices, or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- (d) Facilitates online abuse of children, or
- (e) Records sexually explicit acts with children in any electronic form,

will result in imprisonment for up to five years and a fine of up to ten lakh rupees on first conviction, and seven years for second or subsequent conviction. Thus, with the addition of Section 67B, Child Pornography received its first unique and devoted statute.

Furthermore, according to information acquired from the Ministry of Electronics and Information Technology, the government's policies are geared at guaranteeing a safe, trustworthy, and accountable Internet for all users. The publication or transfer of obscene material in electronic form constitutes cybercrime. The Information Technology Act of 2000 ("IT Act") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021 ("IT Rules, 2021") provide for penalties and punishments for such acts, as well as obligations on intermediaries, including social media intermediaries, to exercise due diligence under rule 3(1)(b).

In the event that intermediaries fail to meet the diligence requirements outlined in the IT Rules, 2021, they will lose their safe harbour protection under Section 79 of the IT Act and will be subject to consequential action under such law.

¹² Section 67B, Information Technology Act, 2000.

According to Section 77B¹³, such cybercrimes are punishable violations. According to the requirements of the Code of Criminal Procedure, 1973, the police are responsible for the prevention and investigation of cognizable offences, and 'Police' is a State subject under the Constitution's Seventh Schedule. As a result, states are primarily responsible for the prevention, investigation, and prosecution of such cybercrimes through their police departments, which take preventive and penal action as required by law, including in the case of cybercrimes involving the publication or transmission of sexually explicit or obscene material in electronic form.

The Information Technology Act, 2000 ("IT Act") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"), together, have made a framework that cast obligations on intermediaries, including social media intermediaries, to observe due diligence and provide that if they fail to observe such due diligence, they shall no longer be exempt from their liability under law for third-party information, data, or communications. This due diligence involves the following:

- i. Users must make reasonable efforts not to host, display, upload, modify, publish, transmit, store, update, or share information that is harmful to children, obscene, invasive of bodily privacy, or violates any law¹⁴.
- ii. If a grievance, court order, or notice from the appropriate government or agency is received, users must not host, store, or publish unlawful information.
- iii. Upon receiving a legitimate order from a government agency, give information or assistance for prevention, detection, investigation, or prosecution within 72 hours.
- iv. Establish a grievance redressal mechanism to resolve violations of the rules within 72 hours of reporting. If a complaint is made by an individual or their authorised representative, remove any content that potentially exposes their private area within 24 hours. The rules were amended on 28.10.2022 to include the establishment of a Grievance Appellate Committee(s) for users to appeal¹⁵.

¹³ Section 77B, Information Technology Act, 2000 ("IT Act")

¹⁴ Information Technology Act, 2000 ("IT Act")

¹⁵ the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")

- v. For social media intermediaries with over 50 lakh registered users in India, it is recommended to appoint a Chief Compliance Officer, a nodal contact for 24x7 coordination with law enforcement agencies, and a Resident Grievance Officer. Technology-based measures, such as automated tools, should also be used to proactively identify informants¹⁶.
- vi. If a social media intermediary primarily provides messaging services, they must identify the first originator of information on their computer resource to prevent, detect, investigate, prosecute, or punish rape, sexually explicit material, or child sexual abuse offences.

Keeping in mind complaints regarding action or inaction on the part of the social media intermediaries and other intermediaries on user grievances regarding objectionable content or suspension of their accounts, the Central Government has also established three Grievance Appellate Committees (GACs), as provided for in the said IT Rules, 2021, to enable users to appeal against the decisions made by the Grievance Officer of intermediaries on user complaints.

Furthermore, under the Code of Ethics prescribed in the Part III of IT Rules, 2021, publishers of an online content curator are required to classify all content transmitted, published, or exhibited by them, based on the nature and type of content, into various rating categories, including content suitable for children, content suitable for persons aged 7 years, 13 years, 16 years and above, or persons under the said ages with parental guidance, and to display such content¹⁷. They are also expected to restrict a child's access to specific curated content by implementing adequate access control mechanisms.

CHAPTER -3 NEGLECTED VICTIM IDENTITY

In *Ranjit D Udeshi v. State of Maharashtra* (AIR 1965 SC 881)¹⁸, the Honourable Supreme Court stated that the test of obscenity to be used in India is that if an obscenity is published for commercial purposes rather than social purposes, it cannot be protected by the constitutional

¹⁶ *Ibid*

¹⁷ Part-III, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")

¹⁸ *Ranjit D Udeshi v. State of Maharashtra* (AIR 1965 SC 881)

right to free speech and expression. Obscenity is defined as treating sex in an appealing manner or with the intention of appealing to human nature's carnal desires.

Child pornography can be divided into two categories: paedophilia, in which people enjoy the involvement of children, and human trafficking, in which children are given hormone tablets to make them appear older before being recorded.

Administering hormone tablets to minors in order to change their appearance for the aim of producing pornographic content creates major legal concerns¹⁹. Depending on the circumstances and jurisdiction, this practice could result in medical malpractice, child abuse, or other criminal offences.

Paedophiles who exchange child pornography on computers actively utilise encryption. Criminal organisations appear to be leveraging the proceeds from IP-infringing products to support pornography²⁰. When encrypted data is intercepted by an unauthorised entity, the intruder must determine which cypher was used to encrypt the data and what key is necessary to decrypt it²¹. Pornographic websites expose the syndicate to legal liability by failing to block access to such material simply because the technology exists.

Obscene content can emerge from a variety of sources, including electronic and print media. To comprehend what constitutes obscenity or pornography in electronic (digital) form, one must first understand the accessible media in society and how it is used. Any content in the context would include video files, audio files, text files, photos, animations, and so on, all of which may be kept on CDs, websites, laptops, or cell phones. While the Internet promotes knowledge-based enterprises and trade, it also facilitates the theft, production, and distribution of items such as software, music, films, books, and games²². With the click of a mouse, identical copies may be created and shared quickly, cheaply, secretly, and repeatedly.

The Internet has increased the variety, volume, and availability of sexually harmful imagery, including pornography. Law enforcement's databases are not ideal since they rely on humans

¹⁹ Flowers, R. Barri. "The Sex Trade Industry's Worldwide Exploitation of Children." *The Annals of the American Academy of Political and Social Science*, vol. 575, pp. 147–57 (2001). <http://www.jstor.org/stable/1049185>.

²⁰ Herrmann, Kenneth J. "Children Sexually Exploited for Profit: A Plea for a New Social Work Priority." *Social Work*, vol. 32, no. 6, pp. 523–25, (1987) <http://www.jstor.org/stable/23715528>.

²¹ *ibid*

²² Chertoff, Michael, et al. "THE IMPACT OF THE DARK WEB ON INTERNET GOVERNANCE AND CYBER SECURITY." *Cyber Security in a Volatile World*, Centre for International Governance Innovation, pp. 29–36, (2017).

to determine whether or not files include child pornography.

The National Centre for Missing and Exploited Children (NCMEC), a US-based NGO, runs a Child Victim Identification Lab. This lab compares the hash values provided by law enforcement through the CVIP programme. NCMEC staff determine whether or not the image or video contains child pornography. This is often completed swiftly in United States Postal Inspector Offices, Regional Computer Forensics Labs, Attorney General Offices, Crime Labs, and other locations where NCMEC has established specialised PCs with VPN connections to their database for matching purposes²³. The option is to send a CD, DVD, or hard drive to CVIP for processing and wait for the results.

In a similar case that has outraged India, a 17-year-old Delhi schoolboy allegedly used his cell phone to record a sex act with a 16-year-old girl. The clip was eventually sold on video CDs via the auction site Baazee.com,²⁴ prompting the arrest of the company's India manager. A juvenile court gave the child bail while ordering him not to leave the country. Mr Bajaj was also granted bail. He was arrested under the Information Technology Act of 2000, which forbids the use of the Internet to spread obscene or pornographic content. According to Baze.com, the offending clip was removed off the site as soon as the nature of its contents became known. The alleged the supplier of the 2 minute and 37 second a film, is an engineering student, and has also been arrested.

It is evident that the Child abuse material reporting present currently is unreliable to protect victim's identity, since by the time databases try to acknowledge it as a video of pornography it is circulated around and is in possession of others. Moreover, the content that gets reported on these databases is unlimited. even if they do identify it as a video of child pornography due to the encryption used it becomes difficult to track the circulation and the first user.

CHAPTER - 4 LEGAL COMPLICATIONS OF EQUATING CHILD PORNOGRAPHY WITH OTHER OFFENCES

Sections 23 of the POCSO Act and Section 74 of the Juvenile Justice Act address the identification of child victims. Section 23(2) of the POCSO Act prohibits the disclosure of any

²³ Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, BERKELEY TECH. pp-1227-1239 (2004).

²⁴ Paul Watson, *American Freed in Indian Scandal*, Los Angeles Times, (2017).

information that could identify the identity of a juvenile victim of sexual offences, such as the child's name, residence, portrait, family information, school, locality, or other facts²⁵. Violating this prohibition is a criminal punishable by a six-month to one-year jail sentence and a fine.

Section 74 of the Juvenile Justice Act prohibits the publication of "name, residence, school, or any other detail" that could be used to identify a child who is a victim of a crime, or even a kid accused of committing a crime, as well as minors who witness a crime²⁶.

Violating this limitation is a criminal offence punishable by a fine and/or up to six months in prison. Both of these prohibitions are intended to prevent the release of any material that could be used to identify a child victim, such as photographs or information about their parents. Section 228A of the Indian Penal Code 1860 (IPC) prohibits the printing or publication of a rape victim's name or any other information revealing their identity. Adults and minors should be aware of this²⁷.

This restriction, however, may be waived by the survivor or, in circumstances where the victim has died (or is unable to give consent), by the victim's family, in writing to a designated welfare institution or other suitable entity.

In December 2019²⁸, Justices Madan B. Lokur and Deepak Gupta's bench issued a directive declaring that FIRs filed for rape charges under the Protection of Children from Sexual charges (POCSO) Act and the Indian Penal Code (IPC) shall be kept confidential. The top court also said that the names and identities of rape and sexual assault victims, even those who have died, cannot be revealed in any form. It went on to say that as long as the victim is willing to provide their identify, nobody can object. The judges also warned the media to avoid "sensationalising" similar situations and advised caution.

The court further ordered the police to store all documents including the victim's name in a sealed cover and replace them with identical documents that exclude the victim's name from any records that the general public can view or study.

²⁵ Sections 23, POCSO Act, 2012

²⁶ Section 74 of the Juvenile Justice Act, 2015

²⁷ Indian Penal Code, 1860 (IPC)

²⁸ Nipun Saxena and another vs. Union of India and others, (2019) 2 SCC 703

In the matter of XXXXXXXXXXXX v. State of Kerala & Ors. [WP(C) NO. 40709 OF 2023]²⁹, the court ruled that omission would subject the learned Magistrate to criminal prosecution under Section 228 A of the IPC. I have no doubt that the answer is negative because Section 228 A of the IPC states that "whoever prints or publishes the name or any matter which may make known the identity of a person against whom an offence under Section 376, among others, of the IPC is alleged, or found to have committed, shall be punished with imprisonment of either description for a term which may extend to two years and a fine." Further observing that Section 228 A could not, by any stretch of the imagination, apply in the situation of a court, the Court noted, "The forensic position, therefore, is completely clear. The offence under Section 228 A of the IPC would be attracted to a person who prints or publishes any matter in order to reveal the identity of the victim of an offence under Section 376 of the IPC, but it does not cover a case where a Court inadvertently reveals such name in Court proceedings or orders."³⁰

The main concern with the forensic is that the identity collection is on par with the other provisions involving sexual conduct. It is important to note that child pornography involves a significant element of having a digital existence, so treating it on par with other offences increases the likelihood that the images are already circulated before action is taken.

CHAPTER-5 PROPOSING GUIDELNES FOR TREATMENT OF CHILD PORNOGRAPHY

It is recommended to strengthen coordination between government agencies, non-governmental organisations, and international partners in combating child pornography, as well as drafting a policy recommendation for legislative reforms or new laws addressing child pornography specifically.

The fight against child pornography began with the United Nations Convention on the Rights of the Child, which recognised it as a violation of children's rights. Member nations were urged to implement specific measures to prevent children from being exploited in pornographic materials (Article 34 of the UNCNC, 1989). Currently, Directive 2011/93/EU of the European

²⁹ XXXXXXXXXXXX v. State of Kerala & Ors. [WP(C) NO. 40709 OF 2023]

³⁰ Moharana ,S.D.,*Protection of Child against Sexual Offences Act, 2012: An Analytical Study*, International Journal of Academic Research, pp- 85-92 (2015).

Parliament and of the Council of 13 December 2011, on fighting child sexual abuse and exploitation, as well as child pornography, outlines European actions in this field.

This directive, along with the Budapest Convention³¹ (Convention on Cybercrime of November 23, 2001) and the Lanzarote Convention³² (Convention of the Council of Europe for the protection of children against sexual exploitation and abuse, October 25, 2007), served as the foundation for recent reforms to Spanish criminal law aimed at combating this type of crime³³. When making provisions for child pornography, it is necessary to consider the rationale behind the aforementioned standards.

More awareness programmes, such as the Internet Sex Offender Treatment Programme, which the British National Offender Management Service implements in its probation services, are a group treatment programme for those convicted of crimes including the distribution of child pornography³⁴. The program's goals are to lessen the possibility of both future Internet-related crimes and actual sexual abuse. The i-SOTP is essentially a cognitive-behavioural programme designed to modify risk variables. The treatment method consists of a pre-program meeting as an introduction, six modules (35 two-hour sessions), and a review meeting. This serves to dissuade people from desiring to consume child pornography and, as a result, does not allow websites to profit from child exploitation.

Mainly, an act that establishes a mechanism for all digital crimes and adopts a different adjudication approach for such crimes in which the victim's identity is protected, where their privacy is utmost.

CHAPTER-6 CONCLUSION

To summarise, in cases involving paedophilia, legal systems may need to evaluate the perpetrators' mental health. While paedophilia is not a crime in and of itself, exploiting minors to satisfy those needs is illegal. Rehabilitation programmes and therapeutic interventions may

³¹ Budapest Convention, 2001

³² Lanzarote Convention, 2007

³³ Osborn J, Elliott I, Middleton D, Beech A, "The use of actuarial risk assessment measures with U.K. internet child pornography offenders", J Aggress Confl Peace Res;2(3): pp.no 16–24, (2010).

³⁴ Marcus K. Rogers, Kathryn C. , Sienna Bates, Kayla Rux, "Online child pornography offender risk assessment using digital forensic artifacts: The need for a hybrid model", Psychiatry & Behavioral Science; Digital & Multimedia Sciences (2021).

be used in the legal process to address underlying issues and lessen the likelihood of reoffending³⁵.

Even with such elaborate legislative mechanisms for penalising child pornography, reducing child pornography is a difficult challenge. The current technology is not sufficiently advanced to produce child pornography from a wide range of pornography. As a result, forensics must be modified to facilitate easy reporting and tracking, reducing dependency on human-operated databases.

Hence the hypothesis is hereby proven as positive.

³⁵ Henshaw M, Ogloff JRP, Clough JA. *“Looking beyond the screen: A critical review of the literature on the online child pornography offender”*, Sex Abuse; Vol 29(5): pp.no 416–45, (2017).

REFERENCES

- Herrmann, Kenneth J. “Children Sexually Exploited for Profit: A Plea for a New Social Work Priority.” *Social Work*, vol. 32, no. 6, pp. 523–25, (1987) <http://www.jstor.org/stable/23715528>.
- Flowers, R. Barri. “The Sex Trade Industry’s Worldwide Exploitation of Children.” *The Annals of the American Academy of Political and Social Science*, vol. 575, pp. 147–57 (2001). <http://www.jstor.org/stable/1049185>.
- Chertoff, Michael, et al. “THE IMPACT OF THE DARK WEB ON INTERNET GOVERNANCE AND CYBER SECURITY.” *Cyber Security in a Volatile World*, Centre for International Governance Innovation, pp. 29–36, (2017).
- Marcus K. Rogers, Kathryn C. , Sienna Bates, Kayla Rux, “*Online child pornography offender risk assessment using digital forensic artifacts: The need for a hybrid model*,” Psychiatry & Behavioral Science; Digital & Multimedia Sciences (2021).
- Osborn J, Elliott I, Middleton D, Beech A, “*The use of actuarial risk assessment measures with U.K. internet child pornography offenders*”, J Aggress Confl Peace Res;2(3): pp.no 16–24, (2010).
- Henshaw M, Ogloff JRP, Clough JA. “*Looking beyond the screen: A critical review of the literature on the online child pornography offender*”, Sex Abuse; Vol 29(5): pp.no 416–45, (2017).
- Belur Jyoti, Singh Brijesh Bahadur, *Child Sexual Abuse and Law in India, Crime Science – An Interdisciplinary Journal*, (2015).
- Moharana ,S.D.,*Protection of Child against Sexual Offences Act, 2012: An Analytical Study*, International Journal of Academic Research, pp- 85-92 (2015).
- Khushboo R. Hotchandani, *every child is special- a study of child sexual abuse and the law (POCSO) in India*, International Journal of Creative Research Thoughts (IJCRT)Volume 6, Issue I (2018) <www.ijpub.org>

- Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, BERKELEY TECH. pp-1227-1239 (2004).
- Wendy Walsh, Melissa Wells, Janis Wolak, *Challenges in Investigations and Prosecutions of Child Pornography Crimes*, *Refining Child Pornography Law: Crime, Language, and Social Consequences*, (2016).
- Courtney Fraser, *From "Ladies First" to "Asking for It": Benevolent Sexism in the Maintenance of Rape Culture*, *California Law Review*, (2015).
- Reporting abuse, *Reporting abusers- reflections from survivors on mandatory reporting*, Arpan organisation (2018).
- Budapest Convention, 2001
- Lanzarote Convention, 2007
- POCSO Act, 2012
- Section 74 of the Juvenile Justice Act, 2015
- Indian Penal Code, 1860 (IPC)
- Paul Watson, *American Freed in Indian Scandal*, Los Angeles Times, (2017).
- Ranjit D Udeshi v. State of Maharashtra (AIR 1965 SC 881)
- Convention on the Rights of the Child, 1989
- Protection of Children from Sexual Offences (POCSO) Act of 2012
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")