Mataram Journal of International Law
Volume 4, No. 1, June 2026
open access at : https://journal.unram.ac.id/index.php/majil/index
Department of Law, Faculty of Law, University of Mataram

THE URGENCY OF RATIFICATION OF THE UNITED NATIONS CONVENTION AGAINST CYBERCRIME IN THE ERADICATION OF CRIMES RELATED TO ONLINE SEXUAL VIOLENCE AGAINST CHILDREN IN INDONESIA

Muhammad Haikal Bassam
University of Mataram
E-mail: haikalthehuman@gmail.com

Erlies Septiana Nurbani
University of Mataram
E-mail: erliesseptiana@unram.ac.id

Abstract

The threat of child sexual exploitation in the digital space is transnational and continues to increase, requiring the strengthening of a more progressive national legal framework. This study aims to analyze the limitations of national legal instruments in addressing online child sexual abuse crimes and to examine the urgency of ratifying the United Nations Convention against Cybercrime (UNCC) as a strategic step in combating these crimes. The research questions in this study focus on the regulation of child protection and the criminal liability of perpetrators of child sexual violence in current national law, as well as the significance of ratifying the UNCC in strengthening cross-border law enforcement jurisdiction. Using a doctrinal legal research method with a legislative, comparative, and case-based approach, the researcher mapped the norms of the ITE Law, the Child Protection Law, the TPKS Law, and international instruments such as the ICCPR, CRC, Budapest Convention, and UNCC. The results of the study show that national legal regulations are still sectoral, reactive-territorial, and have legal loopholes in criminalizing acts such as psychological manipulation carried out by perpetrators to build trust with children for the purpose of sexual violence (child grooming) and sexually violent material produced using technology (deepfake). In addition, dependence on bureaucratic Mutual Legal Assistance (MLA) procedures is a significant operational obstacle. In conclusion, the ratification of the UNCC is an urgent necessity to close the normative gap through the standardization of criminal acts (as in Articles 14 and 15) and the provision of a special (fast-track) access to digital evidence across jurisdictions in order to ensure maximum protection for Indonesian children in the global cyberspace.

Keyword : Child Sexual Abuse Material; Electronic Information and Transactions Law; ; Ratification

A. INTRODUCTION

The rapid development of information technology has fundamentally changed the pattern of global interaction. This allows cross-border data exchange to take place without any real physical boundaries. However, this progress has given birth to *cyberspace* as a new arena of complex crimes that are difficult to reach by a country's traditional jurisdiction. One of the most serious threats in international law is *Child Sexual Abuse Material* (CSAM). The term CSAM is now used globally to replace the term child pornography because it is considered more appropriate in emphasizing aspects of violence, exploitation, and psychological suffering of child victims. This phenomenon

DOI: https://doi.org/10.29303/n3p3q604

not only threatens the security of individuals, but also tests the effectiveness of national law and the strength of international cooperation.[1]

The escalation of CSAM as a transnational crime shows a very worrying trend. The *National Center for Missing and Exploited Children* report through *CyberTipline* recorded that there were 35.9 million reports of alleged online child sexual abuse in 2023. This figure increased by 18.4 % compared to 2021.[2] The fact that 91.7 % of the report came from outside the United States underscores the cross-border dimension that demands global law enforcement synergy. It is estimated that there are 300 million children or around 12.5 % of the world's child population who are victims of online sexual exploitation every year. This challenge is complicated by the use of *Generative Artificial Intelligence* (GAI) which is able to create *fake* fake children and fictional children. In addition, the use of *end-to-end encryption* paradoxically makes it difficult for the authorities to detect and track the traces of criminals.[3]

Indonesia is currently in a state of national emergency related to child protection in the digital space. The Ministry of Communication and Information Technology report in 2024 places Indonesia in third place in the world with more than 1.45 million cases of online child sexual exploitation. However, law enforcement in Indonesia faces significant obstacles due to the limitations of national legal instruments.[4]The Electronic Information and Transaction Law (ITE Law), especially Article 27 paragraph (1) of Law Number 1 of 2024, still uses a general approach through the term violating morality which refers to *contemporary community standards*. This definition creates legal uncertainty, especially in AI-generated material that does not involve real children physically. Although the ITE Law and the Child Protection Law are complementary to each other, they do not specifically regulate AI technology and effective sanction mechanisms for Electronic System Operators (PSEs).[5]

Jurisdictional constraints and lack of harmonization of international regulations are the main obstacles in transnational cases where the perpetrators, victims, and storage media are in different countries. In response to this vacuum, the UN General Assembly in 2024 adopted the *United Nations Convention Against Cybercrime*. The Convention is the first international instrument to comprehensively regulate global cooperation, including the obligation to criminalize CSAM in Article 14. The advantage of this convention lies in the stronger framework of extradition procedures and mutual legal assistance than current domestic regulations.[6]

Article 14 of the convention extends protection through phrases that describe, describe or represent anyone under the age of 18. This provision is very crucial for Indonesia because it covers materials that are produced digitally without any factual physical victims. This closes the legal loophole related to the content of artificial intelligence

1 K. Parti dan J. Szabó. (2024). "The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe". *Laws*, 13(6): 3–4.

2 National Centre for Missing & Exploited Children. (2023). *CyberTipline 2023 Report*.

3 Childlight. (2024). *Over 300 Million Children a Year are Victims of Technology-Facilitated Sexual Exploitation and Abuse*. *Global Child Safety Institute*.

4 Ministry of Communication and Information of the Republic of Indonesia. (2025). "Record 1.45 Million Cases of Online Child Sexual Exploitation, Nezar Patria: Digital Literacy and AI Regulation as the Key to Protection". *Press Release No. 188/HM-KKD/10/2025*.

5 M. Martono, M. G. G. Akbar, dan H. Rahmatiar. (2025). "Law Enforcement of Transnational Cybercrime: Case Study in Indonesia". 10: 280.

6 P. Hartono, et al. (2024). "Challenges of Criminal Investigation Cyber Crime". *Awang Long Law Review*, 7(1): 1.

engineering. The focus of the regulation now shifts to the criminal responsibility of the perpetrator who creates or distributes the sexual representation of the child.[7]

Therefore, the ratification of the *United Nations Convention Against Cybercrime* is a normative urgency for Indonesia. This ratification has the potential to strengthen the domestic legal framework by harmonizing the definition of cybercrime, establishing procedural standards for data access, and closing legal loopholes related to artificial intelligence-based exploitation. Through this harmonization, Indonesia is expected to increase its law enforcement capacity to provide more optimal protection for future generations in the increasingly complex digital era.

Based on the above background, the problems that will be discussed in this study are: 1. How is the regulation of criminal acts related to child sexual violence according to the national legal framework? 2. What is the urgency of ratifying the *United Nations Convention against Cybercrime* for Indonesia in strengthening the national legal framework to eradicate the crime of online child sexual violence?

B. METHOD

Penelitian ini menggunakan analisis hukum normatif dengan pendekatan perundang-undangan, komparatif, dan kasus melalui pemetaan norma terhadap bahan hukum primer nasional dan internasional, seperti ICCPR, CRC, dan fokus utama pada *United Nations Convention against Cybercrime*. Analisis dilakukan dengan membandingkan definisi tindak pidana, mekanisme bukti elektronik lintas yurisdiksi, serta kewenangan penegak hukum, khususnya merujuk pada Pasal 14 dan 15 Konvensi terkait materi kekerasan seksual anak dan *child grooming*.

Dengan teknik deskriptif-analitis, penelitian ini menyintesis bahan hukum primer dan sekunder untuk mengidentifikasi kesenjangan normatif serta prosedural antara regulasi domestik (UU ITE, UU Perlindungan Anak, UU TPKS, dan PP No. 17 Tahun 2025) dengan standar internasional guna merumuskan kebutuhan harmonisasi dan penguatan kerangka hukum nasional dalam penanganan kejahatan siber lintas negara.

C. ANALYSIS AND DISCUSSION

1. Normative Basis and National Legal Framework Governing the Crime of Child Sexual Violence

1.1 Law Number 1 of 2024 concerning the Second Amendment to the ITE Law

The Government of Indonesia responded to the complexity of cybercrime by establishing Law Number 1 of 2024 as the second amendment to the ITE Law. This regulatory update fundamentally strengthens the legal framework for dealing with crimes in the digital space through a more comprehensive approach, covering preventive, administrative, and repressive aspects. In the context of child protection, Article 27 paragraph (1) of the ITE Law is the primary *legal tool* to ensnare the circulation of *Child*

7 The United Nations, *Convention Against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, 2024, G.A. Res. 79/243, Annex. https://undocs.org/A/RES/79/243.

Sexual Abuse Material (CSAM) through the prohibition of the distribution of electronic information that violates morality.[8]

Normatively, the use of the phrase "make accessible" in Article 27 paragraph (1) reflects legislative efforts to close a technical loophole for perpetrators who facilitate illegal content, even though they are not the primary creators of the material. However, the use of the general term "decency" triggers a discourse about the urgency of the specification of child sexual violence offenses. This is crucial so that the handling of CSAM is not trapped in a subjective morality interpretation, but is seen as a crime against humanity that is in line with international standards.

Furthermore, Law No. 1 of 2024 introduces a breakthrough through Article 40A which regulates the Government's responsibility in building a secure digital ecosystem. This provision gives the government administrative authority to order Electronic System Operators (PSEs) to take certain actions, including cutting off access to illegal content. This PSE obligation creates a system of collective responsibility; Platforms that allow CSAM to circulate can be subject to severe administrative sanctions, ranging from fines to operational termination. This mechanism allows for quick intervention without having to wait for a lengthy criminal justice process, so that the distribution chain of exploitative content can be disconnected immediately from the source.

This legal synergy is emphasized by criminal sanctions in Article 45 paragraph (1) which targets personal liability with *the* threat of imprisonment for up to six years and a fine of one billion rupiah. The merger of administrative supervision in Article 40A and criminal law enforcement in Article 45 paragraph (1) creates a layered protection mechanism. This legal construction shows that there is synchronization with the spirit of *the United Nations Convention against Cybercrime*, which demands accountability not only from physical perpetrators, but also from digital platform managers in mitigating the circulation of child sexual violence materials online.[9]

1.2 Law Number 35 of 2014 concerning Child Protection

Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak berfungsi sebagai fundamen yuridis dalam menjamin hak fundamental anak, termasuk proteksi terhadap integritas fisik dan moral di ranah daring.[10] Pasal 15 huruf f menetapkan mandat bagi negara untuk melindungi anak dari kejahatan seksual. Namun, secara normatif, pasal ini masih bersifat konvensional dan cenderung berfokus pada kekerasan fisik. Dalam dimensi digital, diperlukan penafsiran progresif terhadap Pasal 76E sebagai "pasal induk" yang melarang tipu muslihat atau rangkaian kebohongan untuk membujuk anak melakukan perbuatan cabul. Unsur "membujuk" dalam pasal ini menjadi pintu masuk krusial bagi aparat penegak hukum untuk menjerat praktik *cyber grooming*, di mana predator membangun keterikatan emosional melalui media sosial sebelum terjadinya kekerasan fisik.

---

8 M. A. M. Bastian, R. Sutanto, and Raden. (2024). "Evaluation of the Effectiveness of Law No. 1 of 2024 concerning Information and Electronic Transactions in the Prevention of Cyberterrorism". *Journal of Law of the Pulpit of Justitia (JHMJ),* 10(2): 432.

9 Indonesia, *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions*, Article 27 paragraphs (1) and (2).

10 S. Ramadhani, et al. (2025). "Perlindungan Hukum terhadap Hak Privasi Anak yang Dipublikasikan di Media Massa Menurut Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak". *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh*, 8(2).

In addition to the aspect of harassment, Article 76I provides strict limits on sexual and economic exploitation. In the context of cybercrime, this article is a vital instrument to crack down on the phenomenon of commercialization of children's sexual material, such as forcing the delivery of content through *video call sex* (VCS) for sale or dissemination. This construction is in line with the mandate of Article 14 *of the United Nations Convention against Cybercrime* regarding the criminalization of the production and distribution of child sexual exploitation material. However, the challenge of law enforcement remains in the actions of perpetrators who have not escalated into direct physical violence, thus demanding more specific regulatory harmonization.

As a form of strict action, Article 82 and Article 88 stipulate severe criminal sanctions with a special minimum threat system (5 years) and fines of up to five billion rupiah. The existence of one-third criminal penalty for guardians or educators in Article 82 paragraph (2) emphasizes that the abuse of trust against children is a serious offense. The synergy between the norms of the ban and the severity of these sanctions creates a layered protection mechanism that aims to provide a deterrent effect as well as justice for victims, ensuring that every form of child manipulation and exploitation on digital platforms has real legal consequences.[11]

1.3 Law Number 12 of 2022 concerning the Crime of Sexual Violence (TPKS Law)

The presence of Law Number 12 of 2022 concerning the Crime of Sexual Violence (TPKS Law) marks a major evolution in Indonesia's positive law[12] by introducing a special offence for Electronic-Based Sexual Violence (KSBE). Through Article 14, this regulation criminalizes the act of recording, transmission, and electronic stalking with sexual content that are carried out without consent. In the context of child protection, Article 14 has double significance as in paragraph (3) it is emphasized that KSBE against children is an ordinary offense, so that law enforcement does not depend on the victim's complaint, then in paragraph (5) it is emphasized that the consent of the child victim does not abolish criminal charges. This construction automatically aborts the "consensual" pretext often used by perpetrators of digital manipulation or *cyber grooming* to avoid legal trapping, while aligning national law with the mandate of the *United Nations Convention against Cybercrime*.

The accountability system in the TPKS Law also shows a holistic criminal policy by combining criminal sanctions of imprisonment and significant fines. This aims to provide economic deterrence for perpetrators while acknowledging the impact of profound immaterial losses on child victims. Furthermore, Article 15 paragraph (1) letter d regulates the criminal burden of one-third if the criminal act is committed by a party who has a power relationship, such as a public official, employer, or superior. This provision is particularly relevant to close the loophole for abuse of authority in a formal work or parenting environment that forces children or adolescents to engage in the creation of electronic sexual material. This charge views the act as not just ordinary sexual violence, but a betrayal of professional responsibility and public trust.

11 Indonesia, *Law No. 35 of 2014 concerning Amendments to Law No. 23 of 2002 concerning Child Protection*.

12 A. Pratama, O. S. Mandala, and A. Rahmatyar. (2025). "Analysis of the Implementation of the Policy for the Protection of Children Victims of Sexual Violence in Indonesia in Law Number 12 of 2022 concerning the Crime of Sexual Violence". *Journal of Law*, 4.

The TPKS Law shifts the legal paradigm from retributive to restorative through the mandate of restitution rights regulated in Article 30. Child victims are entitled to compensation for loss of wealth, medical treatment costs, and psychological recovery charged directly to the perpetrator. The provision of restitution ensures that the burden of long-term trauma recovery is no longer borne by the victim's family, but rather becomes a form of real accountability from the perpetrator. The synergy between specific criminalization of KSBE, the imposition of sanctions for authority holders, and the certainty of restitution makes the TPKS Law the most progressive legal instrument in strengthening Indonesia's position when ratifying international conventions related to cybercrime in the future.[13]

1.4 Juridical Analysis of Law Enforcement of Crimes Related to Online Child Sexual Violence in the Case of AKBP Fajar Widyadharma Lukman Sumaatmaja

The rapid development of information technology has changed the pattern of global interaction, but on the other hand it has triggered the emergence of complex cybercrimes that go beyond the boundaries of traditional jurisdictions. The case of AKBP Fajar (2025) is crucial empirical evidence of the urgency of strengthening the national legal framework in dealing with *the transnational phenomenon of Child Sexual Abuse Material* (CSAM). Although the Indonesian judicial system through the Kupang District Court has shown firmness by imposing a sentence of 19 years in prison and a restitution obligation of Rp359,000,000.00 for the victim, the process of disclosing this case actually reveals the operational vulnerability of domestic law enforcement. The fact that this crime was detected for the first time by the *Australian Federal Police* (AFP) through cyber intelligence activities shows that without the initiative of foreign authorities, the national legal system tends to be passive and reactive in reaching out to digital evidence stored on overseas servers.[14]

Normatively, Indonesia actually has layered legal instruments through synergy between the Child Protection Law, the ITE Law, and the TPKS Law. Articles 76E and 76I of the Child Protection Law provide the basis for prohibiting seduction and sexual exploitation, while the ITE Law through Article 27 paragraph (1) focuses on criminalizing the distribution of content that violates morality. Furthermore, the TPKS Law is present as a progressive instrument that specifically criminalizes Electronic-Based Sexual Violence (KSBE) through Article 14, which abolishes the relevance of consent of child victims and establishes this offense as an ordinary offense. This regulatory synergy allows for comprehensive law enforcement, ranging from prison sentences, administrative fines for electronic system operators, to a restorative approach through the provision of restitution rights for victims to recover from long-term trauma.[15]

The revelation of criminal events through the cyber intelligence activities of *the Australian Federal Police* confirms that the main source of evidence is in foreign jurisdictions, while the Indonesian legal system does not yet have operational instruments that allow direct access, rapid preservation, and exchange of electronic evidence across countries in *real-time*. In this context, the application of Article 45 paragraph (1) jo.

13 Indonesia, *Law Number 12 of 2022 concerning the Crime of Sexual Violence.*

14 M. A. Yozami. (2026). "AKBP Fajar Sentenced to 19 Years in Prison in Case of Sexual Violence on Children". *Hukumonline*.

15 The Secret Life of the Beatles - The Beatles. (2026). "Chronology of the Arrest of the Ngada Police Chief AKBP Fajar Entangled in Alleged Pedophilia". *detikjateng*.

Article 27 paragraph (1) of the ITE Law does provide a basis for criminalization of the distribution or transmission of content that violates morality, but the formulation that is still general does not specifically accommodate the characteristics of CSAM as a crime based on the possession, production, and circulation of child sexual exploitation content connected to foreign servers. On the other hand, the TPKS Law through Article 6 letter c, Article 12, Article 14 paragraph (1), and Article 15 paragraph (1) has provided a basis for criminalization of acts of sexual violence, including those involving child exploitation, but the construction of the norm is still oriented towards criminal events and the relationship between the perpetrator and the victim directly, so it is not fully integrated with the needs of cross-jurisdictional digital proof mandated in the *United Nations Convention against Cybercrime*.[16]

2. The Urgency of Ratification of the *United Nations Convention against Cybercrime* for Indonesia in Strengthening the National Legal Framework to Eradicate the Crime of Online Child Sexual Violence

2.1 Normative Analysis of Articles 14 and 15 of *the United Nations Convention against Cybercrime*

Article 14 *of United Nations Convention againts Cybercrime*

Article 14 *of the United Nations Convention against Cybercrime* is a fundamental provision that affirms the international community's commitment to addressing child sexual abuse in the cyber realm. As a form of serious cybercrime that violates the human rights and dignity of children, this Article establishes a comprehensive definition of *Child Sexual Abuse Material* (CSAM). In its official formulation, CSAM includes visual, written, or audio material that *depicts, describes, or represents (depicts, describes, or represents*) individuals under the age of 18 who engage in real or simulated sexual activity, including visualization of sexual parts for sexual purposes, as well as acts of sexual torture. This broad and detailed definition reflects the application of *the principle of anticipatory law*, where legal norms are constructed to reach the evolution of complex digital modus operandi, including material generated through technological engineering such as *Computer-Generated Imagery* (CGI) or *deepfakes*.

The normative significance of Article 14 lies in the expansion of legal protections that go beyond the real physical subject of the child through the aspect of "representation". By setting an absolute age threshold of under 18 years old, this provision is synchronized with the principle *of the best interests of the child* in the UNCRC, while shifting the paradigm of child placement from just a criminal object to the main subject of law. This provides a critical foundation for Indonesian national law, which is often still stuck with the burden of conventional physical proof. Through ratification, the Article 14 standard can transform the paradigm of child protection to be more progressive and human rights-based, ensuring that children's dignity remains protected in the midst of cyberspace anonymity without loopholes for perpetrators who utilize artificial intelligence technology. [17]

Article 15 *of the United Nations Convention againts Cybercrime*

16 S. P. Hukmana. (2026). "The Chronology of Asusila AKBP Fajar, Information from Hubinter to Check Hotel Data on June 11, 2024". *Indonesian media*.

17 *United Nations Convention Against Cybercrime*, Pasal 14.

In addition to regulating exploitative material, Article 15 of this Convention presents a juridical response to acts of persuasion or *child grooming* through information technology systems. Normatively, this Article expands the spectrum of legal protection by reaching the pre-delicacy stage, where *grooming* is no longer seen as merely a preparatory act, but as a sui *generis* criminal act. The focus of criminalization in this Article lies in the *evil intent* of the perpetrator which manifests through active communication to manipulate the victim. This approach marks an international paradigm shift from reactive to preventive-proactive, allowing law enforcement to intervene early before physical contact occurs, while addressing the challenges of *transborder crimes* that utilize online communication features.

Further analysis of Article 15 shows the recognition of *grooming* as an *international minimum standard* that must be criminalized by the state party. The Convention provides flexibility for the domestic legal system to require an *act in furtherance*, while still emphasizing a clear and directed *aspect of mens rea*. In addition, the expansion of coverage for individuals who are "*believed to be a child*" in paragraph 3 aims to close the legal loophole for perpetrators who argue that they do not know the real age of the victim. On the other hand, paragraph 4 provides the discretion to exclude criminalization if the act is committed by a fellow child, reflecting the restorative justice and rehabilitation approach.

Systematically, there is a close intertextual relationship between Article 14 and Article 15, where the *act of grooming* is seen as an initial phase that has the potential to continue in the production or distribution of CSAM. This linkage builds a holistic and tiered cyber-based child protection regime, removing fragmentation between prevention and enforcement efforts. For Indonesia, the integration of these two articles through ratification will strengthen the country's legal sovereignty in protecting the dignity of children in a sustainable manner, ensuring that law enforcement is able to reach digital threats ranging from the stage of communication manipulation to the stage of material exploitation in the digital space that goes beyond the boundaries of traditional jurisdiction.[18]

2.2 The Position of *the United Nations Convention against Cybercrime* in the International Legal System

The evolution of international cyber law has entered a new chapter with the birth *of the United Nations Convention against Cybercrime* which was passed through Resolution 79/24 in December 2024. Although *the 2001 Budapest Convention on Cybercrime* has been pioneered and ratified by 81 countries by 2025, the instrument is often considered "Western-centric" and less inclusive for developing countries. On the contrary, this UN Convention offers stronger global legitimacy because it involves the active role of countries such as Indonesia in its formulation, thus being able to maintain a fairer balance between the interests of national sovereignty and the needs of international law enforcement in the digital space.[19]

As the first comprehensive international agreement that regulates cybercrime strategies globally, the convention consists of 9 chapters and 71 articles covering

18 *United Nations Convention Against Cybercrime*, Pasal 15.

19 Dewi Bunga. (2019). "Legal Response to Cybercrime in Global and National Dimensions". *Padjadjaran Journal of Legal Studies*, 6(1): 77–81.

crucial aspects such as the standardization of digital crime typologies and cross-border electronic evidence collection mechanisms. The legitimacy of this instrument is further emphasized by the fact that as of January 2026, as many as 74 countries, including major powers such as the United States, China, and France, have signed it as a form of commitment to national ratification. Based on the principle of *pacta sunt servanda* in Article 26 of the 1969 Vienna Convention, the adoption of this convention creates an obligation for member states to implement the substance of the agreement in good faith in order to create a secure and universally standardized cyberspace.[20]

In this new cyber law regime, child protection is placed as a fundamental transnational issue that is strengthened through two main pillars, namely Article 14 and Article 15. Article 14 specifically criminalizes the production and possession of child sexual exploitation material (CSAM), including technologically engineered content such as *deepfakes* or CGI, in order to protect the dignity of children under the age of 18. Meanwhile, Article 15 regulates the criminalization of *child grooming* or online manipulation as a preparatory offense, which allows law enforcement to take a preventive-proactive approach before physical violence occurs. For Indonesia, the ratification of this convention is a crucial step to harmonize national legal standards and remove regulatory loopholes (*safe haven*), while demonstrating a real commitment to an international legal architecture that prioritizes *the best interests of the child*.

2.3 The Urgency of Ratification of the *United Nations Convention against Cybercrime* in the Eradication of Crimes Related to Online Child Sexual Violence in Indonesia

The National Legal Gap with *the United Nations Convention against Cybercrime* and the Legal Contribution of the Convention

The fundamental gap in Indonesian national law is first seen in the definition aspect, where there is a conceptual ambiguity between general pornographic content and child sexual exploitation. The use of the term ”violating morality” in Article 27 paragraph (1) of the ITE Law is considered too broad and subjective, thus creating obstacles for law enforcement to criminalize *Child Sexual Abuse Material* (CSAM) specifically, while Article 76I of the Child Protection Law has not yet reached complex digital technical aspects. In this regard, Article 16 of the Convention contributes through the introduction of a more precise ”*intimate image*” standard. The most crucial point lies in Article 16 paragraph (4) which emphasizes that children under 18 years old cannot legally consent to the dissemination of intimate images, thus breaking the ”consensual” argument that perpetrators often use to avoid the snares of domestic law.

Operationally, although Article 14 of the TPKS Law has progressively regulated Electronic-Based Sexual Violence (KSBE), its territorial reach is still limited to Indonesia’s sovereign territory, so that the handling of cross-border cases such as AI abuse (*deepfakes*) often only stops at administrative steps in the form of blocking access. The Convention is here to fill this gap through Article 35 which provides a special (*fast-track*) channel for the collection and distribution of electronic evidence in *real-time*. In addition, Article 35 paragraph (3) provides flexibility to the principle *of dual criminality*, where international cooperation is still considered valid as long

20 Euronews. (2024). “UN committee approves first cybercrime treaty despite opposition”. *Euronews*.

as the substance of the act is a criminal offense in both countries, without being hampered by the differences in legal terminology used by each state party.

Another very real gap has to do with the execution and jurisdictional aspects, where Article 2 of the ITE Law is often a ”paper tiger” because it lacks the instrument to force other countries to hand over perpetrators in the absence of a bilateral agreement. On the other hand, Article 7 of Law No. 1 of 1979 which prohibits the extradition of citizens themselves risks creating impunity for transnational perpetrators. Article 37 of the Convention closes this loophole by establishing cybercrime as automatically *extraditable offences* and can be the main legal basis for extradition even without a bilateral agreement. Moreover, through the principle *of aut dedere aut judicare* in Article 37 paragraph (11), Indonesia is obliged to prosecute Indonesian citizens who are not extradited with the support of international evidence, so that there is no room for perpetrators to hide behind their citizenship.

Finally, the ratification of this Convention provides international legitimacy for the expansion of Indonesian jurisdiction which has been difficult to implement through Article 2 of the ITE Law. Through Article 22 paragraph (2) letter a, Indonesia obtains authority based on the principle of passive personality to prosecute cybercrime perpetrators wherever they are, as long as the victim is an Indonesian citizen. This is strengthened by the coordination mechanism in Article 22 paragraph (5) which requires consultation between countries to avoid overlapping investigations. Thus, the integration of the Convention’s standards into national law not only strengthens the substantive aspects at home, but also provides a procedural instrument capable of penetrating the boundaries of international jurisdiction in dealing with global pedophilia syndicates.

Child protection in the digital space is a manifestation of the mandate of Article 28B paragraph (2) of the 1945 Constitution as well as Indonesia’s international obligations under *the Convention on the Rights of the Child* (CRC). The ratification of the *United Nations Convention against Cybercrime* is an urgent constitutional need to harmonize international human rights standards into responsive domestic policies. Technically, Article 14 of the Convention implements the *function of anticipatory law* through a broad definition of CSAM, covering technological engineering such as *deepfakes*, while Article 15 strengthens the preventive dimension by criminalizing *grooming* as a *preparatory offence*. The absence of ratification risks making Indonesia a *safe haven* for cyber predators due to weak access to extradition mechanisms and cross-border digital evidence exchange, which ultimately weakens Indonesia’s bargaining position in transnational law enforcement.

In the perspective of legal harmonization theory, the ratification of this convention serves as a normative instrument for harmonizing national laws vertically and horizontally. This is crucial to fill the void of norms and insynchronization of terminology, such as the use of the phrase ”morality” in Article 27 paragraph (1) of the ITE Law which is multi-interpreted. Harmonization with Articles 14 and 15 of the Convention will provide legal certainty through *common legal language* that facilitates coordination between law enforcement officials. In line with that, Harold Hongju Koh’s theory of transnational legal processes views ratification as the starting point for the organic internalization of norms through the stages of interaction and interpretation. This process will change the paradigm of Indonesian law enforcement officials from a

territorial approach to a transnational approach, so that enforcement hukum tidak lagi terhambat oleh batas yurisdiksi konvensional.

Voluntarily, this ratification is not a form of subordination, but a manifestation of Indonesia's digital sovereignty that is active in responding to the threat of cross-border cybercrime. Without this international commitment, state sovereignty is factually reduced due to the absence of effective instruments to reach actors outside the national territory. Through ratification, Indonesia's sovereignty is transformed into a cooperative sovereignty that provides access to a global *fast-track* mechanism . This includes the availability of a 24/7 emergency contact network (Article 41) as well as *an expedited preservation of stored computer data* (Articles 25 and 42) that ensures digital evidence is not lost before processing, an operational capability that national law cannot provide on its own.

This operational urgency is strengthened by Article 35 which functions as a juridical bridge for the freezing and seizure of transnational electronic evidence with the flexibility *of the dual criminality* principle. In addition, Article 37 closes the gap in impunity by designating all cybercrimes as *extraditable offences*, even allowing this convention to become the main legal basis for extradition for countries that do not have bilateral agreements with Indonesia. By applying *the principle of aut dedere aut judicare* (extradition or trial) through Article 22, Indonesia gains legitimacy to prosecute cybercriminals wherever the victim is an Indonesian citizen. Thus, ratification is an absolute prerequisite for the creation of a modern criminal justice system that has legitimacy, evidentiary effectiveness, and global reach to eradicate child sexual violence completely.

The Urgency of the Ratification of the United Nations Convention against Cybercrime: Constitutional Perspectives and Legal Theory

Child protection in the digital space is a manifestation of the mandate of Article 28B paragraph (2) of the 1945 Constitution as well as Indonesia's international obligations under *the Convention on the Rights of the Child* (CRC). The ratification of the *United Nations Convention against Cybercrime* is an urgent constitutional need to harmonize international human rights standards into responsive domestic policies. Technically, Article 14 of the Convention implements the *function of anticipatory law* through a broad definition of CSAM, covering technological engineering such as *deepfakes*, while Article 15 strengthens the preventive dimension by criminalizing *grooming* as a *preparatory offence*. The absence of ratification risks making Indonesia a *safe haven* for cyber predators due to weak access to extradition mechanisms and cross-border digital evidence exchange, which ultimately weakens Indonesia's bargaining position in transnational law enforcement.

The state as an independent subject has the sovereignty to conduct government affairs,[21] but in the context of *the United Nations Convention against Cybercrime*, this sovereignty is transformed into cooperative sovereignty through the mandate of cross-border mutual legal assistance. The ratification of this convention makes a significant contribution to Indonesia's legal framework by presenting a more precise standard definition of cybercrime through Article 16, and effectively closing the impunity

21 Muh. Risnain. (2020). *International Law & Indonesian National Interest*. Jakarta: Sanabil, pp. 27–28.

gap through the principle *of aut dedere aut judicare* in Article 22 which requires the prosecution of citizens for crimes abroad if extradition is refused.

In the perspective of legal harmonization theory, the ratification of this convention serves as a normative instrument for harmonizing national laws vertically and horizontally. This is crucial to fill the void of norms and insynchronization of terminology, such as the use of the phrase "morality" in Article 27 paragraph (1) of the ITE Law which is multi-interpreted. Harmonization with Articles 14 and 15 of the Convention will provide legal certainty through *common legal language* that facilitates coordination between law enforcement officials. In line with that, Harold Hongju Koh's theory of transnational legal processes views ratification as the starting point for the organic internalization of norms through the stages of interaction and interpretation. This process will change the paradigm of Indonesian law enforcement officials from a territorial approach to a transnational approach, so that law enforcement is no longer hampered by conventional jurisdictional boundaries.

Voluntarily, this ratification is not a form of subordination, but a manifestation of Indonesia's digital sovereignty that is active in responding to the threat of cross-border cybercrime. Without this international commitment, state sovereignty is factually reduced due to the absence of effective instruments to reach actors outside the national territory. Through ratification, Indonesia's sovereignty is transformed into a cooperative sovereignty that provides access to a global *fast-track* mechanism . This includes the availability of a 24/7 emergency contact network (Article 41) as well as *an expedited preservation of stored computer data* (Articles 25 and 42) that ensures digital evidence is not lost before processing, an operational capability that national law cannot provide on its own.

This operational urgency is strengthened by Article 35 which functions as a juridical bridge for the freezing and seizure of transnational electronic evidence with the flexibility *of the dual criminality* principle. In addition, Article 37 closes the gap in impunity by designating all cybercrimes as *extraditable offences*, even allowing this convention to become the main legal basis for extradition for countries that do not have bilateral agreements with Indonesia. By applying *the principle of aut dedere aut judicare* (extradition or trial) through Article 22, Indonesia gains legitimacy to prosecute cybercriminals wherever the victim is an Indonesian citizen. Thus, ratification is an absolute prerequisite for the creation of a modern criminal justice system that has legitimacy, evidentiary effectiveness, and global reach to eradicate child sexual violence completely.

D. CONCLUSION

The regulation of child protection and criminal responsibility for perpetrators in the online sexual violence ecosystem in Indonesia is currently still sectoral and limited to the instruments of the ITE Law, the Child Protection Law, and the TPKS Law. Substantially, the domestic legal framework is still dominated by general terminology such as "violating morality" which creates ambiguity in ensnaring *the Child Sexual Abuse Material* (CSAM) ecosystem specifically. Although normatively it has accommodated the

Electronic-Based Sexual Violence (KSBE) offense, Indonesia still faces a legal vacuum in criminalizing preparatory actions such as *grooming* and technological engineering content (*deepfakes*). In addition, there are significant operational limitations due to the reliance on bureaucratic *Mutual Legal Assistance* (MLA) procedures, thus placing children's constitutional rights at risk of juridical vulnerability due to the protection paradigm that is still reactive-territorial.

Facing these challenges, the ratification of the *United Nations Convention against Cybercrime* is an urgent need as an instrument of legal transformation that is able to close the gap between national policies and the reality of cross-border cybercrime. This urgency rests on strengthening three main aspects, namely standardization of norms, operational efficiency, and fulfillment of constitutional mandates. Normatively, this Convention acts as a trigger mechanism to harmonize the definition of criminal acts more precisely, such as the criminalization of *child grooming* (Article 15) and sexually violent material resulting from technological engineering (Article 14). Operationally, ratification provides an "executive hand" for law enforcement through a *fast-track* of international cooperation, flexible extradition (Article 37), and quick access to volatile electronic evidence to break bureaucratic barriers.

In the end, the ratification of the *United Nations Convention against Cybercrime* is a tangible manifestation of the country's constitutional obligation to protect the human rights and digital dignity of Indonesian children in accordance with the mandate of the 1945 Constitution, *the Convention on the Rights of the Child* (CRC), and the ICCPR. This step ensures that Indonesia's digital sovereignty is not only upheld domestically, but also has operational reach in the global cyberspace to eliminate impunity for perpetrators of child sexual crimes. The synergy between strengthening domestic regulations and commitment to multilateral instruments is an absolute prerequisite for the creation of a safe, fair, and child-oriented digital ecosystem.

BIBLIOGRAPHY

Books

Jan Klabbers. (2023). *The Concept of Treaty in International Law*. Jilid 22. Leiden: Brill, hlm. [masukkan nomor halaman].

Risnain, Muh. (2020). *Hukum Internasional & Kepentingan Nasional Indonesia*. Jakarta: Sanabil.

Journals

Bastian, M. A. M., R. Sutanto, dan Raden. (2024). "Evaluasi Efektivitas Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik dalam Pencegahan Cyberterrorism". *Jurnal Hukum Mimbar Justitia (JHMJ)*, 10(2).

Bunga, Dewi. (2019). "Legal Response to Cybercrime in Global and National Dimensions". *Padjadjaran Journal of Legal Studies*, 6(1).

Hartono, P., et al. (2024). "Challenges of Criminal Investigation Cyber Crime". *Awang Long Law Review*, 7(1).

Martono, M., M. G. G. Akbar, dan H. Rahmatiar. (2025). "Law Enforcement of

Transnational Cybercrime: Case Study in Indonesia". 10.

Parti, K. dan J. Szabó. (2024). "The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe". *Laws*, 13(6).

Pratama, A., O. S. Mandala, dan A. Rahmatyar. (2025). "Analisis Implementasi Kebijakan Perlindungan Anak Korban Kekerasan Seksual di Indonesia dalam Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual". *Jurnal Hukum*.

Ramadhani, S., et al. (2025). "Perlindungan Hukum terhadap Hak Privasi Anak yang Dipublikasikan di Media Massa Menurut Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak". *Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh*, 8(2).

Regulations

Council of Europe, *The Budapest Convention on Cybercrime (ETS No. 185) and its Protocols*, 2001.

Indonesia. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, Pasal 27 ayat (1) dan (2).

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

Indonesia. *Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual*.

The United Nations, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, G.A. Res. 79/243, Annex, December 24, 2024.

Internet

Childlight. (2024). "Over 300 Million Children a Year are Victims of Technology-Facilitated Sexual Exploitation and Abuse". *Global Child Safety Institute*, https://childlight.org/newsroom/over-300-million-children-a-year-are-victims-of-online-sexual-exploitation-and-abuse.National Centre for Missing & Exploited Children. (2023). *CyberTipline 2023 Report*. https://missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf, hlm. 1.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2025). "Catat 1,45 Juta Kasus Eksploitasi Seksual Anak Daring, Nezar Patria: Literasi Digital dan Regulasi AI Jadi Kunci Perlindungan". *Siaran Pers No. 188/HM-KKD/10/2025*.

M. A. Yozami. (2026). "AKBP Fajar Divonis 19 Tahun Penjara dalam Kasus Kekerasan Seksual pada Anak". *Hukumonline*.

Tim detikBali - detikJateng. (2026). "Kronologi Penangkapan Kapolres Ngada AKBP Fajar Terjerat Dugaan Pedofilia". *detikjateng*.

S. P. Hukmana. (2026). “Kronologi Asusila AKBP Fajar, Informasi dari Hubinter hingga Cek Data Hotel 11 Juni 2024”. *Media Indonesia*.

Euronews. (2024). “UN committee approves first cybercrime treaty despite opposition”. *Euronews*.