

Regulating AI-Generated Child Sexual Abuse Material in Indonesia: State Obligation under Human Rights Standards

Hafina Haula Arsy¹, Hadi Rahmat Purnama²

¹Faculty of Law, University of Indonesia, Indonesia, Email: hafina.haula@ui.ac.id

² Faculty of Law, University of Indonesia, Indonesia, Email: hadi.rahmat@ui.ac.id

Abstract

Generative artificial intelligence (AI) has created new forms of child sexual abuse material that challenge existing child protection and cybercrime frameworks. This study explores the extent to which the national legal framework can address AI-generated child sexual abuse material (AI-CSAM), including semi-synthetic and fully synthetic materials. It also evaluates whether the state has fulfilled its obligations to protect children's rights, as a component of human rights, in digital environments. This study employed a doctrinal legal research methodology, utilizing statutory and conceptual approaches. The analysis is grounded in a human rights-based approach and the theory of state obligations, with a focus on four principles of state obligation in the context of children's rights protection: non-discrimination, the best interests of the child, participation, accountability, and the duties to respect, protect, and fulfill children's rights. The study finds that existing legal frameworks function in a fragmented and insufficiently responsive manner to the technological characteristics of AI-generated abuse materials, particularly deepfake manipulation, prompt-based generation, synthetic victims, the abuse of datasets, and the legal obligations of digital platforms and AI developers. The state's obligations remain only partially fulfilled due to inadequate procedures for handling digital evidence, preventing revictimization, regulating corporate responsibility, facilitating child-friendly mechanism for content reporting and removal, supporting victim recovery, coordinating institutions, and strengthening AI-specific enforcement capacity. This study conceptualizes AI-CSAM as a distinct form of technology-enabled sexual exploitation, extending beyond conventional online abuse and deepfake cases. The study argues that a more explicit, child-centered, and preventive legal framework is necessary to ensure effective protection, reporting, content removal, accountability, and recovery.

Keywords: *Accountability; Artificial Intelligence; Child Protection; Child Sexual Abuse Material; Human Rights-Based Approach.*

1. INTRODUCTION

Artificial intelligence (AI) is one of the innovations born from technological development and has become an inseparable part of everyday life.¹ However, AI development has also enabled increasingly sophisticated forms of sexual violence. One such form of sexual violence is the generation of child sexual abuse material that is partly or entirely synthetic, known as AI-generated child sexual abuse material (AI-CSAM).² AI-CSAM is a technologically enabled evolution of conventional child sexual abuse material, which raises new legal and human rights concerns.³ Unlike conventional

¹Ayu Riska Amalia, Diva Pitaloka, dan Adhitya Nini Rizki Apriliana, "Gender Discrimination in Artificial Intelligence: An International Human Rights Law Perspective and the Quest for Binding Regulation," *Unram Law Review* 9, no. 2 (2025): 311–33, <https://doi.org/10.29303/ulrev.v9i2.450>

²Caoilte Ó. Ciardha, John Buckley, dan Rebecca S. Portnoff, "AI-Generated Child Sexual Abuse Material: What's the Harm?," *AI & Society* (2026), <https://doi.org/10.1007/s00146-026-02932-y>

³United Nations Committee on the Rights of the Child, "Guidelines regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornog-

CSAM, AI-CSAM requires a distinct legal analysis because it may be partly or entirely synthetic and may not involve a real, identifiable child. These characteristics have created specific legal questions, including those concerning victim recognition, criminalization, and platform responsibility.

The generation and distribution of CSAM can make children permanent victims because of the risk of revictimization that can last a lifetime.⁴ The urgency of this problem is evidenced by data showing that one in eight children worldwide (approximately 300 million children) has become a victim of the distribution and dissemination of sexual images and videos taken without consent.⁵ This is reinforced by data reported by the WeProtect Global Alliance in 2023, which indicates that there were more than 32 million reports of child sexual abuse materials globally, showing an 87 % increase since 2019.⁶ The development of AI has further compounded the complexities of this problem. A study conducted by the United Nations Interregional Crime and Justice Research Institute in 2024 reported that out of approximately 36 million global reports related to online child exploitation, 4,700 of them involved CSAM generated by artificial intelligence.⁷ These figures indicate that AI-generated material is an emerging component of the broader problem of online child sexual exploitation.

In the context of Indonesia, AI-CSAM is a reasonably foreseeable risk. AI technology is becoming increasingly accessible, with widespread availability to all segments of society. This can be seen from the temporary access termination of Grok (an AI system integrated with X) by the Ministry of Communication and Digital Information. The termination was prompted by the widespread misuse of Grok for generating sexual material that exploited representations of women and children.⁸ This tendency toward misuse shows the urgency of establishing a legal framework that can respond to the misuse of AI for generating content containing sexual violence or sexual exploitation against children.

From the perspective of international law and human rights, the protection of children from sexual exploitation is considered a fundamental obligation of the state. As children are inherently vulnerable rights holders, protecting them from exploitation is an integral part of the broader protection of human rights.⁹ The Convention on the Rights of the Child (CRC) guarantees the right of children to obtain protection from all forms of sexual violence and exploitation, including in the digital environment. Furthermore, the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC) calls upon states to take all possible measures to prevent and address all forms of sexual violence and exploitation, including those perpetrated with the assistance of digital technology, through their national laws

raphy," CRC/C/156 (10 September 2019).

⁴Jennifer Foster, "Pixelated Harm: An Analysis of the Impact of AI-Generated Images on CSAM Criminalization and Child Safety," *Oklahoma City University Law Review* 49, no. 3 (2025): 425–40.

⁵Jennifer Foster, "Pixelated Harm: An Analysis of the Impact of AI-Generated Images on CSAM Criminalization and Child Safety," *Oklahoma City University Law Review* 49, no. 3 (2025): 425–40.

⁶WeProtect Global Alliance, *Global Threat Assessment 2023 Press Release* (17 October 2023)

⁷United Nations Interregional Crime and Justice Research Institute (UNICRI), *Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse* (Turin: UNICRI, September 2024), <https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf>

⁸Kementerian Komunikasi dan Digital Republik Indonesia, "Pemerintah Putus Akses Sementara Grok demi Lindungi Masyarakat di Ruang Digital," *DJED Komdigi*, accessed on 21 April 2026, <https://djed.komdigi.go.id/news/pemerintah-putus-akses-sementara-grok-demi-lindungi-masyarakat-di-ruang-digital>

⁹Abdul Rahman, Zainal Amin Ayub, dan Ratnawati, "Legal Framework for Protecting Children from Commercial Sexual Exploitation," *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi* 8, no. 1 (2025): 87–110, <https://doi.org/10.24090/volksgeist.v8i1.13156>.

and policies.¹⁰ States are obligated to criminalize these forms of exploitation in order to protect children from the risks of exploitation that are associated with technological development.¹¹ Online child sexual exploitation increasingly operates through organized networks, advanced digital infrastructure, and cross-border coordination, while existing international instruments concerning this problem remain fragmented in their definitions, jurisdictional rules, and enforcement standards.¹²

The state's obligation in the protection of children's rights encompasses the obligations to respect, protect, and fulfill the rights to dignity, privacy, and personal integrity of children as part of the universal protection of human rights.¹³ The human rights-based approach (HRBA) provides a framework for evaluating the performance of these obligations through a child rights-based approach. This approach places the best interests of the child as the main principle in the design and use of digital technology. It also demands the existence of accountability and prevention mechanisms against the misuse of AI for generating child sexual exploitation material, including in the form of synthetic representation.¹⁴

The absence of explicit legal provision on AI-CSAM creates uncertainty in victim recognition, protection, recovery, and platform responsibility, particularly in cases involving fully synthetic content and AI-generated manipulation. This condition shows that, despite the existence of national laws that stipulate the prohibition of obscene content and the responsibility of electronic information system providers in general, the existing legal framework is not yet fully responsive to child sexual exploitation accommodated by AI. Consequently, a legal gap exists in the handling of AI-CSAM cases in Indonesia. This legal gap reflects a broader challenge that has been identified in recent Indonesian scholarship, namely the absence of a coherent AI-specific legal framework, with existing legislation addressing only certain consequences of AI misuse through fragmented legal provisions rather than through comprehensive AI regulation.¹⁵ The misuse of AI, particularly deepfake, further exposes weaknesses in Indonesia's existing legal framework and demonstrates the need for comprehensive legal mechanisms grounded in transparency and accountability.¹⁶

Although previous studies have examined AI-CSAM in relation to legal gaps, enforcement challenges, and the risks of generative AI, these studies have not specifically evaluated the application of Indonesian law within the combined framework of HRBA and state obligation. Based on this background, this study aims to evaluate legal framework in Indonesia in addressing CSAM and the extent to which existing legal

¹⁰United Nations Committee on the Rights of the Child, Guidelines regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, U.N. Doc. CRC/C/156 (September 10, 2019).

¹¹United Nations, Convention on the Rights of the Child (New York: United Nations, 1989), arts. 19, 34, dan 36; United Nations, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (New York: United Nations, 2000), arts. 2 dan 3.

¹²Hesti Septianita, Pujiyono, and Irma Cahyaningtyas, "Online Child Sexual Exploitation and Abuse as Organized Crime: Towards a New International Legal Framework," *Jurnal Litigasi* 27, no. 1 (2026): 1–3, <https://doi.org/10.23969/litigasi.v27i1.43221>.

¹³United Nations, *International Covenant on Civil and Political Rights* (New York: United Nations, 1966), arts. 7, 17, dan 24.

¹⁴UNICEF, Guidance on AI and Children, 3rd ed. (New York: UNICEF, 2025); UNESCO, Recommendation on the Ethics of Artificial Intelligence (Paris: UNESCO, 2021).

¹⁵Evyta Rosiyanti Ramadhani, Ayudya Rizqi Rachmawati, dan Roro Hera Kurnikova, "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia," *De Jure: Jurnal Hukum dan Syar'iah* 17, no. 1 (2025): 118–119, <https://doi.org/10.18860/j-fsh.v17i1.28880>.

¹⁶Hesti Armiwulan, Rofi Aulia Rahman, Valentino Nathanael Prabowo, and József Hajdú, "Artificial Intelligence and Its Challenges to Elections in Indonesia: A Legal Analysis," *Jambura Law Review* 6, no. 2 (2024): 264–285, <https://doi.org/10.33756/jlr.v6i2.24243>.

norms adequately regulate AI-CSAM. Furthermore, it aims to analyze the fulfillment of the state's obligations in protecting children's rights from AI-CSAM using the human rights-based approach (HRBA) and the four principles of state obligation in international human rights law as the analytical framework. The four principles of state obligation are non-discrimination, the best interests of the child, participation, accountability, and the obligations to respect, protect, and fulfill human rights. Additionally, this study used a doctrinal legal methodology, with statutory and conceptual approaches, to evaluate the conformity of legal provisions in Indonesia with international human rights standards concerning the protection of children from AI-CSAM. By examining AI-CSAM beyond deepfakes to include semi-synthetic and fully synthetic AI-CSAM, and by evaluating Indonesia's obligation to protect children from AI-enabled sexual exploitation, the present study is expected to fill the aforementioned legal gap.

2. ANALYSIS AND DISCUSSION

2.1. Legal Provisions regarding CSAM in Indonesia and Their Scope in Addressing AI-CSAM

2.1.1. Characteristics of AI-CSAM as a New Legal Challenge

The development of AI technology has enabled the generation of child sexual abuse material that is partially or entirely synthetic, known as AI-CSAM,¹⁷ a novel form of CSAM that has evolved from traditional forms into a more complex digital form facilitated by AI technology. The term "CSAM" itself is used to replace "child pornography," as recommended by the Committee on the Rights of the Child in the 2019 Guidelines regarding the implementation of the OPSC.¹⁸ This shift in terminology is based on the view that sexual material depicting children is not pornography but a form of sexual abuse. The use of the term "child pornography" is considered highly inappropriate because it may be interpreted as an act committed with the consent of the child, thereby disregarding the nature of CSAM as a form of exploitation and violence against children.¹⁹ Furthermore, AI-CSAM refers to child sexual abuse material generated using artificial intelligence, including material that features the image or identity of a real child and fully synthetic representations of a child in a sexual context.

Although AI-CSAM may be synthetic, this does not negate the dimension of children's rights violation and must still be viewed within the scope of child protection. Based on its characteristics, AI-CSAM can be classified into two main forms: semi-synthetic AI-CSAM (also known as "deepfake") and fully synthetic AI-CSAM.²⁰ Semi-synthetic AI-CSAM, or deepfake, is a form of child sexual abuse material that involves the misuse of AI technology for manipulating a child's image, such as removing or changing clothing to generate fabricated nude images (AI-generated non-consensual intimate imagery).²¹

¹⁷C Caoilte Ó. Ciardha, John Buckley, dan Rebecca S. Portnoff, "AI-Generated Child Sexual Abuse Material: What's the Harm?," AI & Society (2026), <https://doi.org/10.1007/s00146-026-02932-y>

¹⁸Caoilte Ó. Ciardha, John Buckley, dan Rebecca S. Portnoff, "AI-Generated Child Sexual Abuse Material: What's the Harm?," AI & Society (2026), <https://doi.org/10.1007/s00146-026-02932-y>

¹⁹United Nations Committee on the Rights of the Child, Guidelines regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, U.N. Doc. CRC/C/156 (September 10, 2019), para. 55.

²⁰Caoilte Ó. Ciardha, John Buckley, dan Rebecca S. Portnoff, "AI-Generated Child Sexual Abuse Material: What's the Harm?," AI & Society (2026), <https://doi.org/10.1007/s00146-026-02932-y>

²¹Desara Dushi, Nertil Berdufi, dan Anastasia Karagianni, "The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material," Computer Law & Security Review 59 (2025): 106205, <https://doi.org/10.1016/j.clsr.2025.106205>

This manipulation is often perpetrated by using photos from the victim's social media and other online uploads to place the victim in an artificial sexual situation. The risk of victimization increases when the manipulated image is used to humiliate, threaten, or sexually extort the victim (sextortion).²² The use of a child's image or identity without consent can result in the child becoming a direct victim,²³ which can cause psychological harm and lead to other forms of sexual abuse. Therefore, semi-synthetic AI-CSAM can be regarded as a form of sexual violence, as it attacks the dignity, privacy, and sexual autonomy of the victim.²⁴

Fully synthetic AI-CSAM is material that is entirely generated by generative AI and displays the representation of a fictional child in a sexual context without always using a real, identifiable child.²⁵ A common misconception is that, because this type of AI-CSAM does not involve a real child, no victim is harmed. In fact, although fully synthetic AI-CSAM does not involve direct physical sexual violence, various studies have shown that it causes real harm to children and is difficult to distinguish from real material.²⁶ The production and consumption of fully synthetic AI-CSAM may exacerbate the normalization of the sexual exploitation and objectification of children, abet grooming and sexual extortion, expand the CSAM market, and create a new pathway toward sexual offending behavior against children.²⁷ Exposure to child sexual content can also form cognitive associations between children and sexuality. Therefore, the danger of fully synthetic AI-CSAM lies not only in its production process, but also in the effects of its consumption and circulation.²⁸

The distinction between the two forms of AI-CSAM previously discussed becomes important for assessing the scope of the law. The first form of AI-CSAM is easier to connect with violations of specific children's rights, such as the rights to privacy, dignity, integrity, and safety, because there is a real child whose identity is used. Meanwhile, the second form poses challenges related to the substantiation of evidence and the conceptualization of victims within the context of criminal law, but remains relevant within the framework of children's rights due to its role in exacerbating the normalization of child sexual exploitation, expanding the market for CSAM, and weakening the collective protection of children from technology-based sexual violence.²⁹

2.1.2. Normative Scope of AI-CSAM and the Limitations of Legal Provisions in Indonesia

²²Rick Brown et al., "Artificial Intelligence and Child Sexual Abuse: A Rapid Evidence Assessment," Trends & Issues in Crime and Criminal Justice, no. 711 (2025), https://www.aic.gov.au/sites/default/files/2025-01/ti711_artificial_intelligence_and_child_sexual_abuse.pdf?utm_source

²³UNICEF, "'Deepfake Abuse Is Abuse': UNICEF Calls for Criminalization of AI Content Depicting Child Sex Abuse," February 6, 2026.

²⁴John Danaher, "The Law and Ethics of Deepfakes," *Oxford Journal of Legal Studies* 37, no. 3 (2017): 534–61, <https://doi.org/10.1093/ojls/gqw033>

²⁵Caoilte Ó. Ciardha, John Buckley, dan Rebecca S. Portnoff, "AI-Generated Child Sexual Abuse Material: What's the Harm?," *AI & Society* (2026), <https://doi.org/10.1007/s00146-026-02932-y>

²⁶A. Pocol et al., "Seeing Is No Longer Believing: A Survey on the State of Deepfakes, AI-Generated Humans, and Other Nonveridical Media," dalam B. Sheng, L. Bi, et al., eds., *Advances in Computer Graphics, Lecture Notes in Computer Science* 14496 (Cham: Springer, 2023), 434, https://doi.org/10.1007/978-3-031-50072-5_34 https://doi.org/10.1007/978-3-031-50072-5_34

²⁷Caoilte Ó Ciardha, John Buckley, and Rebecca Portnoff, "AI-Generated Child Sexual Abuse Material: What's the Harm?," *AI & Society* (2026), <https://doi.org/10.1007/s00146-026-02932-y>

²⁸Bryant Paul dan Daniel G. Linz, "The Effects of Exposure to Virtual Child Pornography on Viewer Cognitions and Attitudes Toward Deviant Sexual Behavior," *Communication Research* 35, no. 1 (2008): 3–38, <https://doi.org/10.1177/0093650207309359>

²⁹Desara Dushi, "The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material," *Computer Law & Security Review* 58 (2025): 106167.

The legal provisions in Indonesia have yet to fully address AI-CSAM. Although the protection of children from sexual exploitation has a constitutional basis in Article 28B paragraph (2) of the 1945 Constitution, the term “child sexual abuse material” (CSAM) has not yet been explicitly adopted as an independent legal concept in Indonesian law. Existing legal provisions still refer to related conduct through different terminology, such as “child pornography,” “sexual exploitation of children,” “electronic information-violating decency,” and “electronic-based sexual violence.” These terms are used across several legal instruments, including the Law on Child Protection, the Law on Pornography, the Law on Electronic Information and Transactions (ITE), the Law on Sexual Violence Crimes (TPKS), and the Law on Personal Data Protection.³⁰ Therefore, in order to assess the scope of Indonesian positive law toward AI-CSAM, it is necessary to examine whether existing norms under the Law on Child Protection, the Law on Pornography Law, the Law on ITE, the Law on TPKS, and the Law on Personal Data Protection can be applied to such conduct. However, these laws can only be used against AI-CSAM if the elements of AI-CSAM can still be included within the formulation of the applicable offense.

a. Law on Pornography

The Law on Pornography (Law No. 44 of 2008 on Pornography) prohibits the involvement of children in activities and/or as objects of pornography. According to the provision of the law, the term “child pornography” refers to all forms of pornography involving children or adults who act or behave like children.³¹ In this respect, the Law on Pornography may be used to address certain cases of CSAM, particularly where children are involved as objects of pornographic material. However, the use of the term “child pornography” has the potential to obfuscate the position of the children as victims and reduce CSAM to a moral or ethical violation.³²

The limitation imposed by the Law on Pornography can be seen from the definition of pornography within the law, which is material or messages of sexuality that contain obscenity or sexual exploitation and contravene societal norms of decency.³³ Accordingly, the Law on Pornography is more focused on the prohibition of the production, distribution, provision, and consumption of pornographic material than on the character of CSAM as evidence, representation, and continuation of sexual violence against children.³⁴

This limitation adds a layer of complexity in the context of AI-CSAM. AI technology enables the creation of child sexual material in the form of deepfakes, semi-synthetic material, and fully synthetic content.³⁵ Concurrently, the Law on Pornography has not specifically covered the revictimization character of CSAM, where harm may continue each time the material is stored, viewed, shared, downloaded, or

³⁰Sudikno Mertokusumo, *Penemuan Hukum: Sebuah Pengantar* (Yogyakarta: Liberty, 2007).

³¹Indonesia, Penjelasan Pasal 4 ayat (1) huruf f Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.

³²Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 2nd ed. (Luxembourg: ECPAT International, 2025), 1–2, 10–11.

³³Indonesia, Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Pasal 1 angka 1.

³⁴Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, 2nd ed. (2025), 67–78; John Carr, “Child Abuse, Child Pornography and the Internet,” *International Review of Law, Computers & Technology* 18, no. 2 (2004): 169–84.

³⁵Desara Dushi, “The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material,” *Computer Law & Security Review* 58 (2025), <https://www.sciencedirect.com/science/article/abs/pii/S2212473X2500077X>

redistributed.³⁶ Moreover, AI-CSAM does not always involve a real children with real identities in real life, while the law continues to adhere to the conventional definition of “child pornography” as material involving real children as the objects of pornography.³⁷ This provision under the Law on Pornography reveals a legal gap. While the Law on Pornography may be used to address certain cases of CSAM, it remains inadequate to address AI-CSAM. This is because it does not specifically regulate synthetic content, deepfakes, digital manipulation, the use of children’s data in AI systems, or the responsibility of digital platforms.

b. Law on Child Protection

Unlike the Law on Pornography, which addresses CSAM within the framework of public decency, the Law on Child Protection (Law No. 35 of 2014) has a broader scope, as it recognizes children as legal entities who must be protected from sexual exploitation and sexual offences. Article 76I of the Law on Child Protection prohibits any individual from placing, permitting, committing, ordering, or participating in the economic and/or sexual exploitation of children. This provision is particularly relevant to CSAM, insofar because it allows such material to be understood not merely as pornographic content, but as a manifestation of the sexual exploitation of and violence against children.

However, the ambit of the Law on Child Protection remains limited in the context of AI-CSAM because its protection model is primarily based on the existence of a real and identifiable child. The law focuses on exploitative conduct against children, rather than on the existence, possession, distribution, or circulation of digital material as a standalone criminal object. As a result, it may cover AI-CSAM involving real children, such as the exploitation of a child’s photograph, likeness, body, voice, or identity to generate sexual deepfakes or semi-synthetic material, because such conduct can be regarded as a form of sexual exploitation and a violation of the child’s dignity.³⁸ Nevertheless, the law remains insufficient to address fully synthetic AI-CSAM. If the material is entirely created by AI, without involving an identifiable real child, the element of “child” as a direct victim becomes difficult to prove. Therefore, although the Law on Child Protection can serve as a foundational framework for addressing CSAM and certain forms of AI-CSAM involving real children, it has not yet covered the full range of characteristics of AI-CSAM, particularly fully synthetic material, which is AI-manipulated material that does not involve any identifiable child; the use of data in AI systems; and the responsibility of the technological ecosystem that enables the production and dissemination of such material.

Notwithstanding the issue regarding terminology, the Law on Child Protection Law is concerned with the protection of child victims of pornography and child victims of sexual crimes. This protection is facilitated through guidance, assistance,

³⁶Michael Salter, “Child Sexual Abuse Material and the Digital Economy,” *New Media & Society* 25, no. 9 (2023): 2277–95; Michael Salter dan T. Wong, “The Production and Distribution of Child Sexual Abuse Material by Parental Figures,” *Child Abuse Review* 30, no. 3 (2021): 206–18.

³⁷Dushi, “The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material.”

³⁸Desara Dushi, “The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material,” *Computer Law & Security Review* 58 (2025): 106167.

and social, physical health, and mental recovery.³⁹ Moreover, the law stipulates special protection of child victims of sexual crimes through education, social rehabilitation, psychosocial assistance, and the provision of protection.

c. Law on Electronic Information and Transactions (ITE)

Article 27 paragraph (1) of the Law on Electronic Information and Transactions (ITE), as amended by law No. 1 of 2024, prohibits any individual from intentionally and without authorization broadcasting, displaying, distributing, transmitting, and/or making accessible electronic information and/or electronic documents that contain material violating decency to the public. This provision may be applied to the dissemination of CSAM and AI-CSAM via digital platforms, as such material can be classified as electronic information or electronic documents containing sexual content. However, as with the Law on Pornography, the scope of the Law on ITE remains limited because its orientation lies in electronic content and public accessibility, rather than in the recognition of CSAM as a form of sexual exploitation against children.

The Law on ITE is more applicable in instances where AI-CSAM has already been disseminated, transmitted, or made accessible. However, the law does not specifically regulate the generation of AI-CSAM, the use of a child's face or data as AI input, the use of CSAM datasets to train AI models, prompt-based generation, or the responsibility of AI system providers. As a result, AI-CSAM poses a risk of being treated merely as indecent electronic content, rather than as conduct that seriously affects children's dignity, privacy, safety, and recovery. This limitation indicates that the Law on ITE does not provide adequate victim protection mechanisms, particularly in cases where AI-CSAM manipulates children's identities or reproduces child-like sexual representations without involving an identifiable victim.⁴⁰

d. Law on Sexual Violence Crimes (TPKS)

The Law No. 12 of 2022 on Sexual Violence Crimes (TPKS) signifies an important development in Indonesian criminal law by including sexual violence perpetrated through electronic means as one category of criminal offense.⁴¹ The legal framework of the Law on TPKS is more adaptable in addressing AI-CSAM when compared with the frameworks of the Law on Pornography and the Law on ITE. This is because it is not limited to considerations of morality or public decency. Rather, it recognizes sexual material as a form of sexual violence. In the context of CSAM or AI-CSAM, this is important because sexual material involving children should be understood as a form of sexual violence against children, rather than as a violation of morality or decency.⁴²

The Law on TPKS covers acts perpetrated through the abuse of digital technology. These include the recording, transmission, dissemination, or breach of electronic information containing sexual material without consent. Accordingly, the law may be applicable to certain forms of AI-CSAM, particularly where the material

³⁹Indonesia, Undang Undang Nomor 35 Tahun 2014 tentang Perubahan atas Undang Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak, Pasal 67B.

⁴⁰Desara Dushi, Nertil Bërdufi, and Anastasia Karagianni, "The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material," *Computer Law & Security Review* 58 (2025): 106167.

⁴¹Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Pasal 4

⁴²Clare McGlynn dan Erika Rackley, "Image-Based Sexual Abuse," *Oxford Journal of Legal Studies* 37, no. 3 (2017): 534–61.

involves the abuse of electronic means. Examples include child sexual deepfakes, the manipulation of children's images, or the distribution of child sexual content through digital platforms.

Nevertheless, the normative reach of the TPKS Law in addressing AI-CSAM is inherently limited. Article 14 of the Law on TPKS principally focuses on acts involving the recording, photographing, transmitting, or disseminating of electronic information containing sexual material.⁴³ However, AI-CSAM does not always originate from the direct recording of a child. AI technology has enabled perpetrators to generate child sexual material through text-based instructions or prompt-based generation, facial or bodily manipulation, the use of datasets, or the creation of fully synthetic content resembling children. Regrettably, these acts have not yet been explicitly regulated under the Law on TPKS.

In summary, the Law on TPKS can be utilized to address certain forms of AI-CSAM, especially semi-synthetic AI-CSAM involving real children, such as child sexual deepfakes, image manipulation, or the non-consensual use of a child's identity in sexual material.⁴⁴ The law, however, is inadequate to regulate fully synthetic AI-CSAM, prompt-based generation, the use of CSAM datasets, AI model training, or the responsibility of digital platforms and AI system providers.

2.2. Obligation of Indonesia as a State to Address AI-CSAM in accordance with International Human Rights Standards

2.2.1. Evaluation of regulations using the HRBA approach

The human rights-based approach (HRBA) requires human rights to serve as the basis for the formulation and evaluation of state policies. Given that AI-CSAM implicates children's dignity, privacy, security, protection from sexual exploitation, and recovery, the present study sought to evaluate the fulfillment of obligations from Indonesia as a state in addressing AI-CSAM and to evaluate whether the state's protection of children's rights operates effectively in the digital environment. To this end, the study relies on four main principles that are most relevant in the context of children's rights, namely non-discrimination, the best interests of the child, participation, and accountability. These principles are rooted in the Convention on the Rights of the Child (CRC), particularly Article 2 (non-discrimination), Article 3 (the best interests of the child), and Article 12 (the right of the child to be heard).⁴⁵

a. Non-Discrimination

The principle of non-discrimination under Article 2 of the CRC requires that states ensure the protection of children's rights without discrimination in any form. Article 2 unequivocally proscribes discrimination on the basis of "race, color, sex, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth, or other status." The term "other status" has been interpreted broadly by the Committee on the Rights of the Child to include various grounds of discrimination that are not expressly mentioned in the text of the CRC. In the digital context, General Comment No. 25 affirms that states must ensure equal protection for children in both the digital and physical environments.

⁴³Indonesia, Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, Pasal 14 ayat(1).

⁴⁴Clare McGlynn and Erika Rackley, "Image-Based Sexual Abuse," *Oxford Journal of Legal Studies* 37, no. 3 (2017): 534–61, <https://doi.org/10.1093/ojls/gqw033>

⁴⁵United Nations, Convention on the Rights of the Child (New York: United Nations, 1989), arts. 2, 3, dan 12.

Accordingly, in the case of AI-CSAM, child protection policies are applicable not only to victims who can be physically identified but also include children whose faces or identities are digitally replicated using deepfake or generative AI.⁴⁶ While conventional CSAM victims are more clearly recognized under the existing legal framework, children affected by AI-CSAM may face uncertainty regarding their legal recognition as victims, access to remedies, content removal, and recovery mechanisms. The absence of legal protection for unidentified victims, for example, children whose images are manipulated without their knowledge, reflects *de facto* discrimination that places certain groups of children in a more vulnerable position than others.⁴⁷

Nevertheless, no laws currently in force in Indonesia explicitly address AI-CSAM or sexual material synthetically generated using artificial intelligence. This creates a protection gap between victims of conventional CSAM, who are relatively more protected under the Law on Child Protection and the Law on ITE, and victims of AI-CSAM, whose identities are digitally manipulated. In addition, the absence of legal definitions of “virtual victims” or “synthetic victims” in Indonesian positive law may exclude children depicted in AI-CSAM from access to formal recovery mechanisms, thereby creating discrimination based on the form of victimization. Thus, legal provisions in Indonesia have yet to fully align with the non-discrimination standard stipulated in the CRC with respect to the protection of children from AI-CSAM.

b. Best Interest of the Child

Article 3 of the CRC affirms that in all actions concerning children, whether undertaken by public or private social welfare institutions, courts, administrative authorities, or legislative bodies, the best interests of the child shall be a primary consideration.⁴⁸ In the context of AI-CSAM, the state is obliged not only to pursue a repressive-punitive stance toward perpetrators, but also to ensure that all policies are designed with the protection and recovery of children as rights holders as a primary concern.⁴⁹ The principle of the best interests of the child is formally adopted in Article 2(d) of the Law on Child Protection as one of the principles that govern child protection. Article 59 of the Law on Child Protection further regulates the state’s obligation to provide special protection for children who are victims of sexual crimes, including through rehabilitation and social reintegration. However, in practice, Indonesia’s legal provision is more oriented toward the punishment of perpetrators than on the recovery of victims. Article 67 of the Law on TPKS indeed stipulates the rights of victims with regard to handling, protection, and recovery. However, the implementation of this article is constrained by limited budgets, the capacity of human resources in service institutions, and the absence of specific protocols for victims of AI-based technology-enabled sexual violence.⁵⁰

⁴⁶Internet Watch Foundation (IWF), *AI-Generated CSAM: A Threat Assessment* (Cambridge: Internet Watch Foundation, 2023), 6–9; Stanford Internet Observatory, *Generative AI and Child Safety: An Emerging Challenge* (Stanford, CA: Stanford Internet Observatory, 2024), 3–5.

⁴⁷ECPAT International, *Disrupting Harm: Evidence on Online Child Sexual Exploitation and Abuse* (Bangkok: ECPAT, 2021), hlm. 44–47.

⁴⁸United Nations, *Convention on the Rights of the Child*, art. 3(1).

⁴⁹ECPAT International, *Disrupting Harm: Evidence on Online Child Sexual Exploitation and Abuse*, 22–25.

⁵⁰Indonesia, *Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual*, Pasal 67; Lembaga Bantuan Hukum Asosiasi Perempuan Indonesia untuk Keadilan (LBH APIK Jakarta), *Laporan Kekerasan Seksual*

In the specific context of AI-CSAM, this gap is reflected in the absence of technical procedures for victim handling, rapid content takedown, and recovery mechanisms that are responsive to AI-based technology-enabled sexual violence. As a result, the state still bears a substantive obligation in this regard.⁵¹

c. Participation

Article 12 of the CRC acknowledges the right of the child to express their views freely on all matters that affect them, and these views must be accorded due weight in accordance with the child's age and maturity.⁵² The Committee on the Rights of the Child, in General Comment No. 12 (2009), affirms that participation within the framework of the HRBA requires more than a symbolic right to be heard; it requires children's meaningful participation at every stage of the policy cycle relating to their protection.⁵³

In the context of AI-CSAM, the state is obligated to establish child-friendly reporting mechanisms so that children can report experiences of victimization without encountering procedural or psychological barriers.⁵⁴ In addition, the state needs to involve children in the policy-making process through consultations that are safe, structured, and non-retraumatizing. General Comment No. 25 specifically emphasizes that digital policies concerning children must be formulated through active engagement with children as active stakeholders, rather than merely as objects of protection. Normatively, Article 10 of the Law on Child Protection recognizes the child's right to express their views and to have these views heard.

However, children's participation in the formulation of digital policy in Indonesia is almost not institutionalized. There is no systematic child consultation mechanism in legislative processes related to technology and child protection, including in the deliberation of the Law on ITE and the Law on TPKS.⁵⁵ Moreover, existing AI-CSAM reporting mechanisms, such as complaints submitted through the Ministry of Communication and Digital Affairs or reports to the police, have not been designed with child users in mind. These have limited children's rights, not only in terms of being heard in digital policy-making, but also in terms of participating effectively in the enforcement of their own rights.⁵⁶ This condition demonstrates a significant gap between Indonesia's normative commitment and the operational realization of the principle of participation.

d. Accountability

Berbasis Digital 2023 (Jakarta: LBH APIK Jakarta, 2024), 17–19.

⁵¹ECPAT International, *Disrupting Harm: Evidence on Online Child Sexual Exploitation and Abuse*, 59; bandingkan dengan Indonesia, Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

⁵²United Nations, *Convention on the Rights of the Child*, adopted November 20, 1989, entered into force September 2, 1990, 1577 U.N.T.S. 3, art. 12.

⁵³Committee on the Rights of the Child, General Comment No. 12 (2009): *The Right of the Child to Be Heard*, U.N. Doc. CRC/C/GC/12 (July 20, 2009), paras. 3, 12, 27, dan 134.

⁵⁴Convention on the Rights of the Child, adopted November 20, 1989, entered into force September 2, 1990, 1577 U.N.T.S. 3, art. 12.

⁵⁵Committee on the Rights of the Child, General Comment No. 25 (2021) on *Children's Rights in Relation to the Digital Environment*, U.N. Doc. CRC/C/GC/25 (March 2, 2021), paras. 51–56, 80–82.

⁵⁶Committee on the Rights of the Child, General Comment No. 25 (2021) on *Children's Rights in Relation to the Digital Environment*, U.N. Doc. CRC/C/GC/25 (March 2, 2021), paras. 46–49, 51–56, 80–82; ECPAT, INTERPOL, dan UNICEF, *Disrupting Harm in Indonesia: Evidence on Online Child Sexual Exploitation and Abuse* (Bangkok: ECPAT International, 2022), 72–76.

The principle of accountability in the HRBA establishes the state as a duty bearer that must be held accountable for the fulfillment of children's rights. The concept of accountability in this context includes two complementary dimensions: first, internal accountability through monitoring and enforcement mechanisms within the state's legal system; and second, external accountability through the reporting of obligations to international human rights bodies and the responsiveness to the recommendations provided by these bodies.⁵⁷ The United Nations Guiding Principles on Business and Human Rights (UNGPs) further affirm that the state has an obligation to protect children's rights from violations by third parties, including corporate actors that develop and operate AI technologies.⁵⁸

The effective implementation of laws should strengthen coordination among law enforcement agencies, child protection institutions, digital platforms, and other relevant stakeholders.⁵⁹ However, the evaluation of internal accountability has exposed the problem of complex institutional fragmentation in Indonesia. The Ministry of Communication and Informatics (Komdigi) has the authority to block illegal content but does not have a criminal investigation mandate. The Indonesian Child Protection Commission (KPAI) fulfills supervisory and advocacy functions but lacks law enforcement authority. The Cyber Crime Directorate of the Criminal Investigation Agency of the Indonesian National Police has enforcement authority but limited AI-specific digital forensic capacity. The National Cyber and Encryption Agency (BSSN) focuses on national cybersecurity without a specific child protection mandate.⁶⁰ This fragmentation has created an accountability vacuum, as each institution refers matters to the authority of another institution. Consequently, responses to AI-CSAM are at risk becoming slow, fragmented, and uncoordinated, weakening the point of accountability required by the HRBA.⁶¹

A further consequence is that generative AI platforms operating in Indonesia remain largely outside a robust child-protection accountability framework. This creates an accountability gap, as corporate actors may facilitate, host, or enable the circulation of AI-CSAM without being subject to clearly defined duties of care. When viewed through the lenses of the CRC, the OPSC, and the UNGPs, this gap is not merely a regulatory weakness, but a failure of the state to effectively regulate private technology entities in order to prevent foreseeable harms against children in the digital environment.

2.2.2. Analysis of the Obligation to Respect, Protect, and Fulfil

⁵⁷Paul Hunt & Gunilla Backman, "Health Systems and the Right to the Highest Attainable Standard of Health," *Health and Human Rights* 10, No. 1 (2008): 82.

⁵⁸United Nations, *Guiding Principles on Business and Human Rights*, UN Doc. HR/PUB/11/04 (2011), Prinsip 1–3.

⁵⁹Abdul Rahman, Zainal Amin Ayub, dan Ratnawati, "Legal Framework for Protecting Children from Commercial Sexual Exploitation," *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi* 8, no. 1 (2025): 87–110, <https://doi.org/10.24090/volksgeist.v8i1.13156>.

⁶⁰Perpres No. 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital; UU No. 23 Tahun 2002 tentang Perlindungan Anak sebagaimana diubah dengan UU No. 35 Tahun 2014, Pasal 74–76; Sekretariat Negara RI, "Komisi Perlindungan Anak Indonesia," diakses 1 Juni 2026; Kementerian Kominfo RI, "Direktorat Siber Polri, Tameng Hadapi Kejahatan Siber di Era Digital," 27 September 2024; Perpres No. 53 Tahun 2017 tentang Badan Siber dan Sandi Negara sebagaimana diubah dengan Perpres No. 133 Tahun 2017.

⁶¹United Nations Development Group, *The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding Among UN Agencies* (New York: United Nations, 2003).

a. The Basis for State Obligation to Address AI-CSAM

In the context of AI-CSAM, the production, distribution, and consumption of such material are generally committed by private entities, including individuals, technology users, digital platform providers, AI system developers, and electronic service providers. However, the private nature of these entities does not absolve a state of its obligation in this regard. The state, in fact, retains a positive obligation to establish legal, administrative, technical, and institutional systems capable of protecting children from sexual exploitation in the digital environment.

The obligation to respect, protect, and fulfill provides an analytical framework for assessing the extent to which a state has fulfilled its obligations to address AI-CSAM. In the context of child protection, these obligations must also be read together with the CRC, the OPSC, and the general principles of child protection, particularly non-discrimination, the best interests of the child, the child's right to be heard, and the right to protection from all forms of violence and sexual exploitation.⁶²

b. The Obligation to Respect Children's Rights

The obligation **to respect** children's rights requires the state to cease actions that directly or indirectly violate these rights. In the context of AI-CSAM, this obligation means that the state, through its officials, institutions, or policies, must not create, store, disseminate, use, or be permissive of material that sexually exploits children. General Comment No. 13 affirms that a child rights-based approach necessitates the state to respect the dignity and physical and psychological integrity of the child, rather than merely perceiving the child as a passive victim.⁶³ The CRC provides that no child shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, and that every child has the right to legal protection against attacks on their honor and reputation.⁶⁴ In cases of AI-CSAM, the abuse of a child's image, identity, voice, or likeness to create sexual material using AI is a violation of the child's dignity, privacy, and integrity, even in instances where the material does not originate from physical sexual abuse.

The obligation to respect also means that the state must ensure that law enforcement against AI-CSAM is carried out without sacrificing the rights of children as victims. In the context of Indonesia, this obligation is supported by the constitutional guarantee of children's protection from violence and discrimination. However, it has not yet been translated into specific procedures for handling AI-CSAM evidence and for protecting child victims from revictimization during investigation and prosecution.

c. The Obligation to Protect Children's Right

The obligation **to protect** is the most important dimension in the context of AI-CSAM because the majority of violations are committed by non-state actors. This obligation requires the state to prevent, regulate, investigate, punish, and remedy violations of children's rights committed by individuals, groups, technology companies, digital platforms, or electronic service providers.⁶⁵ The state is not only obligated

⁶²United Nations, Convention on the Rights of the Child, adopted November 20, 1989, entered into force September 2, 1990, 1577 U.N.T.S. 3, arts. 2, 3, 12, 19, dan 34; United Nations, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, adopted May 25, 2000, entered into force January 18, 2002, 2171 U.N.T.S. 227, arts. 1–3.

⁶³Committee on the Rights of the Child, General Comment No. 13 (2011): The Right of the Child to Freedom from All Forms of Violence, U.N. Doc. CRC/C/GC/13 (April 18, 2011), paras. 3, 17, 41–44.

⁶⁴United Nations, Convention on the Rights of the Child, art. 16.

⁶⁵Christian Djefal, "Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," *Laws* 11, no. 6 (2022): 84, <https://doi.org/10.3390/laws11060084>

to refrain from directly violating rights, but also to establish an effective protection system against threats originating from third parties. In the context of AI-CSAM, this means ensuring that private entities do not exploit digital technologies in a manner that violates children's dignity, safety, and protection from sexual exploitation.

The obligation imposed on the state to protect requires the state to ensure that criminal law and digital regulation are capable of addressing semi-synthetic material manipulation involving real children, fully synthetic material depicting children or persons appearing to be children, and the use of AI-CSAM for grooming, sexual extortion, or threats against children. The scope of protection cannot be limited to material involving direct physical abuse or an identifiable child victims.

Because the existing instruments do not explicitly regulate synthetic, semi-synthetic, or manipulative AI-CSAM, Indonesia's legal protection obligation remains only partially fulfilled. The state is therefore obligated to undertake legal reform. The proposed reform should include expanding the definition of CSAM to cover synthetic and manipulative representations. Furthermore, the reform should entail the enforcement of legal obligations for technology business entities and electronic information system providers and the establishment of specific procedures for the protection and recovery of child victims.

d. The Obligation to Fulfill Children's rights

The obligation to fulfill children's rights requires the state to take active measures to ensure that children's rights are upheld in reality. In the context of AI-CSAM, this obligation is not sufficiently fulfilled through criminalization. The state is also obligated to establish a protection system that includes prevention, education, reporting, law enforcement, victim recovery, institutional coordination, and supervision of digital actors. Therefore, the obligation to fulfill children's rights concerns its institutional and operational capacity to ensure effective child protection in the digital environment.

In addressing the problem of AI-CSAM, the state's obligation to fulfill children's rights can be translated into four measures. The first measure to be implemented by the state is the provision of reporting mechanisms that are accessible, child-friendly, safe, and responsive to victims. Children or their legal representatives must be assured of the ability to report AI-CSAM without fear of being blamed, humiliated, or revictimized. The second measure is to ensure the availability of a content removal mechanism that is fast and effective, because the dissemination of digital material can cause repeated and long-term harm. The third measure is to provide victims with recovery services, including legal assistance, psychological support, social rehabilitation, and identity protection. The fourth measure necessitates the state to enhance the capacity of law enforcement officials and child protection institutions. This capacity enhancement is to ensure that these entities understand the characteristics of AI technology, digital evidence, and the protection of child victims.

A closer look at AI-CSAM reveals the key question of whether Indonesia's public protection system is sufficiently adaptable to forms of sexual violence that do not always occur physically but may cause serious harm through digital manipulation, content dissemination, and the exploitation of children's identities.⁶⁶ Therefore, the obligation to fulfill children's rights requires the establishment of an integrated public protection system linking criminal law, child protection, personal data protection,

⁶⁶Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual, arts. 66–70; Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak sebagaimana diubah dengan Undang-Undang Nomor 35 Tahun 2014, arts. 59, 59A, 69A.

digital platform governance, digital literacy, and victim recovery. Effective assistance for children and women affected by violence also requires sustainable institutional cooperation, adequate funding, advocacy, and supportive policy development.⁶⁷

e. Evaluation of the Fulfillment of State Obligations

Indonesia's legal framework shows that the state has only partially fulfilled its obligations to protect children from CSAM and AI-CSAM. Instruments such as the Law on Child Protection, the Law on Pornography, the Law on ITE, the Law on TPKS, and the Law on Personal Data Protection are in place to address these problems. However, these instruments have not been specifically designed to address the synthetic, manipulative, easily reproducible, and ecosystem-based characteristics of AI-CSAM.

The obligation to uphold children's rights has been fulfilled only at a general normative level. Although Indonesia has constitutional and statutory provisions for the protection of children from violence and discrimination, these provisions have not yet been operationalized into AI-CSAM-sensitive procedures.⁶⁸ The fulfillment of the obligation to uphold children's rights is not yet fully adequate when viewed in relation to the AI-CSAM problem because there is no specific protocol regarding the handling of digital evidence containing AI-based child sexual material.⁶⁹ While Indonesia substantive law acknowledges the use of electronic evidence, its procedural law lacks specific standards for evaluating the authenticity, integrity, traceability, reliability, identity attribution, and accountability of AI-generated material.⁷⁰ The potential for AI-CSAM, especially that abuses the biometric data, such as face, body, and voice, or identity of a real child, to cause revictimization if not stored, analyzed, or redistributed with strict protection standards, is a relevant concern. Previous scholarship has observed that Indonesian criminal law does not yet specifically regulate online sexual crimes against children.⁷¹ Therefore, the state is obligated to guarantee that the investigative process, the collection of evidence, and enforcement of law pertaining to AI-CSAM do not prolong the suffering of victims or treat children merely as objects of evidence.⁷²

The state's partial fulfillment of its obligation to protect children from third parties is further demonstrated in the Law on Child Protection, the Law on Pornography, the Law on ITE Law, the Law on TPKS, and the Law on Personal Data Protection. The main limitation of these legal provisions lies in the absence of a specific definition of CSAM and AI-CSAM. As a result, the existing morality- and decency-based frameworks remain insufficient to categorize AI-CSAM as a form of sexual violence involving exploitation, revictimization, privacy violations, and the need for recovery.⁷³

Furthermore, the legal obligations of digital platforms and AI developers has not yet been clearly formulated in Indonesian law. General Comment No. 25 asserts the obligation of the state to guarantee that digital companies carry out due diligence in relation to children's rights and prevent their services from being abused to harm

⁶⁷ulianti Muthmainnah, Zakiyuddin Baidhaw, Yusron Razak, and Ilham Mundzir, "Zakat Initiatives for Supporting Victims of Violence against Women and Children in Indonesia," *Ijtihad: Jurnal Wacana Hukum Islam dan Kemanusiaan* 24, no. 2 (2024): 331–357, <https://doi.org/10.18326/ijtihad.v24i2.331-357>.

⁶⁸ulianti Muthmainnah, Zakiyuddin Baidhaw, Yusron Razak, and Ilham Mundzir

⁶⁹Dushi, "The Legal Framework and Legal Gaps"; Ciardha, "AI-Generated Child Sexual Abuse Material."

⁷⁰Hendri Antoro, Danrivanto Budhijanto, and Somawijaya, "Admissibility of Artificial Intelligence as Electronic Evidence: Comparative Perspectives from Indonesia, the United States, and Japan," *Jurnal IUS Kajian Hukum dan Keadilan* 14, no. 1 (2026): 122–139, <https://doi.org/10.29303/ius.v14i1.1880>.

⁷¹Sri Rahayu, Monalisa, Yulia Monita, dan Melyana Sugiharto, "Legal Protection for Children in Cases of Online Sexual Abuse: A Comparative Study," *Jambe Law Journal* 5, no. 1 (2022): 91–92, <https://doi.org/10.22437/jlj.v5i1.18164>.

⁷²UN Committee on the Rights of the Child, *General Comment No. 25*.

⁷³Regulation (EU) 2024/1689, Artificial Intelligence Act.

children. Literature on AI and CSAM governance also shows that effective regulation must impose obligations on system providers as well as end users. Therefore, the obligation to protect children's rights in Indonesia can be said to have been fulfilled only in a limited manner. This is because, while the state has had a legal basis to take action against certain acts, it does not yet have a protection regime that is explicit, comprehensive, and adaptable to AI-CSAM.

The obligation to fulfill children's rights has not yet been adequately realized. Despite the recognition of victims' rights to protection, handling, and recovery in the Law on Child Protection and the Law on TPKS, Indonesia has not yet established specific mechanisms for child-friendly reporting, rapid takedown, victim recovery, digital literacy, law enforcement capacity-building, and institutional coordination with regard to AI-CSAM. These vulnerabilities are further exacerbated by the limited capacity of law enforcement and child protection institutions to handle deepfakes, generative models, metadata, datasets, digital storage systems, and visual manipulation.⁷⁴ These vulnerabilities may hinder victim identification, collecting evidence of criminal elements, tracing perpetrators, cooperating with digital platforms, and preventing revictimization.⁷⁵

In summary, Indonesia's fulfillment of obligations in addressing AI-CSAM can be characterized as partial and fragmented. The state has acknowledged its general obligation to protect children from sexual exploitation, but it has not yet established a specific, integrated, and technologically adaptable protection regime. This indicates the need for legal reform that formally acknowledges AI-CSAM, expands the definition of CSAM to include semi-synthetic and fully synthetic material, establishes regulations for technology business entities, and institutes child-centered mechanisms for reporting, takedown, investigation, and recovery.⁷⁶

3. CONCLUSION

The legal framework in Indonesia for CSAM has not yet fully been able to address the phenomenon of artificial intelligence-generated child sexual abuse material (AI-CSAM). Although there has been several relevant legal instruments in Indonesia, such as the Law on Child Protection, the Law on Pornography, the Law on Electronic Information and Transactions (ITE), the Law on Sexual Violence Crimes (TPKS), and the Law on Personal Data Protection (PDP), these instruments are still fragmented and do not explicitly recognize AI-CSAM as a specific form of technology-enabled child sexual exploitation. As a result, forms of AI-CSAM, such as child sexual deepfakes, semi-synthetic content, fully synthetic content, and prompt-based generation, the use of CSAM datasets, and the obligations of AI platforms and AI developers, have not yet been adequately regulated.

From the perspective of the human rights-based approach, this condition shows that the fulfillment of the obligations to uphold children's rights by Indonesia as a state is still partial. The principles of non-discrimination, the best interests of the child, participation, and accountability have not yet been fully realized in the protection of children from AI-

⁷⁴Kimberly J. Mitchell et al., "Identifying Subtypes of Image-Based Sexual Abuse and Their Associations with Harms," *Child Abuse & Neglect* 160 (2025): 107205; Internet Watch Foundation, *How AI Is Being Abused to Create Child Sexual Abuse Imagery* (Cambridge: Internet Watch Foundation, 2023).

⁷⁵Caoilte Ó. Ciardha, "AI-Generated Child Sexual Abuse Material: What's the Harm?," *AI & Society* (2026); Dren Dushi, "The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material," *Computer Law & Security Review* 57 (2025).

⁷⁶United Nations Committee on the Rights of the Child, *General Comment No. 25*, paras. 36–40, 43–46; Dushi, "The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material."

CSAM. The absence of child-friendly reporting mechanisms, fast takedown mechanisms, victim recovery protocols, and effective institutional coordination indicates that the existing legal protection is not yet sufficiently adaptable to the characteristics of AI-CSAM, which is readily produced, disseminated, and repeatedly consumed.

To address these vulnerabilities, Indonesia must update its legal framework by expanding the definition of CSAM to include AI-generated content, both semi-synthetic and fully synthetic. Additionally, the government must expressly criminalize the creation, procurement, possession, and distribution of AI-CSAM. Furthermore, AI developers and technology companies must adhere to a safety-by-design approach, strengthen detection systems, preclude the circulation of AI-CSAM, and expedite the process of AI-CSAM content removal. This update is important for the state to be able to fulfill its obligations to respect, protect, and fulfill children's rights effectively in accordance with international human rights law standards.

REFERENCES

- Amalia, Ayu Riska, Diva Pitaloka, and Adhitya Nini Rizki Apriliana. "Gender Discrimination in Artificial Intelligence: An International Human Rights Law Perspective and the Quest for Binding Regulation." *Unram Law Review* 9, no. 2 (2025): 311–333. <https://doi.org/10.29303/ulrev.v9i2.450>.
- Antoro, Hendri, Danrivanto Budhijanto, and Somawijaya. "Admissibility of Artificial Intelligence as Electronic Evidence: Comparative Perspectives from Indonesia, the United States, and Japan." *Jurnal IUS Kajian Hukum dan Keadilan* 14, no. 1 (2026): 122–139. <https://doi.org/10.29303/ius.v14i1.1880>.
- Armiwulan, Hesti, Rofi Aulia Rahman, Valentino Nathanael Prabowo, and József Hajdú. "Artificial Intelligence and Its Challenges to Elections in Indonesia: A Legal Analysis." *Jambura Law Review* 6, no. 2 (2024): 264–285. <https://doi.org/10.33756/jlr.v6i2.24243>.
- Ayalew, Yohannes Eneyew, Valerie Verdoodt, and Eva Lievens. "General Comment No. 25 on Children's Rights in Relation to the Digital Environment: Implications for Children's Right to Privacy and Data Protection in Africa." *Human Rights Law Review* 24, no. 3 (2024).
- Brown, Rick, et al. "Artificial Intelligence and Child Sexual Abuse: A Rapid Evidence Assessment." *Trends & Issues in Crime and Criminal Justice*, no. 711 (2025). https://www.aic.gov.au/sites/default/files/2025-01/ti711_artificial_intelligence_and_child_sexual_abuse.pdf
- Carr, John. "Child Abuse, Child Pornography and the Internet." *International Review of Law, Computers & Technology* 18, no. 2 (2004): 169–184.
- Christensen, L. S., D. Moritz, and A. Pearson. "Psychological Perspectives of Virtual Child Sexual Abuse Material." *Sexuality & Culture* 25 (2021): 1354–1368. <https://doi.org/10.1007/s12119-021-09820-1>
- Ciardha, Caoilte Ó., John Buckley, and Rebecca S. Portnoff. "AI-Generated Child Sexual Abuse Material: What's the Harm?" *AI & Society* (2026). <https://doi.org/10.1007/s00146-026-02932-y>.

- Committee on the Rights of the Child. *Concluding Observations on the Combined Fifth and Sixth Periodic Reports of Indonesia*. U.N. Doc. CRC/C/IDN/CO/5-6. July 28, 2025.
- Committee on the Rights of the Child. *General Comment No. 12 (2009): The Right of the Child to Be Heard*. U.N. Doc. CRC/C/GC/12. July 20, 2009.
- Committee on the Rights of the Child. *General Comment No. 13 (2011): The Right of the Child to Freedom from All Forms of Violence*. U.N. Doc. CRC/C/GC/13. April 18, 2011.
- Committee on the Rights of the Child. *General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration*. U.N. Doc. CRC/C/GC/14. May 29, 2013.
- Committee on the Rights of the Child. *General Comment No. 20 (2016) on the Implementation of the Rights of the Child during Adolescence*. U.N. Doc. CRC/C/GC/20. December 6, 2016.
- Committee on the Rights of the Child. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*. U.N. Doc. CRC/C/GC/25. March 2, 2021.
- Committee on the Rights of the Child. *Guidelines regarding the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*. U.N. Doc. CRC/C/156. September 10, 2019.
- Danaher, John. "The Law and Ethics of Deepfakes." *Oxford Journal of Legal Studies* 37, no. 3 (2017): 534–561. <https://doi.org/10.1093/ojls/gqw033>
- Djeffal, Christian "Children's Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," *Laws* 11, no. 6 (2022): 84, <https://doi.org/10.3390/laws11060084>
- Dushi, Desara, Nertil Berdufi, and Anastasia Karagianni. "The Legal Framework and Legal Gaps for AI-Generated Child Sexual Abuse Material." *Computer Law & Security Review* 59 (2025): 106205.
- Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act." *European Journal of Risk Regulation* 16, no. 2 (2025): 684–703.
- ECPAT International. *Disrupting Harm: Evidence on Online Child Sexual Exploitation and Abuse*. Bangkok: ECPAT International, 2021.
- ECPAT, INTERPOL, and UNICEF. *Disrupting Harm in Indonesia: Evidence on Online Child Sexual Exploitation and Abuse*. Bangkok: ECPAT International, 2022.
- European Parliament and Council of the European Union. *Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence*. Official Journal of the European Union, L 2024/1689. July 12, 2024.
- Foster, Jennifer. "Pixelated Harm: An Analysis of the Impact of AI-Generated Images on CSAM Criminalization and Child Safety." *Oklahoma City University Law*

Review 49, no. 3 (2025): 425–440.

Global Partnership to End Violence Against Children. “Generative AI and Child Sexual Abuse Material (CSAM).” *Global Child Exploitation Policy and Advocacy Centre*. Accessed May 5, 2026. <https://www.globalchildexploitationpolicy.org/policy-advocacy/generative-ai-csam>

Henry, Nicola, and Anastasia Powell. “Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research.” *Trauma, Violence, & Abuse* 19, no. 2 (2018): 195–208. <https://doi.org/10.1177/1524838016650189>

Hunt, Paul, and Gunilla Backman. “Health Systems and the Right to the Highest Attainable Standard of Health.” *Health and Human Rights* 10, no. 1 (2008): 81–92.

Indonesia. *Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat*.

Indonesia. *Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara*.

Indonesia. *Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara*.

Indonesia. *Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital*.

Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.

Indonesia. *Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Lembaran Negara Republik Indonesia Tahun 2002 Nomor 109. Tambahan Lembaran Negara Republik Indonesia Nomor 4235.

Indonesia. *Undang-Undang Nomor 35 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2002 tentang Perlindungan Anak*. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 297.

Indonesia. *Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi*.

Indonesia. *Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 120. Tambahan Lembaran Negara Republik Indonesia Nomor 6792.

Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024.

Interagency Working Group in Luxembourg. *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. 2nd ed. Luxembourg: ECPAT International, 2025. <https://icmec.org.au/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf>

Interagency Working Group on Sexual Exploitation of Children. *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. Luxembourg: ECPAT International, 2016.

- Internet Watch Foundation. *AI-Generated CSAM: A Threat Assessment*. Cambridge: Internet Watch Foundation, 2023.
- Internet Watch Foundation. *How AI Is Being Abused to Create Child Sexual Abuse Imagery*. Cambridge: Internet Watch Foundation, 2023.
- Kementerian Kominfo RI. “Direktorat Siber Polri, Tameng Hadapi Kejahatan Siber di Era Digital.” September 27, 2024.
- Kementerian Komunikasi dan Digital Republik Indonesia. “Pemerintah Putus Akses Sementara Grok demi Lindungi Masyarakat di Ruang Digital.” DJED Komdigi. Accessed April 21, 2026. <https://djed.komdigi.go.id/news/pemerintah-putus-akses-sementara-grok-demi-lindungi-masyarakat-di-ruang-digital>.
- Lazaridou, Maria. *The Criminalization of AI-Generated Child Sexual Abuse Material: Challenges and Prospects under International and European Law*. Master’s thesis, Utrecht University, 2024. https://studenttheses.uu.nl/bitstream/handle/20.500.12932/48359/Master_Thesis_Maria_Lazaridou.pdf
- Lembaga Bantuan Hukum Asosiasi Perempuan Indonesia untuk Keadilan. *Laporan Kekerasan Seksual Berbasis Digital 2023*. Jakarta: LBH APIK Jakarta, 2024.
- Loney-Howes, Rachel. “Technology-Facilitated Re-Victimization: How Video Evidence of Sexual Violence Can Harm Survivors.” *Theoretical Criminology* 27, no. 1 (2023): 94–112.
- McGlynn, Clare, and Erika Rackley. “Image-Based Sexual Abuse.” *Oxford Journal of Legal Studies* 37, no. 3 (2017): 534–561. <https://doi.org/10.1093/ojls/gqw033>
- McGlynn, Clare, Erika Rackley, and Ruth Houghton. “Beyond ‘Revenge Porn’: The Continuum of Image-Based Sexual Abuse.” *Feminist Legal Studies* 25, no. 1 (2017): 25–46. <https://doi.org/10.1007/s10691-017-9343-2>
- Mertokusumo, Sudikno. *Penemuan Hukum: Sebuah Pengantar*. Yogyakarta: Liberty, 2007.
- Mitchell, Kimberly J., Ateret Gewirtz-Meydan, Lisa M. Jones, David Finkelhor, and Heather A. Turner. “Identifying Subtypes of Image-Based Sexual Abuse and Their Associations with Harms.” *Child Abuse & Neglect* 160 (2025): 107205.
- Muthmainnah, Yulianti, Zakiyuddin Baidhawiy, Yusron Razak, and Ilham Mundzir. “Zakat Initiatives for Supporting Victims of Violence against Women and Children in Indonesia.” *Ijtihad: Jurnal Wacana Hukum Islam dan Kemanusiaan* 24, no. 2 (2024): 331–357. <https://doi.org/10.18326/ijtihad.v24i2.331-357>.
- Parti, Katalin, and Judit Szabó. “The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe.” *Laws* 13, no. 67 (2024). <https://doi.org/10.3390/laws13060067>.
- Paul, Bryant, and Daniel G. Linz. “The Effects of Exposure to Virtual Child Pornography on Viewer Cognitions and Attitudes toward Deviant Sexual Behavior.” *Communication Research* 35, no. 1 (2008): 3–38. <https://doi.org/10.1177/0093650207309359>
- Pocol, A., et al. “Seeing Is No Longer Believing: A Survey on the State of Deepfakes, AI-

- Generated Humans, and Other Nonveridical Media.” In *Advances in Computer Graphics*, edited by B. Sheng, L. Bi, et al., 434. Lecture Notes in Computer Science 14496. Cham: Springer, 2023. https://doi.org/10.1007/978-3-031-50072-5_34
- Quayle, Ethel, and Thomas Jones. “The Challenges of Identifying and Classifying Child Sexual Abuse Material.” *Sexual Abuse* 31, no. 2 (2019): 173–196. <https://doi.org/10.1177/1079063217724768>.
- Rahayu, Sri, Monalisa, Yulia Monita, and Melyana Sugiharto. “Legal Protection for Children in Cases of Online Sexual Abuse: A Comparative Study.” *Jambe Law Journal* 5, no. 1 (2022): 91–92. <https://doi.org/10.22437/jlj.v5i1.18164>.
- Rahman, Abdul, Zainal Amin Ayub, and Ratnawati. “Legal Framework for Protecting Children from Commercial Sexual Exploitation.” *Volksgeist: Jurnal Ilmu Hukum dan Konstitusi* 8, no. 1 (2025): 87–110. <https://doi.org/10.24090/volksgeist.v8i1.13156>.
- Ramadhani, Evyta Rosiyanti, Ayudya Rizqi Rachmawati, and Roro Hera Kurnikova. “Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia.” *De Jure: Jurnal Hukum dan Syar’iah* 17, no. 1 (2025): 118–119. <https://doi.org/10.18860/j-fsh.v17i1.28880>.
- Salter, Michael. “Child Sexual Abuse Material and the Digital Economy.” *New Media & Society* 25, no. 9 (2023): 2277–2295.
- Sekretariat Negara Republik Indonesia. “Komisi Perlindungan Anak Indonesia.” Accessed June 1, 2026.
- Septianita, Hesti, Pujiyono, and Irma Cahyaningtyas. “Online Child Sexual Exploitation and Abuse as Organized Crime: Towards a New International Legal Framework.” *Jurnal Litigasi* 27, no. 1 (2026): 1–25. <https://doi.org/10.23969/litigasi.v27i1.43221>.
- Stanford Internet Observatory. *Generative AI and Child Safety: An Emerging Challenge*. Stanford, CA: Stanford Internet Observatory, 2024.
- UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO, 2021.
- UNICEF. *Guidance on AI and Children*. 3rd ed. New York: UNICEF, 2025.
- United Nations. *Convention on the Rights of the Child*. New York: United Nations, 1989.
- United Nations. *Guiding Principles on Business and Human Rights*. U.N. Doc. HR/PUB/11/04. 2011.
- United Nations. *International Covenant on Civil and Political Rights*. New York: United Nations, 1966.
- United Nations. *Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*. New York: United Nations, 2000.
- United Nations Development Group. *The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding among UN Agencies*. New York: United Nations, 2003.

United Nations Interregional Crime and Justice Research Institute. *Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse*. Turin: UNICRI, 2024. <https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf>.

United Nations Office on Drugs and Crime. *United Nations Convention against Cybercrime*. Adopted by U.N. General Assembly Resolution 79/243. December 24, 2024.

United Nations Sustainable Development Group. "Human Rights-Based Approach." Accessed May 5, 2026. <https://unsdg.un.org/2030-agenda/universal-values/human-rights-based-approach>.

U.S. Department of Justice. *Child Sexual Abuse Material*. Washington, DC: U.S. Department of Justice, 2023. <https://www.justice.gov/d9/2023-06/child-sexual-abuse-material-2.pdf>.

WeProtect Global Alliance. *Global Threat Assessment 2023 Press Release*. October 17, 2023.