Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

Propagation of AI-generated child sexual abuse material as a cybercrime commodity in Indonesia

OÑATI SOCIO-LEGAL SERIES VOLUME 16, ISSUE 3 (2026), 1189-1206: FRONTERAS DE EXCEPCIÓN: ENTRE EL CONTROL MIGRATORIO Y LA RESISTENCIA MIGRANTE
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.2579
RECEIVED 15 JANUARY 2026, ACCEPTED 5 MARCH 2026, FIRST-ONLINE PUBLISHED 31 MARCH 2026, VERSION OF RECORD PUBLISHED 1 JUNE 2026

AHMAD JAMALUDIN[1]
HAPPY YULIA ANGGRAENI[2]
SAYID MUHAMMAD RIFKI NOVAL[3]
RATU ARTI WULAN SARI[4]
SAJI SONJAYA[5]
AHMAD MA'MUN FIKRI[6]

Abstract

Artificial Intelligence (AI) and Cryptocurrency are increasingly exploited to facilitate cyber child sexual abuse material (CSAM), creating an illicit ecosystem of "pseudo-pornography". Defined as entirely synthetic, AI-manipulated visual

This research was funded by The Ministry of Education, Culture, Research, and Technology of Indonesia. Publicly available datasets regarding legal regulations and court decisions were analyzed in this study. The quantitative data regarding public perception presented in this study are available on request from the corresponding author due to privacy restrictions involving human participants.
The authors express their gratitude to Universitas Islam Nusantara for providing institutional support throughout this research. We also extend our sincere thanks to the Ministry of Education, Culture, Research and Technology of Indonesia for their guidance and encouragement. Special appreciation was given to the faculty members of the Faculty of Law and Communication at Universitas Islam Nusantara for their valuable administrative and technical support, which greatly contributed to the completion of this study.
[1] Ahmad Jamaludin. Corresponding author. Faculty of Law, Universitas Islam Nusantara, Soekarno Hatta No. 530, Bandung, West Java, Indonesia; jamaludinumam@gmail.com
[2] Happy Yulia Anggraeni. Faculty of Law, Universitas Islam Nusantara Jalan Soekarno Hatta No. 530, Bandung, West Java, Indonesia; happianggraeni27@gmail.com
[3] Sayid Muhammad Rifki Noval. Master of Notary Program, Pasundan University, Sumatera No. 41, Babakan Ciamis, Sumur Bandung District, Bandung City, West Java 40117, Indonesia; sayidrifqi@unpas.ac.id
[4] Ratu Arti Wulan Sari. Faculty of Da'wah and Communication, Sunan Gunung Djati State Islamic University Bandung, A.H. Nasution No. 105, Cipadung, Cibiru, Bandung City, West Java 40614, Indonesia; ratuarti-wulan@uinsgd.ac.id
[5] Saji Sonjaya. Faculty of Law, Universitas Islam Nusantara; Soekarno Hatta No. 530, Bandung, West Java, Indonesia; sajisonjaya@uninus.ac.id
[6] Ahmad Ma'mun Fikri. Postgraduate School of Law, Universitas Islam Nusantara; Soekarno Hatta No. 530, Bandung, West Java, Indonesia; amfirkri69@gmail.com

representations, pseudo-pornography exploits a person's digital identity to depict sexual acts without physical involvement. These manipulated identities are then traded anonymously. Utilizing a juridical-normative approach, this study analyzes the governing legal frameworks. Findings reveal a critical legal vacuum in Indonesia; current laws (Pornography, ITE, TPKS, and Criminal Code) remain oriented toward physical distribution. They lack specific provisions to address non-physical, AI-generated offenses and cryptocurrency-facilitated anonymity, while crypto regulatory dualism further hinders enforcement. To combat this, the government must urgently revise the Pornography and ITE Laws to explicitly prosecute pseudo-pornography creators, mandate platform accountability, and enact specific AI legislation. These measures are vital to closing legal loopholes and protecting Indonesia's digital space.

Key words

Artificial intelligence; cyber-CSAM; legal accountability; cryptocurrency; pseudo-pornography; digital rights

Resumen

La inteligencia artificial (IA) y las criptomonedas se utilizan cada vez más para facilitar la difusión de material de abuso sexual infantil (CSAM, por sus siglas en inglés) en Internet, creando un ecosistema ilícito de "pseudopornografía". Definida como un conjunto de representaciones visuales totalmente sintéticas y manipuladas por IA, la pseudopornografía explota la identidad digital de una persona para representar actos sexuales sin participación física. Estas identidades manipuladas se comercializan posteriormente de forma anónima. Utilizando un enfoque jurídico-normativo, este estudio analiza los marcos legales vigentes. Los resultados revelan un vacío legal crítico en Indonesia; las leyes actuales (Pornografía, ITE, TPKS y Código Penal) siguen orientadas hacia la distribución física; carecen de disposiciones concretas para abordar los delitos no físicos generados por IA y el anonimato facilitado por las criptomonedas, mientras que el dualismo regulatorio de las criptomonedas dificulta aún más la aplicación de la ley. Para combatir esto, el gobierno debe revisar urgentemente las Leyes de Pornografía y de las Tecnologías de la Información y la Comunicación (ITE) para perseguir explícitamente a los creadores de pseudopornografía, exigir la responsabilidad de las plataformas y promulgar legislación específica sobre IA. Esas medidas son vitales para cerrar las lagunas legales y proteger el espacio digital de Indonesia.

Palabras clave

Inteligencia artificial; material de abuso sexual infantil en Internet; responsabilidad jurídica; criptomoneda; pseudopornografía; derechos digitales

Table of contents

1. Introduction

Technological developments are advancing rapidly and making it easier for humans to access information. One of the latest technologies is Artificial Intelligence (AI), a machine that mimics human intelligence to solve human problems in all sectors, such as creating and recognizing images, making data-based predictions, making decisions, identifying patterns, and even solving complex problems quickly, effectively, and efficiently. The rapid trajectory of AI development suggests a shift from assistive roles to autonomous functional integration (Lin 2025). AI technology does not always have a positive impact it can be misused for illegal activities that can threaten and cause harm to humans. One example is the misuse of AI technology in cybercrime involving child sexual abuse material (CSAM). Digital pornography or cyberpornography has grown significantly, becoming more widespread in line with the development of AI technology (Kupriianova and Kupriianova 2023).

AI technology is no longer used to make human life easier, but has become a commodity for cyber child sexual abuse material (CSAM). This has led to the emergence of "pseudo-pornography," a phenomenon where data, such as facial images, is exploited to create highly realistic false representations (imago) of sexual exploitation without exploiting a physical body (corpus). Transactions for this ecosystem use cryptocurrency models that are difficult to detect (Milmo 2025). The large number of unverified AI providers is problematic, making the misuse of AI for criminal acts such as pornography increasingly apparent. The trend of cyber child sexual abuse material (CSAM) crimes such as deepfakes has surged by 550% with 95,820 videos detected in 2023. Deepfakes refer specifically to highly realistic, manipulated images or videos where the face of a real person is digitally superimposed or displayed onto another body without their consent.

AI enables the creation of digital pornographic content (deepfakes) in the form of text, images, videos, or audio through prompt commands, with serious impacts on victims, especially women and teenagers. From October 2021 to March 2023, the FBI and Homeland Security Investigations received over 13,000 reports of online financial sextortion of minors. The sextortion involved at least 12,600 victims primarily boys and led to at least 20 suicides (Federal Bureau of Investigation 2024). The viral case of Taylor Swift's deepfake video in January 2024, with 47 million views on the X platform, underscores the urgency of addressing this issue (Rahman-Jones 2024). Although the US has proposed the DEFIANCE Act (punishable by up to 2 years in prison), regulatory efforts are still lagging behind the production of illegal content.

In various countries, cases of AI-based cyber-CSAM show an alarming trend, with the majority of victims being women and children (Chainalysis 2025). The European Union has enacted the EU AI Act 2024, which prohibits non-consensual AI-based pornographic content, accompanied by fines of up to €35 million, while South Korea has passed the Sexual Violence Prevention and Victims Protection Act with a maximum penalty of 5 years in prison and 50 million won after sexually exploitative content surged to 800 deepfake cases in 2024 (Compliance Hub 2024). In Indonesia, the Ministry of Communication and Information Technology has noted an increase in the exploitation of AI to produce pornographic content by pasting the faces of victims (such as the case of TikToker @safirahunar, which reached 1.5 million views) using deep learning

applications such as DeepFaceLab, taken from the victim's social media data (Civa Melati Aulia 2023).

In this study, researchers conducted a survey using purposive sampling of 400 respondents residing in West Java to measure vulnerability to the use of Artificial Intelligence. The results of the survey found a high level of urgency, with the vast majority of the Indonesian public having been exposed to CSAM content manipulated by artificial intelligence (82.5%), feeling highly vulnerable to becoming victims (74.5%), and believing in the obligation to verify the identity of artificial intelligence users (88.5%). According to the U.S. Department of Justice, bitcoin has been used to monetize the production of child exploitation material, a development that marks a major shift as such practices were rare before the emergence of cryptocurrency. Specifically, transactions for cyber-CSAM crimes have shifted significantly from initially using conventional currencies to cryptocurrencies. This data reflects how dangerous the misuse of AI is for creating CSAM content, especially since cyber-CSAM crime syndicates cover up these crimes by using cryptocurrency transaction tools to avoid detection, allowing the trade of cyber-CSAM content to spread easily to the wider community.

Economic motives are one of the main drivers behind the rise in cybercrime involving CSAM based on artificial intelligence (AI). In the UK, a pedophile gang reportedly earned £5,000 over 18 months from selling sexually abusive images created with AI (Reuters 2025). This illegal business is lucrative due to the high demand for explicit content and varying production costs. For example, a report from Kaspersky revealed that deepfake creation services on the darknet offer video production at costs ranging from USD 300 to USD 20,000 per minute, depending on the complexity and quality of the final product. In 2024, there was a significant shift in the pattern of illegal transactions using crypto assets. Stablecoins such as Tether (USDT) dominated, accounting for 63% of total global illegal transactions, displacing Bitcoin's dominance, which now stands at only 20% (Fauziyah 2025). Meanwhile, Monero (XMR), as one of the privacy coins, contributed 10%, reflecting the tendency of criminals to switch to assets that offer high anonymity and strong liquidity. Anonymity in crypto transactions, as offered by Monero, as well as the use of stablecoins, has become a major concern in law enforcement. Monero is known for its advanced privacy features, enabling transactions that are nearly untraceable, making it attractive to individuals seeking high anonymity.

Until now, cybercrime involving CSAM has been regulated by the Criminal Code, the Pornography Law, the Electronic Information and Transactions Law, and the Child Protection Law. However, these laws and regulations have not been able to address the issue of AI-based cybercrime involving CSAM due to a legal vacuum (Yudhistira and Puspitosari 2025). Therefore, it is necessary to accelerate legal efforts by establishing regulations that include appropriate sanctions for users of AI technology in cyberpornography in the form of internet access restrictions, asset restrictions through transaction reporting to prevent the misuse of crypto assets in cyberpornography crimes, and supervision in the form of AI function verification and sanctions against companies providing AI access in cyberpornography crimes through the revocation of licenses and access in Indonesia.

The purpose of this study is to analyze and discover concepts of prevention and law enforcement against cyber-CSAM through AI using cryptocurrency as a transaction tool. This study uses a legal-normative approach to design an AI-based cyber-CSAM prevention model that is traded with cryptocurrency. The normative aspect includes an analysis of national regulations and global policies through a case approach, statute approach, comparative approach, and analytical approach, specifically examining legal loopholes related to AI-generated child cyber pornography and the anonymity of cryptocurrency transactions (Utami *et al.* 2022). Primary data analysis was conducted using questionnaire surveys to determine the urgency of AI use leading to cyberpornography crimes in Indonesian society, and case analysis to map the technical challenges of deepfake detection and crypto tracking. The integration of these two approaches resulted in recommendations for adaptive regulation (revision of the Electronic Information and Transactions Law to criminalize child cyber pornography through AI, verification of AI service providers) and forensic technology collaboration (blockchain analytics with Bappebti) to break the chain of illegal content distribution and protect victims based on victim-centered justice.

2. Methods

This study uses a legal-normative approach as the main method for designing an AI-based prevention model for cyber-CSAM traded with cryptocurrency, with a focus on analyzing national regulations and global policies. This normative aspect is implemented through a statute approach, a comparative approach to examine regulations in other jurisdictions, a case approach, and an analytical approach to identify legal gaps related to AI-generated cyber-CSAM and the anonymity of cryptocurrency transactions (Esoimeme 2024). To supplement the normative legal data, this study integrates empirical data obtained through a quantitative questionnaire survey. The survey employed a purposive sampling technique involving 400 respondents residing in West Java. The criteria for respondent selection included active internet and social media users aged 18 and above, ensuring they have a baseline awareness of digital trends, artificial intelligence, or cryptocurrency.

The survey design utilized a structured questionnaire with a 5-point Likert scale to measure three main variables: the public's exposure to AI-generated CSAM, their perceived vulnerability to digital identity exploitation, and their perception of how cryptocurrency anonymity hinders law enforcement. The analytical impact of this empirical data is to provide a sociological and factual foundation for the legal arguments. By demonstrating a high level of societal urgency and vulnerability, the survey results directly justify the normative conclusions, specifically the pressing need to revise the Electronic Information and Transactions Law (ITE) and mandate platform accountability.

3. Findings. Public vulnerability and the urgency of legal reform: Survey results

To measure the real-world impact and public perception regarding the exploitation of AI and cryptocurrency anonymity, a quantitative survey was conducted among 400 respondents residing in West Java. The empirical findings directly validate the

normative gaps identified in the current legal framework and emphasize the real-world consequences of pseudo-pornography.

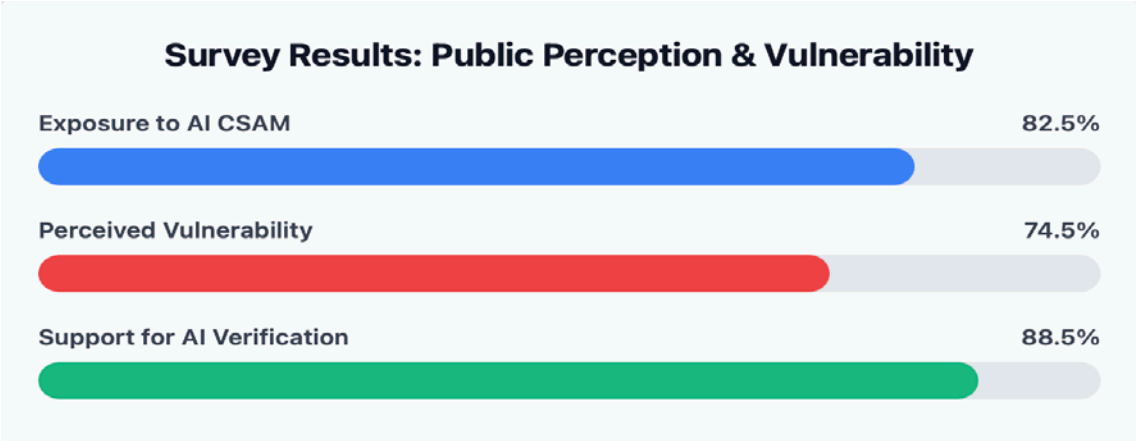
Figure 1: Public perception regarding exposure to AI-manipulated CSAM, vulnerability to digital identity theft, and the need for regulatory intervention.

The survey revealed a critical level of urgency among the public. A vast majority of respondents (82.5%) reported having been exposed to or made aware of CSAM manipulated by artificial intelligence across various social media platforms. Furthermore, the psychological impact of this phenomenon is evident, with 74.5% of respondents expressing that they feel highly vulnerable to becoming victims of digital identity theft for the purpose of pseudo-pornography.

Regarding the financial mechanism facilitating these cybercrimes, the public is highly aware of the systemic obstacles faced by authorities. When asked to what extent they believe the anonymity offered by cryptocurrencies (such as Monero) makes law enforcement against cyber-CSAM difficult, respondents gave an average score of 4.09 out of 5, indicating strong agreement. Moreover, there is overwhelming public support for stricter preventive regulations. Approximately 88.5% of respondents believe it should be a mandatory obligation to verify the identity of artificial intelligence users and hold AI service providers accountable for the content generated on their platforms.

These empirical findings demonstrate a significant disconnect between rapidly evolving technological threats and existing legal protections. The high vulnerability felt by the public emphasizes that the current legal focus on physical human models and distribution as seen in the Pornography Law and the ITE Law is fundamentally inadequate to protect digital identities. Consequently, this survey data provides a robust sociological justification for the proposed legislative recommendations, demanding immediate regulatory measures targeting AI providers, mandatory verification protocols, and enhanced crypto-asset tracing to dismantle this illicit ecosystem.

GRAPH 1



Graph 1. The mechanisms of child exploitation: generating synthetic CSAM through AI technology.

AI technology effectively blurs the line between reality and fiction, creating "victims" without the physical "acts" commonly understood in criminal law (KAN 2024). Victims never participate in the sexual scenes depicted; it is their identities and digital images that are hijacked and exploited. The urgency of this issue has been felt in Indonesia, as

reflected in cases that have come to light, such as the misuse of photos of female students at SMAN 11 Semarang and the practice of buying and selling AI-based pornographic videos in Gresik, which show that this threat is no longer just a hypothesis, but a reality that requires an immediate legal response (Ramadhani *et al.* 2025). The conceptual challenges that this phenomenon presents for the legal system are fundamental. Traditional criminal law, particularly the Pornography Law, was designed to combat the physical exploitation of humans in content production. However, pseudo-pornography does not exploit the body (corpus), but rather utilizes biometric data (facial imagery) to synthesize sexual exploitation (imago) in the absence of a physical subject (corpus) to crimes against digital identity and reputation. As a result, the legal framework that focuses on human "objects or models" who are physically exploited in the production process becomes irrelevant, opening a significant conceptual gap in Indonesian positive law.

The phenomenon of sharenting, the practice of parents routinely sharing photos, videos, and personal information about their children on social media platforms, has become a cultural norm in the digital age. Driven by pride and a desire to share precious moments with family and friends, this practice has inadvertently created a massive, detailed repository of visual data about children that is often accessible to the public. Every graduation photo upload, vacation video, or even simple status update contributes to the construction of a comprehensive digital footprint for children, long before they are old enough to give consent or understand the implications. This seemingly harmless practice has become a crucial bridge to new forms of exploitation (Agarwala 2025). This abundance of visual data has become the main "raw material" for criminals. Investigative reports from dark web forums show that perpetrators actively collect (scrape) images of children from social media to use as training data for AI models. Using techniques such as Low-Rank Adaptation (LoRA), they can "train" generative AI models to specifically mimic a child's face and features, which then allows them to generate new, highly realistic deepfake images of the same child in exploitative and sexual contexts. Thus, sharenting effectively turns children's privacy into a highly vulnerable public commodity. This is no longer merely an ethical issue of consent, but has evolved into a systemic cybersecurity problem (Barnes 2025). Sharing actions based on good intentions and affection directly feed the ecosystem of digital exploitation. In this process, children are transformed from subjects of family memories into objects of data ready for exploitation, and family digital photo albums inadvertently serve as data warehouses for criminals.

The production of CSAM using AI is made possible by rapid advances in deep learning technology, particularly generative models. Two main architectures that are often used are Generative Adversarial Networks (GANs) and diffusion models. GANs work with two competing neural networks one "generator" that tries to create fake images, and one "discriminator" that tries to distinguish between real and fake images (Matters 2024). Through this competitive process, generators become increasingly adept at creating highly realistic images. Meanwhile, diffusion models, which are newer and often more powerful, work by gradually adding "noise" or random disturbances to the original image, then training the model to reverse the process. By learning how to remove noise to reconstruct the original image, these models can start from pure random noise and

generate new, highly detailed and coherent images based on text prompts (text-to-image).

Forensic analysis of dark web environments reveals an expanding ecosystem of synthetic CSAM production. One of the most alarming findings is that the technical barrier to entry has diminished, allowing non-specialist actors to utilize generative AI tools. Instead, they are ordinary individuals who teach and collaborate with each other in closed communities. Tutorials and manuals for creating AI-based CSAM are widely shared, allowing beginners to quickly learn the necessary techniques. They actively share knowledge, ask questions about how to "train" the software, and solve common technical problems such as visual artifacts (e.g., images with the wrong number of fingers).

Within this community, a disturbing subculture has emerged in which the creators of synthetic CSAM are often referred to and praised as "artists." There is a real appreciation and demand for these works, with a particular interest in images of famous children such as child actors or young athletes. This learning process often involves the use of real CSAM as training data for AI models, which means that existing crimes are being used to create new forms of crime. The scale of production in this ecosystem is massive. A report from the Internet Watch Foundation (IWF) found 3,512 AI-generated CSAM images and videos in a 30-day review of just one forum, a 17% increase from the previous review (IWF 2024). Another IWF report even identified more than 20,000 AI-generated images on one forum in a single month. These figures show that the creation of AI-CSAM is no longer a fringe activity, but is becoming common practice among criminals, driven by a feedback loop in which more and more forum members see it, become interested, learn how to make it, and then encourage others to do the same.

Although synthetic CSAM does not involve direct physical contact or violence in its creation, the harm it causes is very real and profound (Lazaridou 2025). For children whose images are stolen and manipulated, the psychological impact can be devastating. They become victims of an extreme form of privacy and dignity violation. The realization that their images have been altered into sexually explicit content and disseminated online can trigger severe stress, deep shame, anxiety, depression, and long-term trauma (Schmidt *et al.* 2023). This can damage their self-confidence, disrupt social relationships, and negatively impact their overall mental health. The fact that the content is "fake" does not lessen the sense of violation for victims, the feelings of being exploited and degraded are just as real.

Beyond individual impacts, the proliferation of deepfakes and synthetic content poses a broader social threat: the erosion of fundamental trust in visual content. This phenomenon is often referred to as the "infopocalypse", a condition in which society loses the ability to distinguish between real and fake information. When videos and images that appear authentic can be easily faked, the value of visual evidence in journalism, the legal system, and even everyday communication becomes degraded. Repeated exposure to manipulative content can create widespread skepticism and cynicism, lowering the level of public trust in the media, public institutions, and each other (Davy 2024). In the long term, this not only complicates the fight against disinformation but also undermines social cohesion, as the shared foundation of verifiable reality begins to crack.

In this regard, cryptocurrencies have become a key pillar supporting the dark economy in the digital space, including illicit markets for CSAM (Harwanto *et al.* 2024). The fundamental nature of decentralized blockchain technology provides a level of pseudo-anonymity that is difficult to achieve with traditional financial systems. Transactions recorded on public blockchains, such as Bitcoin, can indeed be traced, but the identities behind wallet addresses are often hidden. This allows perpetrators to conduct cross-border transactions with little regulatory oversight. This threat is exacerbated by the existence of privacy coins such as Monero, which are specifically designed to obscure transaction details (Atlam *et al.* 2024). Using advanced cryptographic techniques such as ring signatures and stealth addresses, Monero makes it nearly impossible to trace the origin, destination, or amount of funds transferred. This strong anonymity makes it the preferred choice for criminals seeking to avoid detection by law enforcement. In Indonesia, the ambiguous legal status of cryptocurrency adds another layer of complexity. Bank Indonesia strictly prohibits the use of cryptocurrencies as legal tender. However, on the other hand, the Commodity Futures Trading Regulatory Agency (Bappebti) recognizes crypto assets as commodities that can be legally traded on futures exchanges. This regulatory dualism creates a challenging environment for law enforcement in dealing with illegal cash flows related to cybercrime.

Public awareness in Indonesia regarding the risks posed by the anonymity of cryptocurrency is already quite high. Data from a survey conducted for this study shows significant concern. When asked, "To what extent do you believe that the anonymity offered by cryptocurrency makes it difficult to enforce the law against cyber-CSAM crimes?", respondents gave an average score of 4.09 on a scale of 5, indicating a high level of confidence in this statement. These findings indicate that the general public understands that the features that make cryptocurrency attractive to some investors are the same features that are exploited by criminals (Taneska 2022). This public perception reflects the real challenges faced by law enforcement agencies. Investigating crimes involving cryptocurrencies is highly complex and requires a high level of technical expertise. Law enforcement must be able to perform blockchain analysis to track the flow of funds through complex wallet networks, often via mixing services designed to obscure transaction trails. The process of seizing digital assets is also fraught with challenges these assets are protected by private keys, without which they cannot be accessed. Furthermore, the global and borderless nature of cryptocurrency networks means that perpetrators, victims, and servers may be located in different jurisdictions, creating significant legal barriers to international cooperation and extradition.

The dualism of crypto regulation in Indonesia specifically creates loopholes for law enforcement. Policies that simultaneously recognize crypto as a legal investment asset (under Bappebti) while prohibiting it as a means of payment (under Bank Indonesia) result in a fragmented framework. This fragmentation can lead to jurisdictional and procedural confusion (Fitriana and Nuraini 2023). For example, legal instruments designed to oversee traditional financial transactions may not be directly applicable to digital commodity asset transactions. Criminals can exploit this ambiguity to move and launder the proceeds of their crimes. The process of handling crypto assets as evidence in criminal cases, from seizure to management, requires specific protocols that may not yet be fully standardized across law enforcement agencies, which could ultimately slow down the judicial process and benefit criminals.

4. Discussion: Legal accountability of AI providers as technology corporations

One of the biggest obstacles to law enforcement is the difficulty of tracking perpetrators who operate behind the anonymity provided by the internet. Perpetrators often use false identities and operate from different jurisdictions, making identification, investigation, and prosecution very complicated and often impossible using conventional approaches (Nasution *et al.* 2025). This phenomenon can also be seen as a form of democratization of gender-based violence. Traditionally, sexual violence often requires physical proximity or superiority of strength. Deepfake technology removes these prerequisites, allowing anyone, often driven by motives of revenge or hatred, to commit severe psychological and reputational violence remotely and anonymously. This means that the "weapons" for committing violence are now widely available, with women being the primary targets, which has far broader social implications than simply the spread of obscene content.

The main legal framework that has been relied upon to address cybercrimes related to decency is the Electronic Information and Transactions Law (EIT Law) and the Pornography Law. However, both instruments show fundamental weaknesses when faced with the unique characteristics of pseudo-pornography. Historically, through Article 27 paragraph (1) and now Article 27A, the ITE Law focuses its prohibitions on the acts of "distributing" and/or "transmitting" content that violates decency. This focus on the offense of dissemination creates a critical legal loophole (Gunawan and Janisriwati 2023). A person can create thousands of pieces of pseudo-pornography content and, as long as they do not distribute it themselves, they could potentially escape the legal consequences of this article. This does not address the root of the problem, which is the process of creating harmful content itself. This law does not explicitly criminalize the act of creation or even possession with intent to distribute, which would be a much more effective preventive measure. Meanwhile, Law No. 44 of 2008 on Pornography has deeper conceptual flaws. The definition of "pornography" in Article 1 and the prohibitions in Articles 4 and 29 implicitly assume that the content is created with the involvement of "people" as models or objects of physical exploitation. Pseudo-pornography content that is entirely synthetic and does not involve the participation of real humans in the sexual scenes depicted could, argumentatively, fall outside the scope of this definition. This creates a legal paradox the more sophisticated AI technology becomes in creating realistic images without human intervention, the weaker the Pornography Law's ability to prosecute it.

Two other laws, namely the Child Protection Law and the Sexual Violence Criminal Law (TPKS), also face challenges in their application to synthetic crimes. The Child Protection Law lacks clarity on whether the definition of "child sexual abuse material" includes highly realistic synthetic images. In other countries, such as the United States, the law explicitly states that artificial images that are "indistinguishable" from real minors are still considered CSAM. The lack of similar precision in Indonesian law creates dangerous ambiguity, which perpetrators can exploit by arguing that "no real children were harmed" in the process of creating the images. The TPKS Law is a significant step forward, particularly through Article 14, which regulates Electronic-Based Sexual Violence (KSBE) (Rama *et al.* 2025). This article can ensnare perpetrators who "transmit electronic information... that contains sexual content against the recipient's will."

However, this article still has several weaknesses. First, its focus on "transmitting" is still oriented towards distribution offenses, so it does not explicitly target content creators who do not distribute it themselves. Second, its status as a complaint-based offense (unless the victim is a child or person with a disability) places the burden of reporting on the victim. Given the trauma, social stigma, and victim blaming often experienced by victims of deepfake pornography, this reporting obligation can create a chilling effect, where victims are reluctant to seek justice because the legal process itself can be a source of secondary trauma.

The new Criminal Code (KUHP), which will come into effect in 2026, has updated several provisions regarding indecency offenses. Relevant articles, such as Article 406 (indecent acts in public) and other provisions in Chapter XV on Indecent Acts (e.g., Articles 411-423), have been reformulated. However, the New Criminal Code still inherits the old paradigm that focuses on physical acts occurring in physical spaces. Key phrases such as "in public" or "in front of other people present" are difficult to apply directly to the context of the dissemination of digital content that is asynchronous, global, and without simultaneous physical presence. The New Criminal Code does not explicitly anticipate and formulate completely synthetic, non-physical crimes against decency that occur in cyberspace. Thus, despite being a modernization, the New Criminal Code has not fully addressed the challenges posed by generative AI.

As an initial response from the government, the Ministry of Communication and Information Technology has issued Circular Letter (SE) Menkominfo No. 9 of 2023 concerning Artificial Intelligence Ethics. This SE establishes important ethical principles for electronic system operators (PSE), such as transparency, accountability, security, and humanity. This is a positive first step in establishing norms for the industry. However, the fundamental weakness of this instrument is its nature as soft law. The Circular Letter is not legally binding and does not specify direct sanctions for violations. As a result, compliance is voluntary and its effectiveness in preventing harmful practices is very limited (Judijanto *et al.* 2025). However, this SE has the potential to be used as a standard for interpreting "good faith" or 'negligence' in other legal processes, such as in civil lawsuits or as a benchmark for assessing "corporate misconduct" in the context of criminal liability.

Indonesia needs to consider the approaches taken by other jurisdictions that have already faced the challenges of AI regulation. A comparative analysis of regulatory models in the United Kingdom, the European Union, Australia, and the United States (California) provides valuable insights. The United Kingdom, through the Online Safety Act 2023, has taken an approach that focuses on criminal law enforcement and platform responsibility. Various jurisdictions around the world have implemented diverse regulatory models to respond to the threat of AI-based pseudo-pornography, demonstrating a global consensus on the urgency of this issue. The UK, through the Online Safety Act, implements a model that focuses on platform responsibility. A key element is the shift from a reactive to a proactive model through a duty of care, which requires platforms to actively identify, assess, and mitigate the risks of illegal content and protect children (McGlynn 2024). The main breakthrough is the criminalization of the creation of sexual deepfakes, not just their distribution, which closes a significant legal loophole. The law also gives significant powers to the independent regulator,

Ofcom, to impose strict sanctions, including fines of up to 10% of a company's annual global turnover, and requires pornography platforms to implement robust age verification.

The European Union is taking a different approach through the EU AI Act, which is more oriented towards regulating the technology itself with a risk-based framework. Under this scheme, AI systems are classified according to their level of risk, and technology for generating pseudo-pornography falls under the "Limited Risk" category. Although not totally banned, this technology is subject to strict transparency obligations. These obligations include clearly labeling content so that users can see that it is "AI-generated" or "artificially manipulated." In addition, AI system providers are required to ensure that their output is marked in a machine-readable format, such as digital watermarks or cryptographic metadata, which serve as a "digital fingerprint" for automatic detection. Other countries have also taken decisive legislative steps. Australia, through the Criminal Code Amendment (Deepfake Sexual Material) Act 2024, explicitly criminalizes the creation and distribution of non-consensual deepfake sexual material, with the threat of severe criminal penalties, and affirms that it is irrelevant whether the material is original or has been altered. Meanwhile, the state of California in the United States is taking a complementary approach through civil law (Łabuz 2024). Laws such as AB 602 grant victims a private right of action against the creators and distributors of deepfake pornography. Victims can seek significant damages, including statutory damages of up to $150,000 if done with malicious intent, which provides an effective compensation mechanism for victims.

The ideal legal framework for Indonesia is one that integrates behavior-based and technology-based approaches. Technical regulations adapted from the EU AI Act, such as labeling and watermarking requirements, will serve as ex-ante preventive standards. These standards are then integrated with the Duty of Care framework and strict criminal sanctions adapted from the UK Online Safety Act as ex-post enforcement mechanisms. The logic behind this approach is very strong technical standards such as labeling and watermarking provide a clear and measurable definition of "necessary preventive measures" within the Duty of Care framework. Thus, a platform's failure to comply with mandatory technical standards can serve as prima facie evidence of corporate negligence in criminal charges, which significantly facilitates the proof of "corporate fault" and encourages the industry to comply proactively.

In this regard, in order to realize legal reform as recommended, reforms are needed at the level of substantive criminal law. Urgent amendments to the Electronic Information and Transactions Law and the Pornography Law are required. Amendments to the ITE Law must focus on adding new articles that explicitly criminalize the creation and possession with intent to distribute non-consensual synthetic pornographic content, which will close the most fundamental legal loopholes that currently exist (MP 2024). In line with this, the Pornography Law needs to update the definition of "pornography" in Article 1 to explicitly include "visual, audio, or audiovisual representations that are significantly generated or manipulated by artificial intelligence depicting sexual activities or nudity, which to a person of sound mind appear to be real individuals." A long-term solution is the drafting of a Special Law on Artificial Intelligence (AI Law). Indonesia needs to draft a comprehensive AI Law, ideally adopting a model such as

those developed in the EU and UK. This law should include the classification of AI system risks, the establishment of clear obligations for developers and platform providers, and strict and layered criminal and administrative sanction mechanisms.

The empirical data gathered from our survey is not merely illustrative; it provides a crucial sociological foundation that directly justifies the proposed legislative reforms. There is a clear, explicit relationship between the public's lived experiences in the digital space and the specific regulatory interventions required: 1) Amending the ITE and Pornography Laws to Criminalize Creation. The survey revealed that 74.5% of respondents feel highly vulnerable to digital identity theft, and 82.5% have been exposed to AI-manipulated CSAM. These figures expose the fundamental inadequacy of the current ITE and Pornography Laws, which predicate offenses primarily on the physical exploitation of a human corpus and the act of distribution. The public's high vulnerability confirms that the law must shift its paradigm. Therefore, our recommendation to amend these laws to explicitly criminalize the *creation* and *possession* of non-consensual synthetic pseudo-pornography regardless of whether the creator distributes it is a direct response to this widespread societal threat; 2) Resolving Crypto-Regulatory Dualism for Effective Enforcement. Respondents gave a high score of 4.09 out of 5 regarding their belief that cryptocurrency anonymity hinders law enforcement. This public awareness aligns with our legal analysis regarding the problematic regulatory dualism between Bank Indonesia and Bappebti. The empirical acknowledgment of this financial mechanism's danger justifies our recommendation to establish integrated forensic protocols, mandate stricter KYC (Know Your Customer) policies on crypto exchanges, and foster cross-agency collaboration to trace illicit assets used in trading pseudo-pornography; and 3) Enacting a Specific AI Law and Mandating Platform Accountability. Perhaps the most striking empirical finding is the overwhelming public consensus (88.5%) demanding mandatory identity verification for AI users and platform accountability. This provides a strong, democratic mandate for our most significant recommendation: the drafting of a comprehensive AI Law. Borrowing from the UK's *Duty of Care* model and the *EU AI Act*, implementing strict technical standards (such as mandatory digital watermarking) and holding tech corporations criminally liable for negligence is not just a theoretical ideal. It is a necessary legal intervention directly demanded by a public that feels unprotected by the current regulatory vacuum.

The phenomenon of pseudo-pornography facilitated by generative AI technology has presented unprecedented challenges for Indonesia's criminal law framework. An in-depth analysis reveals significant legal gaps, where existing regulations from the ITE Law, Pornography Law, to the TPKS Law were not designed to deal with complex, large-scale cybercrimes that are conceptually "without physical acts." (Halm *et al.* 2020). This study confirms that to effectively address this threat, a paradigm shift is needed. First, a shift from reactive law enforcement to proactive prevention. The focus can no longer be solely on removing content after it has been disseminated, but must be on preventing its creation in the first place. Second, a shift in the focus of law enforcement from anonymous and elusive individual perpetrators to technology providers, which are strategic points of control.

5. Conclusions

The discussion on cyber-CSAM through AI using cryptocurrency as a transaction tool leads to the following conclusions, among others: First, AI technology has created a new form of child exploitation known as pseudo-pornography. This crime is a new form of pornography that exploits children, shifting from physical exploitation to digital identity exploitation. The modus operandi involves stealing and manipulating images of children's faces without physically harming the victims, which ultimately leads to pornography crimes. The impact of this crime creates very real psychological trauma and a broader social threat with the erosion of trust in visual content. This crime is also rapidly metamorphosing, supported by pseudo and anonymous cryptocurrency technology that makes it difficult for law enforcement to track, exacerbated by the dualism of crypto regulations by both Bank Indonesia and Bappepti, which creates legal loopholes that make it difficult to uncover cyber-CSAM transactions through AI. Second, there is a legal vacuum regarding pseudo-pornography crimes in the Pornography Law, the ITE Law, the TPKS Law, and the new Criminal Code. This legal vacuum has been identified because it only regulates and focuses on distribution rather than production and focuses on physical human models, thus failing to ensnare anonymous perpetrators of non-physical crimes, which are cyber-CSAM crimes. The recommendation from this study is that the government needs to show good faith in addressing cybercrimes involving CSAM, especially those that use AI technology and cryptocurrency, by revising the Pornography Law and the Electronic Information and Transactions Law to prosecute perpetrators who create pseudo-pornography content, including holding platform and AI owners accountable, expanding the definition of synthetic content, and promoting an AI law to protect Indonesia's digital space from pseudo-pornography crimes.

References

Agarwala, S., 2025. Children's privacy and the ghost of social media past. *Columbia Human Rights Law Review* [online], *56*(1). Available at: https://hrlr.law.columbia.edu/files/2025/03/Agarwala_Childrens-Privacy-and-the-Ghost-of-Social-Media-Past_Final-Upload.pdf

Atlam, H. F., *et al.*, 2024. Blockchain forensics: A systematic literature review of techniques and tools. *MDPI Electronics* [online], *13*(17), 3568. Available at: https://www.mdpi.com/2079-9292/13/17/3568#

Barnes, E., 2025. Digital innocence lost: How AI and deepfakes are fueling the next generation of child exploitation. *VKTR* [online], 3 October. Available at: https://www.vktr.com/ai-ethics-law-risk/digital-innocence-lost-how-ai-and-deepfakes-are-fueling-the-next-generation-of-child-exploitation/

Chainalysis, 2025. *2025 crypto crime trends from chainalysis* [online]. 15 January. Available at: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/

Civa Melati Aulia, 2023. Safira Hunar Seleb TikTok Jadi Korban Edit Foto Vulgar oleh Orang Tak Dikenal. *Mengerti.id* [online], 22 July. Available at:

https://www.mengerti.id/seleb/6649558930/safira-hunar-seleb-tiktok-jadi-korban-edit-foto-vulgar-oleh-orang-tak-dikenal#google_vignette

Compliance Hub, 2024. *The EU AI act: Comprehensive regulation for a safer, transparent, and trustworthy AI ecosystem* [online]. 23 October. Available at: https://www.compliancehub.wiki/the-eu-ai-act-comprehensive-regulation-for-a-safer-transparent-and-trustworthy-ai-ecosystem/

Davy, D., 2024. *AI-produced child sexual abuse material: Insights from Dark Web forum discussions* [online]. 11 September. WeProtect Global Alliance. Available at: https://www.weprotect.org/blog/ai-produced-child-sexual-abuse-material-insights-from-dark-web-forum-discussions

Esoimeme, E., 2024. *Examining the potential misuse of artificial intelligence to circumvent technology-based processes for AML/CFT compliance in the cryptocurrency ecosysytem* [online]. 22 September. Available at: https://ssrn.com/abstract=4964272

Fauziyah, D., 2025. Transaksi Kripto Ilegal Diperkirakan Tembus US$51 Miliar di 2024. *Coinvestasi* [online], 28 February. Available at: https://coinvestasi.com/berita/transaksi-kripto-ilegal-tembus-miliaran-dollar-as

Federal Bureau of Investigation (FBI), 2024. *Sextortion: A growing threat preying upon our nation's teens* [online]. 17 January. Available at: https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens

Fitriana, W., and Nuraini, M. D., 2023. Juridical analysis of the duality of cryptocurrency status as a payment instrument and investment commodity in Indonesian regulation. *Journal of Transcendental Law* [online], *5*(1). Available at: https://doi.org/10.23917/jtl.v5i1.2476

Gunawan, I. J., and Janisriwati, S., 2023. Legal analysis on the use of deepfake technology. *Law and Justice* [online], *8*(2). Available at: https://doi.org/10.23917/laj.v8i2.2513

Halm, K. C., *et al*., 2020. Two new California laws tackle deepfake videos in politics and porn. *Media Law Monitor* [online], *1*(1), 1–10. Available at: https://www.dwt.com/blogs/media-law-monitor/2020/02/two-new-california-laws-tackle-deepfake-videos-in

Harwanto, F., Febriansyah, A., and Irwantika, N., 2024. Cryptocurrency, crime, and children: Unveiling the dark side of financial technology in child sexual exploitation. *Proceedings of the ASEAN Conference on Sexual Exploitation of Children (ACOSEC 2024)* [online], 876, 29. Available at: https://doi.org/10.2991/978-2-38476-325-2_4

Internet Watch Foundation (IWF), 2024. *What has changed in the AI CSAM landscape?* [online] July. Available at: https://www.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf

Judijanto, L., Utama, A. S., and Setiyawan, H., 2025. Implementation of ethical artificial intelligence law to prevent deepfakes. *The Easta Journal Law and Human Rights* [online], *3*(02), 101–109. Available at: https://doi.org/10.58812/eslhr.v3i02.470

Kan, C. H., 2024. Criminal liability of artificial intelligence from the perspective of criminal law: An evaluation in the context of the general theory of crime and fundamental principles. *International Journal of Eurasia Social Sciences/Uluslararasi Avrasya Sosyal Bilimler Dergisi* [online], *14*(55). Available at: https://doi.org/10.35826/ijoess.4434

Kupriianova, L., and Kupriianova, D., 2023. The AI in the porn industry of social media: Human replacement or precursor for growing the sexual violence and human trafficking indicators? *IV International Scientific and Theoretical Conference «Scientific forum: theory and practice of research. 6 October, Valencia* [online], 75–82. Available at: https://previous.scientia.report/index.php/archive/article/view/1236

Lin, L. S. F., 2025. Organisational challenges in US law enforcement's response to AI-driven cybercrime and deepfake fraud. *Laws* [online], *14*(4), 46. Available at: https://doi.org/10.3390/laws14040046

Łabuz, M., 2024. Deepfakes and the artificial intelligence act: An important step or a missed opportunity? *Policy and Internet* [online], *16*(1), 1–20. Available at: https://doi.org/10.1002/poi3.406

Lazaridou, M., 2025. *Schrödinger's crime: AI-generated child sexual abuse material as a victimless offense* [online]. Master's Thesis. Utrecht University. Available at: https://studenttheses.uu.nl/handle/20.500.12932/48359

Matters, I., 2024. *The new face of digital abuse: Children's experiences of nude deepfakes* [online]. Report. Internet Matters. Available at: https://www.internetmatters.org/hub/research/children-experiences-nude-deepfakes-research/

McGlynn, C., 2024. Deepfakes and the law: Why Britain needs stronger protections against technology-facilitated abuse. *Queen Mary University of London Law Review* [online], *1*(1), 1–15. Available at: https://www.qmul.ac.uk/law/news/2025/items/deepfakes-and-the-law-why-britain-needs-stronger-protections-against-technology-facilitated-abuse.html

Milmo, D., 2025. AI-generated child sexual abuse videos surging online, watchdog says. *The Guardian* [online], 10 July. Available at: https://www.theguardian.com/technology/2025/jul/10/ai-generated-child-sexual-abuse-videos-surging-online-iwf

Nasution, A. V. A., Suteki, and Lumbanraja, A. D., 2025. Addressing deepfake pornography and the right to be forgotten in Indonesia: Legal challenges in the era of AI-driven sexual abuse. *International Journal of Semiotica Iuris* [online], 38, 2489–2517. Available at: https://doi.org/10.1007/s11196-025-10265-0

Rahman-Jones, I., 2024. Taylor Swift deepfakes spark calls in Congress for new legislation. *BBC News* [online], 27 January. Available at: https://www.bbc.com/news/technology-68110476

Rama, A., Lofandri, W., and Saputra, A. F., 2025. Legal gaps in Indonesia's electronic information and transactions law in addressing deepfake technology. *Schoulid Journal of Law and Technology* [online], *5*(2), 203–211. Available at: https://doi.org/10.23916/086155011

Ramadhani, E. R., Rachmawati, A. R., and Kurnikova, R. H., 2025. Integrating Islamic values with the right to be forgotten: A legal approach to addressing deepfake pornography in Indonesia. *De Jure Jurnal Hukum Dan Syariah* [online], *17*(1), 112–131. Available at: https://doi.org/10.18860/j-fsh.v17i1.28880

Reuters, 2025. *Police take down "Kidflix" child abuse platform, Europol says* [online]. 2 April. Available at: https://www.reuters.com/world/europe/police-take-down-kidflix-child-abuse-platform-europol-says-2025-04-02/

Schmidt, F., Varese, F., and Bucci, S., 2023. Understanding the prolonged impact of online sexual abuse occurring in childhood. *Frontiers in Psychology* [online], *14*, 1281996. Available at: https://doi.org/10.3389/fpsyg.2023.1281996

Taneska, M., Dobreva, J., and Dimitrova, V., 2022. Forensics investigation comparison of privacy-oriented cryptocurrencies. *Security and Future* [online], *6*(1), 35–38. Available at: https://stumejournals.com/journals/confsec/2022/1/35

Utami, E., *et al*., 2022. Profiling analysis of DISC personality traits based on Twitter posts in Bahasa Indonesia. *Journal of King Saud University-Computer and Information Sciences* [online], *34*(2), 264–269. Available at: https://doi.org/10.1016/j.jksuci.2019.10.008

Yudhistira, F. A., and Puspitosari, H., 2025. Penegakan Hukum terhadap Pelaku Pembuat Dapat Diaksesnya Website Bermuatan Asusila dan Pornografi Anak. *Jurnal Hukum Lex Generalis* [online], *6*(7). Available at: https://ojs.rewangrencang.com/index.php/JHLG/article/view/1948