

ARTIFICIAL INTELLIGENCE AND DETECTION OF CHILD SEXUAL ABUSE MATERIAL ON THE DARK WEB: LEGAL AND ETHICAL CONCERNS

AUTHOR – S MEHA PRIYADHARSHINI, STUDENT AT SCHOOL OF EXCELLENCE IN LAW, CHENNAI

BEST CITATION – S MEHA PRIYADHARSHINI, ARTIFICIAL INTELLIGENCE AND DETECTION OF CHILD SEXUAL ABUSE MATERIAL ON THE DARK WEB: LEGAL AND ETHICAL CONCERNS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 103-110, APIS – 3920 – 0001 & ISSN – 2583-2344. DOI – <https://doi.org/10.65393/IJLRV6I9I1>

ABSTRACT :

The spread of Child Sexual Abuse Material (CSAM) has greatly grown due to the dark web's and encrypted digital platforms' explosive expansion, posing major problems for law enforcement organisations around the globe. In response, machine learning, picture recognition, predictive analytics, and automated surveillance systems have made artificial intelligence (AI) a crucial technological tool for identifying, tracking down, and stopping online child exploitation. In addition to critically examining the ethical and legal issues of AI-driven surveillance methods, this study looks at how AI can help fight CSAM on the dark web.

The Information Technology Act of 2000, the Protection of Children from Sexual Offences Act of 2012 (POCSO), and pertinent international documents like the Budapest Convention on Cybercrime and the Convention on the Rights of the Child are evaluated in this paper. In view of Justice K. S. Puttaswamy v. Union of India, it dig deeper into constitutional issues of privacy, proportionality, algorithmic bias, and accountability. The study comes to the conclusion that while AI improves efforts to detect cybercrime and protect children, strong legal protections, judicial supervision, transparency, and ethical governance are necessary to strike a balance between child safety and fundamental rights and digital freedoms.

INTRODUCTION

Artificial intelligence (AI) has significantly changed the investigation and prevention of cybercrimes, particularly the detection of Child Sexual Abuse Material (CSAM) on the dark web. Operating through encrypted networks such as Tor, the dark web provides users with anonymity and has developed into a platform for the distribution of illegal information, especially that which exploits minors. The increasing use of CSAM poses serious challenges for law enforcement agencies, as normal cyber investigation methods are often ineffective against encrypted and decentralized Internet platforms. Governments and tech companies have employed AI-based solutions, such as

machine learning algorithms, picture recognition systems, and hash-matching tools, to discover, track, and remove exploitative content from digital platforms." These technologies strengthen child protection measures and increase the efficiency of cyber investigations; however, their use also raises challenging moral and legal questions regarding monitoring, accountability, and privacy.

The primary laws that control online child exploitation in India are the Information Technology Act of 2000 and The Protection of Children from Sexual Offences Act of 2012 (POCSO). Section 67B of the Information Technology Act prohibits the publication,

transmission, or viewing of content that depicts children acting in a sexually explicit manner. Additionally, Section 69A grants the government the power to impose restrictions on Internet content to maintain public order and national security. However, the employment of AI-driven surveillance technology may violate the right to privacy protected under Article 21 of the Constitution, as stated in Justice K. S. Puttaswamy v. Union of India. The absence of defined safeguards and judicial control in AI-based monitoring systems raises concerns regarding algorithmic prejudice, mass espionage, and exploitation of personal data. Therefore, even though AI is an effective strategy to combat CSAM on the dark web, a balanced regulatory framework is necessary to ensure the safety of children without compromising constitutional freedoms and digital human rights.

RESEARCH OBJECTIVES

1. To examine the role of Artificial Intelligence in detecting and preventing the circulation of Child Sexual Abuse Material (CSAM) on the dark web.
2. To analyze the legal framework governing online child sexual exploitation under Indian and international cyber law.
3. To study the effectiveness of AI-based technologies, such as machine learning, image recognition, and automated surveillance systems, in identifying CSAM.
4. To evaluate the constitutional and human rights concerns arising from AI-driven monitoring and surveillance mechanisms.

SCOPE OF STUDY

This study focuses on using AI technology to identify Child Sexual Abuse Material (CSAM) that is distributed through encrypted digital networks and dark web platforms. This study mainly examines the ethical and legal ramifications of AI-driven monitoring systems that governments, law enforcement, and tech corporations use to stop online child exploitation. The Information

Technology Act of 2000, the Protection of Children from Sexual Offences Act of 2012 (POCSO), Article 21 of the Constitution of India's privacy protections, and pertinent international agreements such as the United Nations Convention on the Rights of the Child and the Budapest Convention on Cybercrime are all examined.

Algorithmic bias, mass surveillance, accountability, transparency, and potential misuse of AI technologies are among the ethical concerns explored in this study. It also examines the jurisdictional and evidentiary difficulties pertaining to international cybercrimes committed over anonymous darknet networks. Comparative references to international regulatory techniques employed in nations, including the United States, the European Union, and the United Kingdom, are provided to understand international patterns in the fight against CSAM.

This doctrinal and analytical study cites statutes, judicial decisions, international agreements, policy papers and scholarly publications. This study is limited to the ethical and legal elements of AI-based CSAM detection and excludes technical coding and the forensic use of AI systems.

UNDERSTANDING THE DARK WEB AND CHILD SEXUAL ABUSE MATERIAL

The phrase "dark web" refers to a secret portion of the internet that operates over encrypted networks and is not reachable via conventional search engines. Unlike the publicly accessible surface web, the dark web conceals users identities and whereabouts using anonymity-based technologies such as The Onion Router (Tor). Despite its legal uses for freedom of expression and privacy protection, the dark web has also been exploited by a number of unlawful organizations, including drug trafficking, arms smuggling, cyber fraud, and the distribution of Child Sexual Abuse Material (CSAM). Criminals can distribute exploitative content without being caught by traditional law enforcement

techniques because encrypted communication systems provide anonymity.

Child sexual abuse material is any visual, digital, or computer-generated material that depicts children being sexually exploited or mistreated. The rapid expansion of CSAM's internet circulation has been facilitated by peer-to-peer sharing methods, covert darknet forums, and technological advancements. Every act of watching, disseminating, or copying such content encourages psychological trauma and exploitation, causing child victims to suffer continuously. Children are protected from sexual exploitation worldwide by Article 34 of the United Nations Convention on the Rights of the Child, which mandates that states forbid exploitative sexual actions involving minors. The Information Technology Act, 2000, makes it illegal to publish, browse, download, or transmit content that shows youngsters engaging in sexually explicit behavior or activity via electronic means (Section 67B). Similarly, child pornography and online sexual exploitation are subject to severe penalties under the Protection of Children from Sexual Offences Act, 2012 (POCSO).

Because criminals frequently use encrypted technologies to operate across international borders, the dark web poses serious jurisdictional and investigative challenges. Consequently, to identify and track CSAM networks, governments and cybercrime organizations are increasingly depending on AI-based technology. However, these surveillance methods also raise ethical and legal questions about digital rights, privacy, and the abuse of automated monitoring systems.

ARTIFICIAL INTELLIGENCE TECHNOLOGIES USED IN CSAM DETECTION

To stop the online spread of Child Sexual Abuse Material (CSAM), artificial intelligence (AI) has become a crucial technological tool. This is especially true for encrypted dark web platforms, where traditional cyber investigative methods are frequently unsuccessful. AI-based systems detect, categorize, and track exploitative digital information across Internet networks using

machine learning algorithms, image recognition technologies, natural language processing (NLP), and predictive analytics. These technologies increase the speed and precision of cyber investigations while enabling law enforcement and digital intermediaries to identify large amounts of illicit content in real time. Hash-matching software, such as Microsoft's PhotoDNA, is one of the most commonly used methods. It transforms photographs into distinct digital signatures to recognize previously known CSAM, even when the images are scaled or altered. Similarly, AI-driven web crawlers can search peer-to-peer networks, encrypted marketplaces, and darknet forums for questionable patterns, phrases, and metadata related to child exploitation.

Machine learning models are increasingly being trained to identify abusive visual content using automated image classification and facial identification systems. By examining online discussions, covert chat rooms, and coded language frequently used by criminals on the dark web, natural language processing technology further aids investigators. Additionally, by analyzing behavioral patterns and digital traces, predictive AI systems assist cybercrime agencies in identifying possible criminals and trafficking networks. AI-supported forensic tools have been implemented by organizations such as Europol and INTERPOL to improve international collaboration in the detection of online child exploitation crimes.

The use of AI algorithms for CSAM detection presents significant ethical and constitutional issues. In light of the Supreme Court's recognition of privacy as a fundamental right in Justice K. S. Puttaswamy v. Union of India, automated surveillance technologies may conflict with the right to privacy protected by Article 21 of the Indian Constitution. Furthermore, using AI to scan digital communications could lead to algorithmic bias, false positives, and excessive state surveillance, which could result in unfair investigations and human rights violations. Authorities can monitor and limit internet content involving child sexual exploitation under

Sections 67B and 69A of the Information Technology Act, 2000. However, questions about proportionality and abuse of surveillance capabilities are raised by the lack of clear accountability procedures and judicial oversight in AI-driven monitoring systems. Consequently, even while AI technologies greatly aid in the fight against CSAM on the dark web, their use needs to be controlled by strong legislative safeguards that strike a balance between child safety, constitutional rights and moral values.

LEGAL FRAMEWORK GOVERNING CSAM AND AI SURVEILLANCE

1. International Legal Framework

The proliferation of Child Sexual Abuse Material (CSAM) through dark web networks and encrypted digital platforms has forced many countries to implement more robust legal and technological measures to prevent online child exploitation. States are required by a number of international agreements and treaties to prevent and prosecute child sexual abuse in cyberspace. State parties are required under Article 34 of the United Nations Convention on the Rights of the Child to protect children from all forms of sexual exploitation and abuse, including exploitative pornographic performances and materials. Similarly, states are required by the Optional Protocol on Sale of Children, Child Prostitution, and Child Pornography to make it illegal to produce, distribute, or possess child pornography via digital means.

One of the important international agreements addressing cybercrimes involving CSAM is the Budapest Convention on Cybercrime, ratified by the Council of Europe. Article 9 of the Convention expressly requires Member States to criminalize child pornography committed via computer systems. To combat online child exploitation networks, international organizations such as INTERPOL and Europol have come together to support cross-border collaboration, intelligence sharing, and digital forensic investigations.

International enforcement methods have been reinforced by the development of Artificial

Intelligence (AI)-based surveillance systems. AI tools that use facial recognition, machine learning, and predictive analytics help law enforcement identify and track CSAM in encrypted online environments.

2. Indian Legal Framework Governing CSAM

The Information Technology Act of 2000 and the Protection of Children from Sexual Offences Act of 2012 (POCSO) are the primary laws governing CSAM and cyber surveillance in India. The Information Technology Act, Section 67B, makes it illegal to publish, transmit, browse, download, or possess electronically stored sexually explicit content featuring children. Additionally, the clause forbids the facilitation of abusive digital content and the enticing of minors on the internet. In addition, Section 69A gives the Central Government the authority to restrict public access to Internet content for the sake of public order, sovereignty, and the avoidance of crimes that can be prosecuted. Together, these clauses provide legal power for CSAM-related material restrictions and digital monitoring.

Sections 13, 14, and 15 of the POCSO Act, 2012 criminalize child pornography and online sexual exploitation, adding to the protections provided by cyber law. Additionally, the Bharatiya Nyaya Sanhita (BNS), 2023, and the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, enforce procedures pertaining to electronic evidence and cyber investigations. Additionally, social media platforms and intermediaries are required by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, to remove illegal content and assist law enforcement. In particular situations involving sexual offences against children, Rule 4 expressly requires major social media intermediaries to perform due diligence and activate tracing systems.

However, automated monitoring systems and AI-based surveillance present constitutional issues under Article 21 of the Indian Constitution. The Supreme Court acknowledged privacy as a basic right in Justice K. S. Puttaswamy v. Union of India and ruled that any restrictions on privacy

must meet the requirements of necessity, proportionality, and legality. Therefore, excessive digital monitoring using AI-powered systems may violate constitutional guarantees if carried out without judicial oversight, procedural safeguards, or clear accountability procedures.

3. Legal Issues in AI Surveillance

The use of AI algorithms to identify CSAM raises serious legal issues regarding intermediary liability, surveillance, and the dependability of the evidence. Large-scale data scanning, metadata analysis, and automated content filtering are frequently used by AI-driven systems, which may lead to widespread surveillance and violations of personal privacy rights. Algorithmic bias, false positives, and erroneous investigations can result from the use of facial recognition technologies and predictive policing systems. These concerns are more pertinent when automated systems function without human oversight or sufficient transparency.

In *Shreya Singhal v. Union of India*, the Supreme Court stressed that limitations on digital liberties must continue to be constitutionally sound and narrowly circumscribed. In a similar vein, the Court emphasized procedural protections against arbitrary surveillance and phone interception in *People's Union for Civil Liberties v. Union of India*. In the context of AI-based cyber monitoring systems that can continuously monitor online activity, these concepts are becoming increasingly important.

Therefore, even while AI technologies greatly increase governments' and law enforcement agencies' abilities to battle CSAM on the dark web, the legislative framework controlling these technologies must guarantee proportionality, accountability, transparency, and protection of constitutional rights. In a dynamic cyber ecosystem, a balanced regulatory model is required to balance child protection goals with privacy rights, freedom of expression, and digital civil liberties.

LEGAL CHALLENGES IN AI-BASED DETECTION OF CSAM

1. Privacy and Surveillance Concerns

The use of artificial intelligence (AI) in the detection of Child Sexual Abuse Material (CSAM) has significantly improved law enforcement agencies capacity to monitor illegal online activity on the dark web. AI-powered technologies, such as machine learning algorithms, automated picture identification, predictive analytics, and metadata analysis, enable authorities to swiftly and efficiently uncover dubious digital information. However, new technologies also raise important legal issues regarding privacy and state spying. AI-based surveillance systems, which often involve extensive scanning of private communication, cloud storage, and encrypted digital platforms, may breach the right to privacy, which is guaranteed under Article 21 of the Indian Constitution. The Supreme Court of India has acknowledged privacy as a basic right in *Justice K. S. Puttaswamy v. Union of India*, holding that any state action that violates privacy must meet the requirements of necessity, proportionality, and legality, unlimited AI surveillance without procedural constraints may result in excessive government intrusion into private digital areas and breach constitutional protections.

For cybersecurity and public safety reasons, the Information Technology Act of 2000 gives the government the authority to monitor and intercept online communications under Sections 69 and 69B. However, detractors contend that the combination of AI technology and extensive surveillance powers could promote widespread monitoring and erode civil freedom. Concerns about arbitrary state action and the exploitation of people's personal data are raised by the absence of judicial control and transparency in AI-based monitoring systems.

2. Jurisdictional and Evidentiary Challenges

The international dimension of cybercrime is one of the main legal challenges in the fight against

CSAM on the dark web. Anonymous networks, encrypted systems, and foreign servers situated outside home jurisdictions are common tools used by criminals. This makes it extremely difficult to investigate, extradite, and enforce criminal law. International agreements, such as the Budapest Convention on Cybercrime, promote international collaboration in cybercrime investigations, although effective prosecution is frequently hampered by uneven local laws and disparate standards of digital evidence.

In criminal processes, AI-generated evidence raises evidentiary issues. Because of algorithmic flaws or erroneous datasets, automated systems may mistakenly classify legal information as illegal. False positives produced by image classification or facial recognition systems could result in unfair investigations and damage to a person's reputation. Before being allowed in court, electronic evidence must meet the requirements for validity and dependability under the Bharatiya Sakshya Adhiniyam, 2023. Courts must carefully consider whether AI-generated outputs can be regarded as trustworthy evidence in the absence of human verification. The "black-box problem," which is the lack of explainability in many AI systems, makes the judicial review of automated decisions more difficult.

3. Intermediary Liability and Accountability

AI-based CSAM detection also raises concerns about technology companies and intermediaries responsibilities. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate that social media platforms and digital intermediaries take reasonable steps to eliminate illegal content related to child exploitation. In some situations, Rule 4 requires major social media intermediaries to facilitate the identification of the initial source of illegal content to be identified. Although these regulations improve online protection of children, they can be at odds with end-to-end encryption and users' right to privacy.

In *Shreya Singhal v. In the Union of India*, the Supreme Court stressed that limitations on digital freedom must continue to be narrowly targeted and legally justifiable. To avoid legal liability, platforms may be forced to engage in excessive filtering or intrusive surveillance due to excessive intermediary requirements. Furthermore, if faulty algorithms result in discriminatory or illegal outputs, AI developers and law enforcement organizations may also have to deal with accountability issues. Therefore, transparent regulatory norms, independent oversight systems, and human supervision in AI-assisted cyber investigations are urgently needed.

Therefore, although AI technologies greatly aid in the fight against CSAM on the dark web, the legal system must strike a balance between efficient law enforcement, procedural justice, constitutional protections, and the defence of digital rights.

ETHICAL CONCERNS IN AI-DRIVEN DETECTION SYSTEMS

1. Privacy, Surveillance, and Human Rights

The use of artificial intelligence (AI) in the detection of child sexual abuse material (CSAM) raises significant ethical questions about privacy, digital autonomy, and human rights. AI-driven detection systems frequently use automated scanning of cloud storage, encrypted digital platforms, online chats, and metadata to identify suspicious activities linked to child exploitation. These technologies increase the effectiveness of child protection and cybercrime investigations, but they also increase the risk of excessive surveillance and privacy invasion by the state. The ethical concept of informational self-determination, which maintains people's autonomy over their personal information and conversations, may be compromised by ongoing digital surveillance by governments or private tech firms."

In India, the ethical legitimacy of AI surveillance must be examined in light of the constitutional protections under Article 21 of the Indian

Constitution. In Justice K. S. Puttaswamy v. In the Union of India, the Supreme Court emphasized that privacy is an essential component of human dignity and personal liberty. Therefore, the indiscriminate deployment of AI surveillance technologies without proportional safeguards may lead to ethical violations of individual freedom and democratic accountability. Moreover, AI-driven monitoring systems may disproportionately affect vulnerable communities and create a chilling effect on freedom of expression and online participation.

2. Algorithmic Bias and False Positives

This is another major ethical concern related to algorithmic bias and inaccuracies in AI-generated decisions. AI systems function on the basis of datasets and machine learning models that may contain inherent biases or incomplete information. Consequently, automated detection systems may incorrectly classify lawful content as CSAM or wrongfully identify innocent individuals as such. Facial recognition tools (FCT) and predictive algorithms are particularly vulnerable to false positives, leading to reputational harm, unlawful investigations, and violations of due process rights.

The lack of transparency in many AI systems, often referred to as the "black-box problem" makes accountability even more difficult because those affected by automated judgements frequently do not understand how those decisions were made. Therefore, AI-assisted investigations must continue to be subject to human oversight and court review in accordance with the ethical norms of fairness, explainability, and accountability. The Supreme Court in Shreya Singhal v. The Union of India stated that limitations on digital liberties cannot be arbitrary or ambiguous. The same logic holds for AI-powered content moderation systems that can unduly restrict acceptable online speech.

3. Accountability and Ethical Governance

Governments, law enforcement, and tech businesses must have clear accountability

procedures in place for the ethical application of AI in CSAM detection. As required by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, digital intermediaries are increasingly employing AI-powered moderation systems to detect and eliminate exploitative content. But an over-reliance on automated moderation could lead to over-censorship and the deterioration of encrypted communication systems. Therefore, transparent regulatory frameworks, independent monitoring, recurring algorithmic audits, and safeguards against the abuse of surveillance authorities are all necessary for ethical governance.

While AI technologies offer strong tools to combat CSAM on the dark web, ethical concerns necessitate a balanced strategy that protects children's rights without sacrificing fairness, privacy, human dignity, or constitutional freedoms.

RECOMMENDATIONS AND SUGGESTIONS

A balanced regulatory framework that protects children while upholding ethical standards and constitutional rights is required due to the growing usage of Artificial Intelligence (AI) in identifying Child Sexual Abuse Material (CSAM) on the dark web. Mandatory human monitoring of AI-assisted investigations is one of the most important recommendations. Automated technologies should only be used as auxiliary tools; human verification and judicial review are required for any final decisions pertaining to criminal prosecution, content removal, or monitoring. This is crucial to stop erroneous enquiries brought on by algorithmic bias or false positives. According to the proportionality concept, which was highlighted in Justice K. S. Puttaswamy v. Union of India, digital monitoring methods must continue to be required, reasonable, and legally responsible.

Government should also establish more stringent accountability requirements and transparent AI auditing procedures for the law enforcement organisations and tech firms using AI surveillance technologies. Algorithms may be

routinely examined by an independent regulatory bodies to guarantee their fairness, explainability, and adherence to privacy regulations. To reduce needless interference with private conversations, privacy-preserving technology like limited-data access systems and encrypted AI processing should be promoted. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 could be improved by adding more explicit procedural protections and transparency requirements for intermediaries conducting CSAM-related investigations.

CONCLUSION

The increasing prevalence of Child Sexual Abuse Material (CSAM) on the dark web has become a significant challenge for this modern legal systems and cybercrime enforcement agencies. Artificial Intelligence (AI) has become an important technological tool in identifying, tracing, and preventing the dissemination of exploitative digital content through automated detection systems, machine learning algorithms, and predictive analytics. Although AI improves the efficiency of cyber investigations and strengthens child protection mechanisms, its deployment also raises a serious legal and ethical concerns relating to privacy, surveillance, algorithmic bias, and accountability. The constitutional principles mentioned in Justice K. S. Puttaswamy v. Union of India emphasise the need to strike the balance between individual liberties and fundamental rights and state surveillance. As a result, an efficient regulatory structure must guarantee proportionality, judicial supervision, and openness in AI-driven investigations. To deal with CSAM while upholding democratic ideals and digital civil liberties, a balanced strategy incorporating technological innovation, international cooperation, and human rights safeguards are necessary.

REFERENCE

1. Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (Melville House Publ'g 2015).
2. Luciano Floridi, *The Ethics of Information* (Oxford Univ. Press 2013).
3. Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publ'g Grp. 2016).
4. Hany Farid, *PhotoDNA: A Technological Approach to Combating Child Pornography*, Dartmouth Coll. Res. Papers (2016).
5. Information Technology Act, No. 21 of 2000, Sec 67B, 69A, INDIA CODE (2000).
6. Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 13–15, INDIA CODE (2012).
7. Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Sec 61–63, INDIA CODE (2023).
8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, Part II, sec. 3(ii) (Feb. 25, 2021).
1. Convention on the Rights of the Child art. 34, Nov. 20, 1989, 1577 U.N.T.S. 3.
2. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227.
3. Convention on Cybercrime art. 9, Nov. 23, 2001, E.T.S. No. 185.
4. Justice K. S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
5. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).