



ISSN: 2583-7753

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]



Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

“Law in the Age of Artificial Intelligence: A Fundamental Perspective”

Organised by KES’ Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: <https://doi.org/10.70183/lijdlr.2026.v4si1.06>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

KES' SHRI. JAYANTILAL H. PATEL LAW COLLEGE

About the College



KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

KANDIVLI EDUCATION SOCIETY

Established 1936



Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

EDUCATIONAL COMMITMENT

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

LAW IN THE AGE OF ARTIFICIAL INTELLIGENCE

A Fundamental Perspective



ABOUT THE INTERNATIONAL CONFERENCE

The International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective” provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

PRINCIPAL'S MESSAGE

KES' Shri. Jayantilal H. Patel Law College



It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on “Law in the Age of Artificial Intelligence: A Fundamental Perspective.”

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

DR. VIRAL DAVE

I/c. Principal

KES' Shri. Jayantilal H. Patel Law College

ORGANISING COMMITTEE

International Conference on Law in the Age of Artificial Intelligence



I/c. Principal

Dr. Viral Dave

Convenor

Mr. Mahavir Mandot

Co-Convenors

Dr. Shweta Vijendra Pathak

Ms. Priyanka Khakhadia

Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

*Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of
Doctrinal Legal Research [Volume IV, Special Issue I, 2026]*

AI AND RIGHTS OF THE CHILD: ASSESSING THE EFFECTIVENESS OF INDIAN LAWS IN PREVENTING MALICIOUS USE OF ARTIFICIAL INTELLIGENCE AND THE SCOPE FOR AI-BASED CHILD PROTECTION

Sneha Pandey¹

I. ABSTRACT

Artificial Intelligence is 21st century's equivalent of nuclear technology. For this prime and unreplaceable asset, the humankind has enrolled itself in the never-ending race to secure the highest position in the field of Artificial Intelligence technology. However, history remains the prime witness to the fact that every time the human race has chased its obsession to run after unsustainable development, the marginal sections have had to pay the price in some way or the other. The International AI Safety Report 2025, conducted by over 96 independent international AI experts led by Yoshua Bengio (a machine learning pioneer) was published with the support of the UK's Department for Science, Innovation and Technology (DSIT) and coordinated through the UK AI Safety Institute (AISi). This report highlights the risks of using general purpose AI. One of the risks flagged by the report is the rise in malicious use of the Artificial Intelligence to generate Child Sexual Abuse Material (CSAM). In a recent mortifying incident, this risk's warning was turned true when X's AI Grok was misused on a large scale for creating sexually explicit images of women and minors by "digitally undressing" them in photos they had uploaded on 'X'. In this context, the present research paper aims to assess the effectiveness of the existing legal framework in India to prevent and protect the violation of rights of children by the malicious use of Artificial Intelligence technology. In addition to this, the research paper also attempts to explore the possibility of using Artificial Intelligence as a tool for identifying, tracing and curbing the violation of Rights of Children through AI.

¹ 3rd Semester, LLM in Business Law, student at KES' Shri Jayatilal H. Patel Law College, Independent Advocate practicing on criminal side at Bombay High Court and Metropolitan Magistrates courts in Mumbai (India).Email: sneharp3@gmail.com

II. KEYWORDS

Artificial Intelligence, Child Rights, CSAM, DPDPA, POCSO.

III. INTRODUCTION

“We owe our children- the most vulnerable citizens in any society- a life free from violence and fear” by Nelson Mandela. In recent years, Artificial Intelligence has become a subject of public discourse for people from all walks of life. Artificial Intelligence, which has been defined as “the study and development of computer systems that can copy intelligent human behaviour”, has caused, and is expected to continue causing, a significant transformation in the way the world functions. Transformation in any form requires adaptability, and such adaptability does not come easily to the weakest links of society, namely vulnerable sections.

One such vulnerable section is the “Child”. For the purposes of the present paper, a child is considered to be any human being below 18 years of age. With respect to rights affected by Artificial Intelligence, the present paper focuses on the Right to Privacy and the Right Against Abuse, both of which form an integral part of international and Indian legal frameworks.

The research problem addressed in this paper is that India’s existing child-protection and data-protection laws respond to AI-facilitated harms in a fragmented manner, without a dedicated legal framework for preventing the malicious design, deployment, and use of AI systems against children. While statutes such as the DPDPA, the IT Act, and POCSO provide important safeguards, their adequacy in addressing AI-generated CSAM, automated profiling, online grooming, and privacy violations remains uncertain. This paper therefore investigates whether the existing Indian legal framework is sufficiently equipped to prevent, regulate, and punish AI-enabled violations of children’s rights, and whether AI itself can be responsibly used as a child-protection tool.

A. Research Objectives

1. To assess the effectiveness of the Indian laws in protecting the Rights of the Child, primarily Right to Privacy and Right Against Abuse against malicious use of AI.

2. To consider the challenges faced in use of AI for protecting the Rights of the Children

B. Scope

The scope of the present paper is to assess the effectiveness of Indian laws such as DPDP Act, IT Act 2000 and similar laws in protecting the Right to Privacy and Right Against Abuse of the Child. It also extends its scope to considering the challenges encountered while adopting AI as a tool for child safety. This paper analyses the Indian legal framework to uncover the gaps in them, in order to strengthen child protection framework.

C. Research Questions

1. How effective are Indian laws in protecting the Right to Privacy and Right Against Abuse of the Child against the malicious use of AI?
2. What are the challenges of adopting AI as a tool for child safety?

D. Research Methodology

The present research adopts a doctrinal and analytical legal research methodology. It examines the existing Indian statutory framework governing children's privacy, online safety, and protection from sexual abuse, with particular reference to the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the Protection of Children from Sexual Offences Act, 2012, and the relevant rules framed thereunder. The study also relies upon judicial decisions, government notifications, international reports, and secondary sources such as journal articles, policy documents, and institutional publications to evaluate whether the present legal framework adequately responds to AI-facilitated violations of children's rights.

The paper further uses a limited comparative approach by referring to the European Union and the United Kingdom. These jurisdictions have been selected because the European Union has enacted a comprehensive risk-based AI regulatory framework, while the United Kingdom has taken specific policy and legislative steps to address AI-generated Child Sexual Abuse Material. The comparative discussion is not intended as a full jurisdictional comparison, but is used to identify regulatory

approaches that may assist India in strengthening its child-protection framework against the malicious use of Artificial Intelligence.

E. Literature Review

Artificial intelligence has been a point of concern for India, being the home to the largest young population in the world. Studies have shown that the traditional laws may prove to punish the offenders but may not be well-equipped to fight the malicious use of AI to violate rights of the children. The present paper undertakes to assess the preparedness of Indian laws in preventing and punishing the violation of Right to Privacy and Right against Abuse of the Child. It also undertakes to consider the challenge of using AI in protecting the Rights of the Child.

IV. EFFECTIVENESS OF INDIAN LAWS IN PROTECTING THE RIGHTS OF THE CHILD

A. Right to privacy

Right to privacy is an integral part of Right to Life as held under this well-known landmark case,² that became the basis for enactment of India's Data Protection law, the Digital Personal Data Protection Act, 2023 (DPDPA) is being hailed as the balance between Right to Privacy and responsible collection and processing of data-by-Data Fiduciaries. *Sec 9. of the DPDPA* aims to protect a child's privacy by directing the Data fiduciary to take "verifiable parent consent or legal guardian consent" before processing the data of the child. In addition to the above, it also prohibits the Data fiduciary from tracking or monitoring behaviour of the child and protects a child from targeted advertising. However, there are broad exceptions to such protection given to the child in form of exemptions to be examined in the later part of this paper. It may be noted that DPDPA, is only partially in force at present and is envisioned to be enforced in phases in the later part of 2026 and in 2027.

B. Right against Abuse:

There are myriad laws that target different forms of abuse that a child may face. The laws that are being examined under this paper are:

² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

1. Protection of Children from Sexual Exploitation, 2012 (POCSO)
2. Information Technology Act, 2000

V. THREATS TO RIGHT TO PRIVACY AND RIGHT AGAINST ABUSE AND EFFICACY OF THE INDIAN LAWS

A. Right To Privacy

As it is well-known, in this world where technology is indispensable, data is the currency. In most child related crimes committed through the internet, the collection of data and monitoring the activities of the child forms the necessary part of preparation for the offenders.

Threats to privacy of a child by AI and their corresponding legal safeguards under DPDP Act 2023 and DPDP Rules 2025 are as follows:

THREAT	LEGAL SAFEGUARD
Opaque notice and consent terms: Unclear terms of what data is collected and for what purpose takes away the right to make an informed decision.	<i>DPDP Rules 2025, Rule no. 3</i> provides for an independent, clear and simple notice about the data being processed and the option to withdraw the consent given for processing such data. <i>Sec 9(1) of DPDPA</i> requires the Data Fiduciary to take verifiable consent of the parent of the child before processing any personal data of the child as per the procedure under Rule 10 of DPDP Rules, 2025 subject to certain exemptions.
Data profiling The organisations collecting and processing data used it to carry out targeted advertising. Some	<i>Sec 9 of DPDPA</i> prohibits Data Fiduciaries from carrying out targeted advertising against children but allows certain exemptions.

algorithms run by malicious actors collect data to target vulnerable kids for online grooming	
Tracking and monitoring Tracking and monitoring a child's behaviour and locations may make them an easy target.	<i>Sec 9 of DPDPA</i> prohibits Data Fiduciaries from tracking and monitoring behaviour of a child but allows certain exemptions.

B. Exemptions under DPDPA and DPDP Rules 2025

Rule 12 of the DPDP Rules 2025, the protections given under DPDPA concerned with verifiable consent of parent before collecting personal data and prohibitions on child targeted advertising, tracking and monitoring behaviour of the child have been waived in favour of certain class of:

Data Fiduciaries specified under Part A of Schedule IV of DPDP Rules, 2025	For example: Educational institution and is meant to "include any institution that imparts education including vocational education" ³
Certain purposes specified under Part B of Schedule IV of DPDP Rules 2025.	For example: Creation of a user account for communication by email.

VI. ANALYSIS

The provisions of DPDPA and DPDP Rules 2025 are noteworthy and do provide protections to a child with respect to her privacy. However, there are certain concerns:

³ Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Rules, 2025*, Gazette of India, 13 November 2025, available at: <https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>.

- 1. **Reliance on voluntary declaration:** The onus is on the child to declare herself so in order to proceed forward with the protections offered under this Act.
- 2. **Exemptions to prohibitions on targeted ads, monitoring and tracking:** The exemptions have been at the centre of controversy since the notification of DPDP Rules, 2025. The Act gives liberty to vocational institutions and for purpose of making a user account for the child for communication may prove to be a loophole that malicious entities may exploit for commercial advertising and profiling of children.

A. Right Against Abuse

According to the UK based Internet Watch Foundation, “2025 was the worst year on record for online Child Sexual Abuse Material found by its analysts, with increasing levels of photo-realistic AI material contributing to the dangerous levels”⁴ . Child Sexual Abuse Material (CSAM) can be understood as any material including a video or image or computer-generated content that shows children involved in sexually explicit acts.

The most recent horrifying incident witnessed was when X company’s chatbot Grok was used by multiple users to create non-consensual sexually explicit and intimate images of women and children. This has raised questions about preparedness of Indian laws to deal with the growing volumes of Child Sexual Abuse Material on the internet.

Threats to sexual exploitation and abuse of a child by using AI and their corresponding legal safeguards under Indian laws:

THREAT	LEGAL SAFEGUARD
CSAM generated by AI	<u>POCSO Act 2012 provisions:</u> <u>Sec 2 (da)</u>

⁴ Internet Watch Foundation, “AI becoming ‘child sexual abuse machine’, warns IWF”, available at: <https://www.iwf.org.uk/news-media/news/ai-becoming-child-sexual-abuse-machine-adding-to-dangerous-record-levels-of-online-abuse-iwf-warns>.

	“Child pornography as means any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer-generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child;” Sec 14 punishes a person for using a child for pornographic purposes that includes obscene representation of the child
Possessing and publishing CSAM	Sec 15 of POCSO, 2012 punishes a person for possessing and storing child pornography. Sec 67B of IT Act, 2000 punishes creation, publication and distribution of CSAM along with online grooming by an online relationship that may offend a reasonable adult. Sec 67B (c): Inducing or enticing a child_for online relationship with children for sexually explicit content or inducing or enticing a child in manner that may offend any reasonable adult is a criminal offence. Sec 67B (d): Criminalizes facilitation of abuse of a child online

Removing and restricting access to CSAM	<u>Sec 79 of IT Act, 2000 r/w The IT Rules, 2021</u> casts a duty on the intermediaries to remove any sexually explicit content or content involving nudity within 24 hours of receipt of complaint. In case of non-compliance, the intermediary is held liable. Sec 69A of IT Act, 2000 , empowers the Government to block CSAM content.
--	--

VII. ANALYSIS

The analysis of efficacy of provisions of the above given provisions:

The 2019 POCSO amendment, broadened its scope to include computer generated material in the definition of child pornography. This has been a significant step in targeting CSAM generated by AI. The word child pornography, however, needs to be replaced by CSAM in order to prevent undermining the pain of child abuse victims. The Hon'ble Supreme Court's decision in *Just Rights for Children Alliance v. S. Harish*,⁵ further strengthened the law with respect to possession and storage of CSAM. The Court gave a wide interpretation to 'possession' under Section 15 of the POCSO Act, 2012, so as to include constructive or intangible possession. This means that even accessing or viewing CSAM online may attract liability where the material is retained, not deleted, or not reported. The decision also clarified that the statutory presumption of culpable mental state under Section 30 of the POCSO Act may be relevant even at the stage of quashing proceedings.

This clarification is significant in the context of AI-generated CSAM because offenders may not always store material in a conventional physical form. AI-enabled abuse may involve cloud storage, temporary downloads, cached files, encrypted platforms, or repeated online access without permanent local storage. In such cases, a narrow

⁵ *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716.

understanding of possession may allow offenders to evade accountability. The Court's wider approach therefore assists law enforcement by recognising that digital possession may be constructive, intangible, or technologically mediated. At the same time, its practical application must be balanced with procedural safeguards, because automated detection, accidental exposure, or unsolicited receipt of abusive material should not be treated in the same manner as intentional possession, retention, circulation, or concealment.

IT Act 2000 provides sufficient protection by criminalising creation, publishing and transmission of CSAM under sec 67B along with any form of online grooming. Under 67B (c), Online grooming includes enticing a child to enter into a relationship with other child or children to generate sexually explicit content is covered along with any form of enticement that may offend a reasonable adult. This can be broadly interpreted to include any form of grooming to extract sexually explicit content from a child through an AI chatbot or using AI to generate fake profiles to facilitate online grooming. An unresolved issue here is that there is no explicit mention of Artificial Intelligence (AI) in the act which might lead to multiple interpretations and will hamper administration of justice in favour of survivors of online grooming.

IT Rules 2021, prescribes for a time limit of 24 hours to take down CSAM material. This period is too long considering the damage CSAM can cause to the victim in a matter of seconds.

The above given laws work as patchwork and there is a lack of an independent AI law that would not only punish but also prevent designing of such AI that can be used to generate CSAM material.

VIII. CHALLENGES OF USING AI FOR PROTECTING THE RIGHTS OF THE CHILD

Recently, Raksha AI, an AI-powered child-protection platform developed by Just Rights for Children in collaboration with India Child Protection, was introduced at the Prosperity Futures: Child Safety Tech Summit, a Ministry of Electronics and Information Technology-affiliated event. The platform is aimed at strengthening preventive responses to child marriage, child trafficking, and online child sexual

exploitation, including the identification of vulnerable geographies and emerging risks relating to CSAM. AI is also being used to educate children about their rights and to support the detection of online child-abuse material. However, such tools must be examined with caution, as concerns remain regarding algorithmic bias on the basis of caste, religion, sex, race, and income.

A. Analysis

One such instance was shared by Dhiraj Singha whose surname's first letter was interpreted by ChatGPT as "Sharma", an upper caste surname without much thought.⁶ When the author of the present paper tried to test ChatGPT's bias through prompts like, what is dalit behaviour or get me a picture of a dalit person, the AI gave neutral responses. However, when the author attempted indirect questions like "Create an image of a domestic worker or create an image of a successful person", the results seemed stereotyped.

IX. SUGGESTION

1. **Right to Privacy:** The European Union's Artificial Intelligence Act, Regulation (EU) 2024/1689, provides a comprehensive risk-based model for regulating AI systems. Article 5 prohibits certain AI practices, including systems that exploit vulnerabilities linked to age, disability, or specific social or economic circumstances where such exploitation causes or is reasonably likely to cause significant harm. Annex III further classifies several AI systems as high-risk, thereby subjecting them to stricter regulatory obligations. This approach is relevant for child protection because children are uniquely vulnerable to profiling, behavioural manipulation, emotion-recognition technologies, targeted persuasion, and automated decision-making.

India may draw from this model by placing the primary compliance burden on AI developers, deployers, and data fiduciaries, rather than relying excessively on children or parents to identify and avoid AI-related risks. A child-centred Indian AI framework should therefore include preventive duties at the design

⁶ Nilesh Christopher, "OpenAI is huge in India. Its models are steeped in caste bias", *MIT Technology Review*, 1 October 2025, available at: <https://www.technologyreview.com/2025/10/01/1124621/openai-india-caste-bias/>.

and deployment stage, mandatory risk assessment for AI tools likely to interact with children, restrictions on behavioural profiling, and stronger accountability for systems that enable privacy violations or exploitation.

2. Right against Abuse:

- **Use of the word CSEAM:** The word “Child Pornography” in the POCSO Act, 2013 and IT Act, 2000 needs to be replaced with “Child Sexual Exploitative and Abuse Material” as per the Supreme Court guidelines.
- **Criminalising Child Abuse AI:** Criminalising Child Abuse AI: The United Kingdom’s Crime and Policing Act 2026 introduces specific measures addressing CSA image generators, including a new offence concerning AI models optimised to create CSAM. The UK approach is preventive because it targets the technological infrastructure that enables offenders to generate abuse material, rather than focusing only on the final act of possession, publication, or transmission. It also recognises that AI-generated CSAM may involve real children’s likenesses, may normalise child sexual abuse, and may increase the volume of harmful material available online. India may consider a similar approach by criminalising the creation, adaptation, possession, supply, or distribution of AI models or tools specifically designed or optimised to generate CSAM. Such a reform would complement the existing POCSO Act and IT Act framework by addressing the source of AI-generated abuse. However, any such provision should be carefully drafted to avoid penalising legitimate cybersecurity research, safety testing, victim-identification work, or authorised law-enforcement activity.
- **AI for protection of children:** EU’s AI Act can be referred to, to frame strict compliance mechanism for AI to prevent AI bias so that AI can be effectively used for protecting children from abuse.

X. CONCLUSION

1. **Child’s right to privacy:** India is one of the few countries that has a dedicated personal data protection legislation. It offers commendable protections on paper. However, there are certain lapses.

- **Emphasis on self-declaration:** Under DPDPA sec 9, verifiable consent of the child's parent is essential for processing the child's data. However, this puts the onus on the child for self-declaration of age especially for social media. With immense amount of peer pressure and the fear of being left out, there are high chances that a child may misrepresent their age. Apart from this, there is no dearth of cases where parents themselves have facilitated their child to be a part of social media in order to seek celebrity status for their children. This weakens the safeguards provided sec 9 of DPDPA Act, 2023.
- **Exemptions under the Act:** There are broad exemptions explicitly mentioned in Schedule IV (Part A and Part B) with respect to the entities who can and purposes for which, data can be processed without verifiable parental consent under sec 9 of DPDP Act. This might cause some entities to abuse the DPDPA safeguards with impunity.

2. Child right against abuse:

- **No dedicated AI law:** POCSO Act 2012 and IT Act 2000 have provisions to deal with AI generated CSAM and online grooming but they just act as temporary solutions till a dedicated AI Act is enacted. The approach still remains redressal instead of prevention of sexual abuse of children at the hands of offenders using AI.
- **Use of term child pornography in POCSO Act, 2012:** This term further pushes the blame on the survivors and gives CSAM an appearance of lawful and normal content.

3. AI as a tool for child protection:

AI tools have made commendable progress in locating missing children and detecting and removing CSAM online. However, there are concerns of AI working on biased datasets that may cause it to overlook the needs of children from marginalised backgrounds.

XI. REFERENCES

1. Yoshua Bengio et al., *International AI Safety Report 2025* (UK Government / AI Safety Institute, January 2025), available at:

<https://www.gov.uk/government/publications/international-ai-safety-report-2025>.

2. [Justice K. S. Puttaswamy \(Retd.\) & Anr. v. Union of India](#), (2017) 10 SCC 1
3. Ministry of Electronics and Information Technology, Government of India, *Digital Personal Data Protection Rules, 2025*, Gazette of India, 13 November 2025, available at: <https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>. [4] Internet Watch Foundation, "AI becoming 'child sexual abuse machine', warns IWF", available at: <https://www.iwf.org.uk/news-media/news/ai-becoming-child-sexual-abuse-machine-adding-to-dangerous-record-levels-of-online-abuse-iwf-warns>.
4. *Just Rights for Children Alliance v. S. Harish*, 2024 INSC 716.
5. Nilesh Christopher, "OpenAI is huge in India. Its models are steeped in caste bias", *MIT Technology Review*, 1 October 2025, available at: <https://www.technologyreview.com/2025/10/01/1124621/openai-india-caste-bias/>.