ARTIFICIAL INTELLIGENCE GENERATED CHILD SEXUAL ABUSE MATERIAL (CSAM): A LEGAL VIEW

Parth Malhotra, LL.M., Jamia Millia Islamia, New Delhi

ABSTRACT

There has been a revolution in digital content creation, and AI has also intensified the development of AI-generated Child Sexual Abuse Material (CSAM), a type of exploitation that is not based on the actual abuse of children but perpetuates it, endorses deviant behaviour, and indirectly leads to the harm experienced by the real world. In this paper, the critical analysis of the legal, procedural, and ethical gaps in dealing with AI-generated CSAM is presented with a particular focus on Indian law and some parallels to the international law. The research highlights the weaknesses of the existing frameworks and the urgent necessity to reform with the help of judicial analyses and international views. The paper promotes the clear legislative guidelines that criminalize the AI-created CSAM, empowered cyber forensic capacities, law enforcement preparatory and co-ordinated global legal adjustment. The paper suggests a holistic approach to the fight against synthetic child sexual exploitation, which would help to preserve the legal system at the ability to protect children in the ever-changing digital environment.

Keywords: CSAM (Child Sexual Abuse Material), Artificial Intelligence (AI), Sexual Abuse, Child

Introduction

The sexual abuse of children material (CSAM) has always been known as one of the worst criminal content spread in the digital realm. Historically, the term CSAM has been used to refer to any expression of minors involved in sexually explicit activities in images, videos or text. With the emergence of artificial intelligence, many changes occurred which totally altered the paradigm of how this material is produced, distributed and consumed. Nowadays, AI based tools, such as generative adversarial networks (GANs), diffusion models and deepfake technologies are able to create hyper-realistic images and videos of a child without any real child being involved[1]. It has been a point of deep discussions in criminal jurisprudence, human rights and regulation of cyberspace since the traditional limits of victimhood, exploitation and guilt are challenged as never before.

Firstly, AI-created CSAM might not seem as harmful as traditional forms of abuse image since there is no physical exploitation of a child involved in its creation. However, academics, child protectionists and law enforcers hold the view that the risks are still acute. This material may legitimize abusive fantasy and end up stimulating demand on actual CSAM and lead to a culture of child abuse. Moreover, in the case of victims whose likenesses are reproduced in AI-generated pictures are not with their permission, the damage is very personal and devastating.

Lack of unified and standardized legal frameworks across the jurisdictions increases the difficulty. Although some nations have started to criminalize AI-generated CSAM based on specific provisions like the United States and the United Kingdom. While the others do not have specific laws which results into loopholes in prosecution and transnational enforcement issues. International agencies such as Interpol and Europol have sounded the alarm over the increased menace but the international community is divided[2]. It is on this background that there is need to investigate whether the available legal tools are sufficient or not and how the reforms can be developed in a manner that allows a balance between the civil liberties, technological innovation and the protection of children interests.

[1]Internet Watch Foundation, AI-Generated Videos of Child Sexual Abuse: A Stark Vision of the Future, https://www.iwf.org.uk/news-media/news/ai-generated-videos-of-child-sexual-abuse-a-stark-vision-of-the-future/ (last visited Sept 15, 2025)

[2]Europol, AI-Generated Child Sexual Abuse Material: Combating the Growing Threat, https://www.europol.europa.eu/media-press/newsroom/news/ai-generated-child-sexual-abuse-material-combating-growing-threat (last visited Sept 15, 2025)

The artificial intelligence has presented a new horizon of creativity, innovation and solution, but it has also led to the darker sides that has threatened the very existence of human dignity. One of them is the development of child sexual abuse content by artificial intelligence that can create images, videos or audio recordings that can convincingly portray children in a sexual situation. This content is not always based on real-life abusive experiences rather it is artificially generated by the use of algorithms that are trained on massive amounts of pictures, frequently scraped off the internet without the user's approval. Generative adversarial networks (GANs) and diffusion-based models are the most popular in this respect and both can be used to manipulate the inputs of data to produce hyper-realistic results. The threatening fact is that even fake content is usually difficult to distinguish as real photographs or video recordings making it hard to spot and take action[3].

After being trained, such systems are able to generate fake images of minors who are sexually active but never in real life. The technologies of deepfake enable to overlay a child face on adult pornography which means that there's a text that claims to depict a particular minor in an abusive situation. On the same note, text to image generators, which gained popularity over the last few years can generate explicit images of fictional or non-existent children just by simply describing them. The availability of such tools implies that anybody who is not highly technical can now use it to produce CSAM with little work, creating a shadow economy of demand and distribution.

The classical concept of child abuse pre-supposes that the real children are working on the physical level and synthetic abuse material causes harm both directly and indirectly. First, children whose likenesses have been stolen into deepfake pornography are indirect victims, because their reputations suffer long-term traumatic and stigmatising consequences. Although no real child is presented, the content is extremely dangerous to the society in terms of normalizing and justifying abusive fantasies. The study in criminology suggests that the use of artificial abuse material is able to reduce the inhibitions, intensify the offending behaviour and influencing the tendency of the user to pursue the actual CSAM[4]. By doing so, AI created content can serve as a kind of access point to additional exploitation, making it hard to

[3]Stanford Internet Observatory, Investigation Finds AI Image Generation Models Trained on Child Abuse, https://reap.fsi.stanford.edu/news/investigation-finds-ai-image-generation-models-trained-child-abuse (last visited Sept 15, 2025)

[4]Michael Salter, *Deepfakes and Synthetic Child Sexual Abuse Material: Policy Challenges and Responses*, 13 J. Child Sexual Abuse 1 (2023), https://onlinelibrary.wiley.com/doi/full/10.1002/cri2.66.

distinguish fantasy and reality on the side of offenders.

The fact that the amount of content flowing on the dark web and encrypted networks is enormous and places law enforcement agencies in enormous challenges of detecting and removing traditional abuse imagery. The growth of AI-generated content compounds this pressure by providing content that will not be classified as CSAM in existing legal jurisdictions and thus will not be prosecuted. In addition, the sheer realism of synthetic images poses evidentiary issues in court because it is hard to determine whether the content is artificial or represents real abuse. This does not only hamper prosecutions but also increases chances of wrongful accusations and miscarriage of justice.

Psychologically, the commodification of children bodies continues with the AI-generated CSAM, even in its imaginary character. It supports exploitative discourses that perceive children as objects of sex and thus solidifies unhealthy gender and power relations. According to scholars the acceptance of such material, even in synthetic levels is a failure to uphold the moral and legal obligation of safeguarding the rights of children under the international agreements of protecting the rights of children like the United Nations Convention on the Rights of the Child[5]. Therefore, although the material might not necessarily have a specific, recognizable victim but the damage it inflicts on the society is indisputable.

Existing Legal Frameworks on AI-Generated CSAM

The rapid development of AI-created child sexual abuse images has made legal systems worldwide to deal with the questions which were never meant to be answered by the traditional criminal laws. The majority of the laws on child protection were written during the times when the CSAM was perceived by photographs, videos or written descriptions of the true abuse. The main assumption in such laws was that there was a known child victim with the exploitation which could be proved directly. In case of synthetic CSAM, the lack of an actual victim makes the situation more complicated and it is difficult to find out answer to the question that: is it criminal when no physical child was damaged yet the content of the material is a clear description of child abuse? The jurisdictions have dealt with this dilemma in patchy manner,

[5] Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

resulting in a patchwork of legal strategies that offenders can use[6].

On the global level, the United Nations Convention on the Rights of the Child (CRC) requires countries to ensure that children are not exposed to sexual exploitation and abuse. Although the CRC is older than artificial intelligence, its general adherence has been re-read by child rights organizations to encompass the use of synthetic content that sexualizes children, based on the premise that such content will support negative attitudes and enable exploitation[7]. There is also the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (2000) which defines child pornography as any form of representation by whichever means, of any child taking part in real or simulated explicit sexual acts. The term simulated was added in an effort to include computer generated or morphed images, although the language is subject to discussion[8]. There is a view that AI-generated CSAM is categorically classified as simulated, whereas it is also claimed that the absence of an actual victim is what renders it uncovered by the Protocol. This ambiguity has made it difficult to have global consensus.

In the United States, the law is most significantly given in the PROTECT Act of 2003 that criminalized computer-generated images where children are involved in sexually explicit acts provided that the image is indistinguishable to actual children[9]. This was established under a U.S Supreme Court case, which invalidated previous regulations which prohibited the virtual child pornography using the First Amendment rights. The Court had ruled that fictional descriptions that did not depict real minors were a category of speech which was protected[10]. Although this framework does represent AI generated CSAM in most instances, it has loopholes: hyper-stylized or cartoonish representations can get away with criminalization, and First Amendment obstacles can be a thorn in the flesh.

The United Kingdom has been more liberal in the Coroners and Justice Act 2009 that criminalizes possession of prohibited images of children. This definition extends beyond the photographs and video of real minors, to include computer-generated or non-photographic images, which, in turn, are pornographic, grossly shocking, or offensive[11]. Notably, there is no

[6] Sarah E. Ullman, *Artificial Child Sexual Abuse Material and the Law: Criminalization Without a Victim?* 45 Child Abuse & Neglect 1 (2023), https://doi.org/10.1016/j.chiabu.2023.106236.
[7] Convention, *supra* note 5, at 4
[8] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, G.A. Res. 54/263, 2171 U.N.T.S. 222, arts. 2–3.
[9] PROTECT Act of 2003, No. 18 U.S.C. §§ 2251–2260.
[10] Ashcroft v. Free Speech Coalition, 535 U.S. 234, 255–56 (2002).
[11] Coroners and Justice Act 2009 § No. 25, 62–63 (U.K.)

need of a real child in the law thus sealing a significant loophole. The prosecutions that have been carried out based on the provision have been effective in prosecuting people with AI created material about child abuse, making the UK appear to be among the more aggressive jurisdictions in combating synthetic CSAM.

European Union has realized the challenge as well. The EU Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography defines child pornography in a broadly understood way in which it refers to realistic images of a child that does not exist[12]. Member states are thus bound to criminalize AI-generated CSAM but with differing degrees of implementation. Other states, including Germany and France have gone ahead to adopt stringent policies toward synthetic abuse imagery, whereas other states continue to use outdated definitions that consider only real victims as narrow. Diffusion of the enforcement has led to cross-border loopholes in the EU, which offenders have used.

Going to India, the legal regulatory framework remains immature at best and it has not yet adequately prepared to handle the complications of AI-generated CSAM. Protection of Children from Sexual Offences (POCSO) Act, 2012 makes it a crime to use children to produce pornographic material and distribute, possess, or even create such material. The Act, however, is phrased in such a way that it assumes the presence of a real child and it is unclear whether the synthetic or AI-generated content would be subject to the Act[13]. The Information Technology Act, 2000, and especially, Section 67B, forbids the publishing or transmission of material representing children in sexually explicit acts, but it is once again with reference to actual depictions[14]. The case involving AI-generated CSAM has never been squarely addressed by the Indian courts, which creates the possibility that criminals can use the gap in the definition. Although the Indian government has implemented measures to enhance cyber-policing and make declarations on content takedown, the lack of clear statutory provisions on synthetic abuse imagery is a gaping hole of the existing structure.

In addition to domestic systems, other organizations like INTERPOL and Europol have given warnings over the spread of AI created CSAM, and its challenges to digital forensics. The conventional approaches to the identification of victims that are based on the search of real children in the image become useless in the case when the content is totally synthetic. This

[12] *Id*. at 5
[13] The Protection of Children from Sexual Offences Act, No. 32, Acts of Parliament, 2012(India).
[14] The Information Technology Act, § 67B, No. 21, Acts of Parliament, 2000 (India)

does not only frustrate the process of finding the offenders but it also gives the investigators a lot of unclear contents to handle. Mechanisms of international cooperation, e.g. the Budapest Convention on Cybercrime, offer the cross-border mechanism of cooperation, but is not specific to synthetic content.

Global Trends and Comparative Approaches

The problem of AI-generated Child Sexual Abuse Material (CSAM) is global in nature, transcending the borders of any one country, and thus requires a comparative perspective to understand how different jurisdictions are responding to this emerging threat. Global trends demonstrate that while certain developed jurisdictions, particularly within the European Union, the United States, and Australia, have begun to address the challenges posed by AI enabled CSAM, many other nations are still grappling with outdated legal frameworks[15]. These differences result in an uneven global response, thereby creating safe havens for cybercriminals operating through AI-driven technologies.

The General Data Protection Regulation (GDPR) and the Digital Services Act (DSA) have been the most influential policy responses in the European Union as they aim at holding technology platforms accountable. The EU has been especially active in placing child abuse content, such as imagery generated with the help of generative technologies, in the context of a duty imposed on service providers to spot and eliminate it. Besides, Europol has been actively involved in keeping track of emerging threats and made warnings of the possible abuse of AI to deepfakes and artificial child pornography. The fact that the EU acknowledged that even non-physical, computer-generated CSAM is psychologically injurious and exacerbates the abuse cycle is a good move in solving the issue[16].

In contrast, The United States has taken a great advantage of the current system of the PROTECT Act, 2003, and the federal Child Pornography Prevention Act (CPPA), 1996. Courts have contended over the constitutionality of outlawing virtual child pornography in which no real child is shown as a precaution between the right to free speech under the First Amendment

[15] Childlight Global Child Safety Institute, Action Needed to Close Legal Gaps on AI-Generated Child Sexual Abuse Material (Dec. 31, 2024), https://www.childlight.org/newsroom/action-needed-to-close-legal-gaps-on-ai-generated-child-sexual-abuse-material.

[16] Europol, Europol warns of rise in AI child abuse imagery, DW (Sept. 21, 2025), https://www.dw.com/en/europol-warns-of-rise-in-ai-child-abuse-imagery/a-69733974

and the urgent state interest to safeguard children[17]. The landmark case Ashcroft v. A case in point of this tension is Free Speech Coalition (2002), which the U.S. Supreme Court invalidated the provisions of the CPPA, which aimed to criminalize so-called virtual child pornography, due to being overly broad. Nevertheless, due to the emergence of AI and the creation of realistic synthetic images, this issue has been revived, and policymakers wonder if additional laws should be enacted to make AI-generated CSAM unambiguously criminal.

Australia has been stricter with its approach by introducing stipulations under the Criminal Code Act making the possession, dissemination, and production of child abuse material pictorial content, such as computer-generated or manipulated imagery, which seems to be of a child, a crime. This is an appreciation that the harm does not lie only in the participation of actual children but the institutionalization of child exploitation in the society.

In comparison, the legislative environment of India is still maturing. The Information technology act 2000 especially the section 67B criminalizes the publication and transmission of content that shows children in sexually explicit acts. But this was mainly meant to deal with actual imagery, and its extension to the case of AI-generated material has not been explicitly defined. In spite of the fact that the Protection of Children from Sexual Offences (POCSO) Act, 2012 offers a solid framework that could be used to prosecute the crimes against minors, it does not directly consider the synthetic content[18]. Therefore, the Indian law has a gap with regard to AI-generated CSAM.

These international tendencies suggest that there is a split in the strategies: whereas certain jurisdictions are more concerned with the freedom of expression and, therefore, take a more cautious approach, others focus on harm-prevention and criminalize all the kinds of sexual representations of children, both real and artificial. To allow international cooperation, there is an urgent need to equalize legal standards so that offenders will not be able to use the gaps in the jurisdiction. The fact that the trend is made towards its acceptance of AI-generated CSAM as a valid threat to child protection means that the global consensus is shifting, yet it needs further consolidation in the form of treaties, conventions, and cross-border enforcement strategies.

[17] Ashroff, *supra* note 10, at 5.
[18] Information Technology Act, 2000, § 67B, No. 21, Acts of Parliament, 2000, (India)

Legal Loopholes and Challenges in Prosecuting AI-Generated CSAM

The issue of child sexual abuse content generated by AI lies in a grey area of the law in which the technological reality is ahead of the law. Although the ethically incorrect nature of such material might seem self-evident, it is not so easy to criminalize it. The current legislation on child porn was built on the assumption of identifiable children victims and thus a gap is created in the doctrine when there is no real-life child exploitation in the production of a synthetic image. This uncertainty leaves a rich hunting ground to perpetrators to capitalise on loopholes and prosecutors are faced with inconsistent laws, evidentiary limitation and constitutional restriction[19]. It is not just a problem of updating statutory definitions but rather a question of how to balance the free expression and technological innovation against the absolute necessity of protecting children.

The main loophole is connected to the fact that there is no actual victim in AI-generated CSAM. The classical criminal law is based mostly on the concept of harm: a crime cannot occur without the existence of a victim who has been injured or exploited by the act. This is a key aspect of harm that offenders and civil liberties advocate frequently claim synthetic material because that is a fiction[20]. Although later laws attempted to address this loophole, the case demonstrates that there is always a tension: criminalizing the imaginary world risks excessive generality and censorship, but not doing so, it encourages its production and social injuries. Jurisdictions that are still practicing the harm-based definition of CSAM run the risk of exempting synthetic material to prosecution.

A second major loophole is a result of the ambiguities in the definition of statutes. The phrases like child pornography, sexually explicit representation, or indecent image are frequently formulated with actual pictures. This leaves the courts to determine whether synthetic depictions belong to these categories and the result is inconsistent[21]. As an example, the United Nations Optional Protocol refers to any such representation of a child who has participated in explicit conduct, which has been broadly viewed by some states to include AI-generated content, but others have taken a narrow perspective that requires the participation of actual minors. This ambiguity allows offenders to get away with it by claiming that the content is

[19] Jennifer Daskal & Susan W. Brenner, *Technology Outpaces the Law: Legal Responses to AI-Generated Child Exploitation Material*, 102 J. Crim. L. & Criminology 45 (2023).
[20] Claire Andresen, *Artificially Generated, Genuinely Harmful: Prosecuting AI-Generated Child Sexual Abuse*, SSRN (Sep. 22, 2025), https://papers.ssrn.com/sol3/Delivery.cfm/5381736.pdf?
[21] *Id.* at 9.

artificial, especially in those jurisdictions where there are no clear provisions covering synthetic abuse material.

A third difficulty is the constitutional free expression and artistic freedom. Attempting to criminalize fictional or artistic portrayal in the context of liberal democracies is likely to conflict with constitutional or human rights guaranteed through constitutional or human rights instruments. Lawbreakers can make the argument that synthetic CSAM is another type of expression or fantasy and is unpleasant, but it does not deserve to be suppressed by the state. Although child protection is a strong state interest, in many cases it is up to the court to strike a balance between the protection of speech and the protection of children. The risk here being that ill-conceived legislations can be too wide-ranging, and end up criminalizing innocent or legitimate artistic productions that feature youthful characters, or even age-regressed animations, causing them to be accused of over-criminalization. Parliaments thus have the sensitive role of trying to come up with specific statutory language that would focus on exploitative programmed content without actually interfering with the legitimate freedom.

Practically speaking, the problems of prosecution are complicated by the issue of detection and evidences. The use of AI in creating CSAM is becoming more and more difficult to distinguish between artificial and natural images, which poses a significant problem regarding law enforcement. By taking the material of the offenders, the forensic experts can have serious problems with proving that the images are real children or entirely artificial. This uncertainty of evidence is enough to derail prosecution because the defence counsel takes advantage to present doubts and claim that the crime did not take place. On the other hand, the probability of false accusation is also present, as even the rightful yet stylized digital art can be mistaken as CSAM[22]. The courts are not well prepared to answer such very technical questions especially when there are no expert testimony or standardised forensic tools available to analyse the synthetic media.

Worsening this situation is the fact that online distribution is cross-border. Another common way AI-generated CSAM is generated is in a jurisdiction and served on servers elsewhere around the world. Various jurisdictions have different standards on the law, which allows criminals to act with impunity. An example is that a person in a nation where the use of synthetic CSAM has been legalized can send material to nations where it is illegal, and the law

[22] Joanna Bryson, *Challenges in Digital Forensics of AI-Generated Content*, 18 Comput. L. Rev. 77 (2022).

enforcement could not do anything about it, as the principle of double criminality applies in extradition law[23]. Absence of a unified global standards therefore leaves loopholes in jurisdiction that can be used.

The other problem is that there is a psychological and criminological debate regarding synthetic CSAM. There is an opinion that AI-created content can act as a safety valve to abusers and allow them to find a fictional release, avoiding the cruelty of real children. Some have argued that it is a gateway drug, but reduces inhibitions and creates a demand in the real world to abuse substances. The lack of agreement makes the process of justification of criminalization difficult. The legislatures fear implementing stringent punitive actions where the empirical evidence supporting the fact that synthetic content has direct harmful effects is weak, but child protection Activists say that the dangers to the society are too high to neglect. This debate continues to remind us of how hard it is to base reform on sound criminological theory.

Lastly, technological anonymity and the dark web ecosystem prevent the implementation of an enforcement environment. Generative AI applications that create CSAM are becoming more obtainable in encrypted systems and black markets, as well as on open-source repositories. Anything created and distributed by criminals may remain undetected because there is no fear of being detected and it may be through the anonymizing services and networks like VPNs and Tor networks. Prosecutions have challenges in tracking the offenders, admissible digital evidence, and intent even after they have been detected. Due to the fast rate of technological innovation, the enforcement agencies are always lagging behind in a reactive mode rather than proactive mode[24].

Cumulatively, these loopholes and challenges prove that AI-generated CSAM is under consideration by current legislation. The lack of an actual victim, the lack of definition, the clash of the freedom of speech, the dilemma of the evidence, and the failure to enforce across borders all contribute to the situation when the criminals are left to act with relative impunity. Such a legal void does not only weaken the effort of child protection, but also destroys the faith of the people in the ability of the law to counter the technological threat. The need to reform is thus very clear but reform needs to be well judged in such a way that does not overstep but puts potential means of exploitation to a close decisively.

[23] *Id.* at 10.
[24] Brian Krebs, *The Dark Web and Cybercrime Enforcement Challenges*, 21 Cybersecurity L. Rev. 101 (2021).

Among the most challenging issues when dealing with AI-based Child Sexual Abuse Material (CSAM), the situation does not only have to do with the issue of defining its legal position but also the enforcement of the existing or newly developed legislation. Law enforcement in the digital sector, especially the one that uses artificial intelligence and machine learning as the facilitating factors, is burdened with a mess of technical, legal, and jurisdictional challenges, which in many cases restrict the efficiency of national endeavors. Cyberspace is borderless, offenders are highly sophisticated, and the relative anonymity offered by encrypted platforms makes pursuing and prosecuting offenders an uphill endeavour across all the law enforcement agencies across the globe.

At the outset, the anonymity that the internet provides makes it difficult to trace criminals. There should not be an option of the victim in AI-generated CSAM, unlike in the classical cases of child sexual exploitation where the investigators can often follow the trail of victimization. The fact that there is no physical child does not only make it hard to classify the crime but also removes one of the main points of departure when the law enforcement is conducting an investigation. The attackers can be either individuals trying out generative adversarial networks (GANs), crime syndicates profiting on AI-driven pornography sites, or even hobbyists toying with the production of synthetic images with no evident monetization interest. In this situation, it is both technical and legal because the current laws tend to remain silent regarding virtual victims[25].

Another major impediment is jurisdictional impediments. Cybercriminals that create AI-based CSAM frequently have their servers in one country, their creator in another, and their consumers in different continents. This dispersal complicates the assertion of jurisdiction by the law enforcement agencies. Customary canons of criminal law, including the territoriality or nationality, do not fit well in crimes that occur at the same place at the same time. International conventions such as the Budapest Convention on Cybercrime have tried to facilitate collaboration among nations but the limitation is its number of signatories and those non-signatories, some of which are significant jurisdictions, refusing to use universal standards. This creates huge loopholes in international implementation, and criminals take advantage of those havens that have loose regulatory regulations[26].

[25] Ashroff, *supra* note 10 at 4.
[26] Coroners, *supra* note 11 at 4.

Procedural enforcement is challenging even in the case of jurisdiction. Police departments usually use the availability of information with privately owned technology firms to track criminals. Privacy legislation, data location mandates, and a more or less voluntary cooperation of service providers, however hinder such access. Companies in the European Union, as an example, have to find a balance between meeting the requirements of GDPR and providing support in the investigations of the law enforcement agencies. Though the platform is required in India in accordance with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to practice due diligence and censor unlawful content, they do not necessarily have more sophisticated AI detection systems. It is easy to have AI-generated CSAM circulate long durations without being detected.

Although these encryption technologies are important in protecting the privacy of users, there is a paradox of enforcing them. WhatsApp and Signal are end-to-end encrypted platforms that have been continuously reported to be centres where illicit content including CSAM is exchanged. AI usage helps criminals to produce volumes of content quickly, clogging such sites with artificial content that is being generated almost every second and practically impossible to trace without intercepting encryption itself. There is still an ongoing debate by governments and civil society about the introduction of so-called backdoors to allow law enforcement to access digital information, yet a similar solution is also likely to harm the overall digital security, creating larger issues of privacy and surveillance[27].

The unequal distribution of technical expertise is also a problem that increases issues related to enforcement on the global scale. The developed nations like the United States, the UK, and Australia have invested a lot in cyber forensic units who can utilize AI to identify AI-powered crimes. Nevertheless, developing nations such as India are usually strained by resources; hence, they cannot monitor offenders using advanced equipment. This gap gives the criminals an opportunity to use the weaker jurisdictions as impunity fields, and distribute their content to the dark web all over the world. The next urgent problem is the fact that it is hard to tell AI-generated CSAM and the real images[28]. The developments of the generative adversarial networks have gone to the point where synthetic images are practically indistinguishable between real photographs and synthetic images. This causes evidentiary issues in court: the

[27] Europol, *Exploring the Potential of AI to Combat Child Sexual Abuse Material Online* 15–18 (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/AI_to_Combat_CSAM.pdf.
[28] Interpol, *Global Threat Assessment on Child Sexual Exploitation and Abuse* 22–25 (2022), https://www.interpol.int/en/Crimes/Crimes-against-children/Online-child-sexual-exploitation.

prosecutors need to show beyond a reasonable doubt that the material is not only synthetic, but also within the model of child sexual abuse material under national law. This ambiguity can be used by defence counsel to challenge conviction especially in those jurisdictions where virtual pornography is not explicitly outlawed.

In addition, the varying jurisdictions have high cultural and legal differences as to what is considered child pornography. Whereas there are states like Australia that criminalize even cartoon or animated images of a child being sexually involved, certain states, like the United States have approached it more narrowly. Such inconsistency poses additional challenges to international cooperation. Rapists usually act in a jurisdiction whereby the content made of synthetic is not criminalized, and they share the material throughout the world, which essentially protects them against prosecution.

There is an even deeper layer of complexity brought in by the dark web. The marketplaces with the implementation of the networks allow criminals to buy and sell AI-generated CSAM anonymously in cryptocurrencies. These markets often come and come out in different forms under different identities thus becoming very hard to finalize. Arrest operations which are organized through Helicopter activities like those led by the Europol may only provide a temporary halt with networks restoring themselves in a matter of weeks[29]. Blending AI-presented automation enables such platforms to create and distribute on-demand content without relying on the old methods of finding sources of illegal content and making it hard to detect.

To the point, anonymity, territorial fragmentation, evidentiary obstacles, and technological asymmetries are causes of enforcement and jurisdiction problems in AI-generated CSAM. The digital environment that the world is in now enables criminals to act with a feeling of impunity as they know that the legal frameworks are grappling to cope with the specifics of synthetic material of abuse. Without the states being capable of aligning their regulations, creating sophisticated detection systems, and increasing the level of international collaboration, the process of enforcing AI-CSAM crimes will be severely limited.

[29]Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* 34–38 (2023), https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

Reform Needs and Recommendations

The topic of AI-generated Child Sexual Abuse Material (CSAM) also highlights the urgency of the systematic changes on the national and international levels. The advent of synthetic abuse material has indicated the flaws in criminal law, enforcement systems, rules of evidence, and international collaboration. These gaps can only be addressed with a comprehensive reform, which will then ensure that such offenders will still be able to use the legal loophole, therefore, a new kind of child exploitation will become normalized. The first and the most urgent requirement is the modernization of the legal definitions. The Indian POCSO Act, 2012, and Section 67B of the Information Technology Act, 2000 are laws that are framed with the assumption that there exist actual victims, actual photographs or videos.

This framing creates ambiguity in the situation of AI-generated content. To reduce this, legislatures need to extend the definition of child sexual abuse material to cover morphed, animated, and artificial images of underage children in sexual situations, whether or not the actual child exists or not. The justification of such expansion goes beyond the avoidance of direct harm to the prevention of the normalization of child exploitation in society. Some countries such as Australia and United Kingdom already criminalize the possession and distribution of virtual child pornography and such laws could be emulated to the Indian and international law[30].

In close relation to the definitional reform is the explanation of criminal liability. Currently, there is no real child, and this can be used by offenders to claim that their actions are victimless. However, the hidden injury is that such an ecosystem would justify deviant sexual interests and even promote the shift between the synthetic and the abused. The reform of the legislation should thus make clear that the creation, sale, and ownership of AI-generated CSAM is illegal per se. The intent element can be assumed based on the act in question, which transfers the burden of proving a point upon the defendant. This strategy would reflect the current assumptions in narcotics and anti-terrorism laws, in which societal harms result in a break with hard demands of direct victimization.

The second reform area is connected with evidence and procedure. The current limitation facing the courts is a situation whereby the evidentiary frameworks in place are old and they

[30] *Id.* at 14.

fail to suit synthetic material. An example of this is in the Indian law, whereby the electronic evidence has strict certification requirements in Section 65B of the Evidence Act, 1872[31]. When it comes to AI-generated CSAM, in which digital manipulation is the nature of the crime itself, these requirements tend to fall apart due to defence problems. A revamped evidentiary system must also include AI certification in forensics, the use of blockchain technology to verify content, and the international standards in the preservation of digital evidence. The training of the judiciaries is also critical in order to have the courts prepared to weigh expert evidence on synthetic media thus minimizing the variation in verdicts. Capacity-building reforms are also needed by the enforcers. Traditional cybercrime departments are not always technologically advanced to track criminals using modern AI, encryption and dark web platforms. Special cyber forensic laboratories have to be created, and they have to be manned by experts in artificial intelligence, cryptography, and digital forensics. The governments must set aside specific funds in the identification of detection technology that can watermark AI-generated imagery, spot patterns in GAN-generated material and trace cryptocurrency transactions associated with the trade in synthetic CSAM. Proactive detection and takedown require the participation of public-private partnerships with technological firms having control over the platforms where such content circulates.

At a broader level, harmonization of the laws internationally is a serious reform requirement. The international character of AI-created CSAM is such that the perpetrators tend to take advantage of the jurisdictions that have lighter or no prohibitions. The existing tools, including the Budapest Convention on Cybercrime, have a problem of unequal participation. A new multilateral framework or an enlarged protocol specifically on AI-generated material of abuse is needed, and states are bound to criminalize synthetic CSAM, provide mutual legal assistance and share forensic expertise. In the absence of such harmonization, domestic reforms will be so piecemeal and will be easily bypassed by transnational offenders.

Reforms should also protect overreach in terms of ethical protections. On the one hand, the safety of children is the reason why a criminal ban should be very extensive, but the legislation should be approached with sensitivity not to interfere with rightful areas of artistic expression, education, or satire. This necessitates creation of statutory defences or exceptions on the difference between exploitative depictions and non-sexual fictionalized works. This kind of

[31] Rakesh Kumar Singla v. Union of India, (2018) 2 SCC 342 (India)

balancing would make the legal regime proportionate and in line with constitutional freedoms, which would safeguard it against constitutional scrutiny in the future[32].

Considering the set needs, some recommendations present themselves as priorities. To start with, the amendments that explicitly define and criminalize AI-generated CSAM should be implemented by the legislatures, based on the international examples, though the provision is to be adjusted to the local situation. Second, cyber units should be dedicated to specializing in cyber detection and forensic tools that include AI and have its own funding. Third, the evidentiary law can be reformed to accept new sophisticated methods of forensic systems and simplify the process of dealing with synthetic digital material. Fourth, it is necessary to implement mandatory AI and cyber law training courses in judicial academies so that judges are not left with the technological illiterate. Fifth, jurisdictions such as India are encouraged to advocate internationally on the need to have an international treaty framework in order to align responses of countries allowing cross border enforcement and information sharing. Lastly, intensive social education campaigns should be rolled out to enlighten society about the harm of AI-generated CSAM, and as a result, demand should be lowered, and reporting should also be promoted.

Altogether, the recommendation and needs of the reform are oriented to the future, where the law would adjust to the realities of the technologies. The identification of AI generated CSAM as a serious danger to children protection is the initial step, but it should be succeeded by the intentional and organized changes in the law, enforcement, procedure, and global governance. Only in that case, the legal systems will be able to regain their abilities to safeguard children, even in the world when the exploitation becomes synthetic and digital.

Conclusion

Artificial intelligence has crusaded creativity, interaction, and trade among people, but its negative uses make some of the most aversive weaknesses of the digital age evident. The invention and sharing of AI-generated Child Sexual Abuse Material (CSAM) is one of those and is a deep legal, moral, and social dilemma. Synthetic CSAM, in contrast to traditional forms of child exploitation, does not always need a material child, but it promotes the culture of normalization of sexual violence against minors, encourages deviant behaviour, and

[32] Jennifer Daskal & Susan W. Brenner, *Technology Outpaces the Law: Legal Responses to AI-Generated Child Exploitation Material*, 102 J. Crim. L. & Criminology 45, 85–88 (2023).

preconditions in which real-world abuse has an opportunity to flourish. This phenomenon is thus not only a technological advancement but also a profound danger to the values of child protection, dignity and human rights which are the main pillars of contemporary legal frameworks.

The above discussion shows that the biggest challenge is in the legal vacuum of synthetic CSAM. Current child protection regimes either under Indian law, the U.S. law, or the international conventions were formulated at a period when child pornography was only used in reference to pictures of actual kids. This lack of clear separation on the content generated by AI has enabled criminals to take advantage of the loopholes in definition since no real victims are being hurt. Courts and legislatures have found it difficult to find a balance between the freedom of expression and the necessity to avoid exploitation leading to the use of different approaches depending on jurisdiction. This legal ambiguity has given boldness to offenders to act in safe havens as the dark web provides anonymity and the security of encryption technologies.

The paper has also indicated that the problem is exacerbated by enforcement and procedural challenges. The ineffective prosecutions are impeded by jurisdictional fragmentation, challenges in the form of evidence, and limited resources. The evidence used in digital forensics can be easily challenged, judicial authorities might not be tech savvy to analyse AI-generated data and cross-border collaboration is hindered by red tape. In the instances when the enforcement agencies are able to identify the offenders, cases fail in court because of the admissibility or the failure to establish exploitative intent. These frailties underscore the necessity of introducing structural changes both in substantive and procedural law.

However, AI-generated CSAM does not have impossible challenges. Technology can transform alongside the law as the reform proposals in this paper suggest. Clearly established legislative changes that specify and criminalize AI-generated CSAM, capacity-building in cyber forensic departments, evidence law modernization, judicial education, and partnerships between government and technology firms all are part of the key elements of a comprehensive approach. At the international level, the standardization of laws with the help of an extended international treaty system, possible based on the Budapest Convention, yet with specific references to AI-enabled abuse, will play a decisive role in eliminating the possibility of offenders using the loopholes of a jurisdiction.

Equally important is the recognition that the battle against AI-generated CSAM is not merely legal but also ethical and societal. Protecting children in the digital age requires not only punishing offenders but also reshaping cultural narratives, reducing demand, and building awareness about the harms of synthetic exploitation. This calls for a victim-centric approach that recognizes the indirect yet profound harm inflicted by AI generated content that reverberates across society by perpetuating the sexualization of minors and eroding the protective norms that safeguard childhood.

AI-generated CSAM represents a new frontier of criminality, one that stretches the boundaries of law, ethics, and enforcement. It challenges the very assumptions upon which child protection regimes were built and forces a rethinking of how harm, exploitation, and victimization are understood in the digital age. The task before lawmakers, courts, and enforcement agencies is formidable, but it is also inescapable. A failure to act decisively will leave a generation vulnerable to the normalization of abuse in synthetic form. Conversely, bold reforms grounded in legal clarity, technological innovation, and international solidarity can ensure that the promise of artificial intelligence is not subverted into a tool for the most abhorrent forms of exploitation. The protection of children has always been a measure of a society's moral and legal strength; in the era of AI, it will also be the measure of its capacity to adapt, innovate, and uphold human dignity in the face of unprecedented digital challenges.

References:

1. Internet Watch Foundation, AI-Generated Videos of Child Sexual Abuse: A Stark Vision of the Future, https://www.iwf.org.uk/news-media/news/ai-generated-videos-of-child-sexual-abuse-a-stark-vision-of-the-future/

2. Europol, AI-Generated Child Sexual Abuse Material: Combating the Growing Threat, https://www.europol.europa.eu/media-press/newsroom/news/ai-generated-child-sexual-abuse-material-combating-growing-threat

3. Stanford Internet Observatory, Investigation Finds AI Image Generation Models Trained on Child Abuse, https://reap.fsi.stanford.edu/news/investigation-finds-ai-image-generation-models-trained-child-abuse

4. Michael Salter, *Deepfakes and Synthetic Child Sexual Abuse Material: Policy Challenges and Responses*, 13 J. Child Sexual Abuse 1 (2023), https://onlinelibrary.wiley.com/doi/full/10.1002/cri2.66.

5. Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

6. Sarah E. Ullman, *Artificial Child Sexual Abuse Material and the Law: Criminalization Without a Victim?* 45 Child Abuse & Neglect 1 (2023), https://doi.org/10.1016/j.chiabu.2023.106236.

7. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, G.A. Res. 54/263, 2171 U.N.T.S. 222, arts. 2–3.

8. PROTECT Act of 2003, No. 18 U.S.C. §§ 2251–2260.

9. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 255–56 (2002).

10. Coroners and Justice Act 2009 § No. 25, 62–63 (U.K.)

11. The Protection of Children from Sexual Offences Act, No. 32, Acts of Parliament, 2012(India)

12. The Information Technology Act, § 67B, No. 21, Acts of Parliament, 2000 (India)

13. Child light Global Child Safety Institute, Action Needed to Close Legal Gaps on AI-Generated Child Sexual Abuse Material (Dec. 31, 2024), https://www.childlight.org/newsroom/action-needed-to-close-legal-gaps-on-ai-generated-child-sexual-abuse-material.

14. Europol, Europol warns of rise in AI child abuse imagery, DW (Sept. 21, 2025), https://www.dw.com/en/europol-warns-of-rise-in-ai-child-abuse-imagery/a-69733974

15. Jennifer Daskal & Susan W. Brenner, *Technology Outpaces the Law: Legal Responses to AI-Generated Child Exploitation Material*, 102 J. Crim. L. & Criminology 45 (2023).

16. Claire Andresen, *Artificially Generated, Genuinely Harmful: Prosecuting AI-Generated Child Sexual Abuse*, SSRN (Sep. 22, 2025), https://papers.ssrn.com/sol3/Delivery.cfm/5381736.pdf?

17. Joanna Bryson, *Challenges in Digital Forensics of AI-Generated Content*, 18 Comput. L. Rev. 77 (2022).

18. Brian Krebs, *The Dark Web and Cybercrime Enforcement Challenges*, 21 Cybersecurity L. Rev. 101 (2021).

19. Europol, *Exploring the Potential of AI to Combat Child Sexual Abuse Material Online* 15–18 (2022), https://www.europol.europa.eu/cms/sites/default/files/documents/AI_to_Combat_CSAM.pdf.

20. Interpol, *Global Threat Assessment on Child Sexual Exploitation and Abuse* 22–25 (2022), https://www.interpol.int/en/Crimes/Crimes-against-children/Online-child-sexual-exploitation.

21. Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023* 34–38 (2023), https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023

22. Rakesh Kumar Singla v. Union of India, (2018) 2 SCC 342 (India)

23. Jennifer Daskal & Susan W. Brenner, *Technology Outpaces the Law: Legal Responses to AI-Generated Child Exploitation Material*, 102 J. Crim. L. & Criminology 45, 85–88 (2023).