IJOBSOR, 13 (3) (2025) pp. 80-89
Published by: TRIGIN Publisher
International Journal of Politics and Sociology Research
Journal homepage: www.ijobsor.pelnus.ac.id

Legal challenges of digital technology abuse in cybersex trafficking in Indonesia

Ni Nyoman Juwita Arsawati
Faculty of Law, Universitas Pendidikan Nasional, Indonesia

ARTICLE INFO

Article history:

Received Dec 15, 2025
Revised Dec 20, 2025
Accepted Dec 30, 2025

Keywords:

Cybersex Trafficking;
Digital Criminal Law;
Legal Reform;
Victim Protection.

ABSTRACT

The rapid advancement of digital technology has transformed human trafficking into a technology-enabled crime, particularly cybersex trafficking, in which sexual exploitation is conducted entirely through online platforms without requiring physical movement of victims. In Indonesia, this phenomenon presents a serious legal challenge because existing criminal regulations have not been designed to address the digital, covert, and transnational characteristics of such crimes, resulting in inadequate protection for victims, especially children. This study employs normative legal research using legislative, conceptual, and comparative approaches by examining primary legal materials, including the ITE Law, the Anti-Trafficking Law, the Child Protection Law, and the Criminal Code, as well as secondary materials such as academic journals, international reports, and comparative regulations from Southeast Asian countries, particularly the Philippines and Thailand, published between 2015 and 2025. The analysis reveals that Indonesia's legal framework does not explicitly criminalize cybersex trafficking as a form of trafficking in persons, causing law enforcement to rely mainly on cybercrime and pornography provisions that fail to capture the trafficking dimension inherent in online sexual exploitation. This regulatory gap perpetuates structural victimization, limits access to restitution and rehabilitation for victims, and leaves the criminal responsibility of digital platform providers insufficiently regulated. Furthermore, Indonesia's non-ratification of the Budapest Convention on Cybercrime restricts effective cross-border cooperation and digital evidence handling. The study concludes that cybersex trafficking constitutes a distinct form of technology-enabled human trafficking that requires comprehensive legal reform, including explicit criminalization, the integration of a victim-centered justice approach, the imposition of corporate liability on digital platforms, and alignment with international cybercrime standards to ensure effective legal protection and justice in the digital era.

Corresponding Author:

Ni Nyoman Juwita Arsawati,
Faculty of Law,
Universitas Pendidikan Nasional,
Jl. Bedugul No.39, Sidakarya, Denpasar Selatan, Kota Denpasar, Bali, 80224, Indonesia
Email: juwitaarsawati@undiknas.ac.id

1. INTRODUCTION

The development of digital technology in the past decade has revolutionized various aspects of human life, including the modus operandi of crime. One form of crime that has undergone a significant transformation and is now rampant is cybersex trafficking, which is the practice of sexual exploitation mediated by information and communication technology. This crime no longer requires

direct physical interaction between the perpetrator and the victim, because the entire process of exploitation, content distribution, and economic transactions is carried out online through social media platforms, video-sharing sites, conversation applications, and live streaming services. The characteristics of cross-border (borderless), anonymity, and speed of data exchange make this crime increasingly difficult to detect and act upon by national legal systems that are not yet adaptive to technology.

The phenomenon of cybersex trafficking is not limited to developed countries or conflict areas, but has become a serious threat in the Southeast Asian region, including Indonesia. The ISEAS–Yusof Ishak Institute report (2025) revealed that more than 220,000 people are victims of online-based exploitation in transnational organized crime networks in Myanmar and Cambodia, including for the purpose of sexual exploitation via the internet. These crime schemes reflect the combination of human trafficking, online fraud, and the use of digital technology to facilitate and disguise criminal acts, which have clearly shaped a new dimension of transnational crime (Sriyai, 2025).

In Indonesia, the escalation of cyber-based crime with elements of sexual exploitation shows an increasingly worrying trend. Based on a Komnas HAM report quoted by the Tempo News Agency (2023), in the period from December 2022 to May 2023, there were 5,111 complaints related to online fraud, of which 1,290 cases were forms of online human trafficking.(Tempo, 2024b) The mode used by perpetrators is often in the form of fake job offers or business cooperation through social media, which ultimately plunges the victim into online sexual exploitation practices (Sarkar & Shukla, 2024). This trend is reinforced by the use of cryptocurrencies as a means of payment as well as end-to-end encryption technology, which technically makes it difficult for law enforcement officials to trace, confiscate, and prove them.

The increase in cases is also reflected in data from the National Police of the Republic of Indonesia which shows that from May to November 2024, as many as 58 suspects have been named in 47 cases of online child sexual exploitation, and 689 explicit digital content was successfully confiscated (Antara, 2024). However, many cases cannot be processed completely due to the limitations of the available legal norms. Law enforcement against this crime still depends on Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons (UU TPPO), and Law Number 23 of 2002 concerning Child Protection. Each of these laws has normative limitations and has not specifically formulated elements of cybersex trafficking that are digital, covert, and cross-jurisdictional.

The Indonesian government has actually taken a number of institutional steps, such as the establishment of Cyber Directorates in Regional Police in various regions, as an effort to strengthen institutions in dealing with cybercrime (Abast et al., 2025). This step has received appreciation from civil society institutions such as ECPAT Indonesia. However, these structural reforms have not been balanced with substantial and comprehensive regulatory reforms (Rusfiana & Kurniasih, 2024). The absence of explicit norms regarding the responsibilities of digital platform providers, cross-border tracking mechanisms, and regulations regarding the criminalization of technology-based sexual crimes creates significant legal gaps. This condition has serious implications for the protection of vulnerable groups, especially children and women, who are the main targets of online sexual exploitation.

In addition to limitations in normative aspects, substantive challenges also arise from the technical characteristics of digital crime itself. Cybersex trafficking takes place in a decentralized architecture, utilizing encrypted digital systems, and involving perpetrators from various countries with a high level of anonymity. Many perpetrators use conversational applications with end-to-end encryption systems or access hidden networks such as the dark web, making the process of identifying, tracking assets, and collecting evidence very complex. In many cases, data storage servers and criminal activities are outside Indonesia's jurisdiction, which makes it difficult for cross-border law enforcement cooperation, especially since Indonesia has not ratified the Budapest Convention on Cybercrime, which is the main reference in handling cybercrime internationally.

The problem is even more complex when the approach to victims is not fully based on the principle of human rights protection. The criminal justice system in Indonesia still places

criminalization as the main focus, while aspects of victim recovery, such as psychological assistance, restitution, social reintegration, and the removal of exploitative content have not been prioritized (Ali et al., 2022). In fact, the impact of online-based sexual exploitation is multidimensional and long-term. Victims not only suffer physical and psychological losses, but also digital trauma due to the spread of content that is difficult to remove from the internet (Rozanova-Smith et al., 2025). Indonesia has also not adopted the principle of the right to be forgotten which is an important part of the personal data protection framework, as stipulated in the General Data Protection Regulation (GDPR) in the European Union (Judijanto et al., 2024).

Another aspect that is no less important is that criminal or administrative liability has not been clearly regulated for digital platform operators. In many cases, online service providers used to disseminate sexually exploitative content are not subject to adequate legal obligations. In fact, in the corporate criminal liability approach, corporations can be held accountable if they are negligent or do not provide a mechanism for monitoring and reporting explicit and unlawful content. The absence of norms on digital corporate responsibility creates a serious legal vacuum and opens up space for repeated violations against vulnerable groups.

In the global literature, cybersex trafficking is generally discussed within the broader frameworks of transnational organized crime, cybercrime, and international human rights law. Most studies focus on cross-border enforcement challenges, platform governance, intermediary liability, and international cooperation mechanisms, often referring to regulatory models such as the GDPR, the Digital Services Act, or the Budapest Convention on Cybercrime. However, this body of scholarship tends to treat cybersex trafficking as a subset of cybercrime or online sexual exploitation, without sufficiently integrating it into the doctrinal structure of national anti-trafficking laws, particularly in developing countries.

Positioned within this global discourse, the present research contributes by examining cybersex trafficking as a distinct form of technology-enabled human trafficking within the Indonesian legal system. By integrating victimology, legality principles, and comparative legal analysis, this study addresses normative gaps in domestic trafficking regulations and offers a context-specific perspective that complements and extends existing global debates on digital-era trafficking and victim protection.

Departing from these empirical realities and regulatory complexity, this paper focuses on two main legal issues. First, what is the form of technology abuse in cybersex trafficking practices that occur in Indonesia? Second, what are the problems faced in the national legal arrangement to overcome and crack down on these crimes? Both issues are important to be studied more deeply through normative and comparative approaches, by integrating the theory of victimology, the principles of legality and legal protection, and modern criminal law concepts in an effort to build a legal framework that is responsive to technological developments and oriented towards justice for victims.

Accordingly, this paper aims to examine the forms of digital technology abuse involved in cybersex trafficking practices in Indonesia and to analyze the weaknesses and challenges of the existing national legal framework in addressing such crimes. By employing a normative and comparative legal approach, this study seeks to assess the adequacy of current regulations, identify legal gaps in substance and enforcement, and formulate a more responsive legal framework that aligns with technological developments and prioritizes victim protection, particularly for women and children.

Existing studies in reputable national legal journals have addressed online sexual exploitation and cyber-enabled crimes, yet they have not fully conceptualized cybersex trafficking as a distinct legal phenomenon. (Lisanawati, 2013), in *Pandecta Research Law Journal*, examines cyber child sexual exploitation from the perspective of cybercrime law and emphasizes the limitations of Indonesia's legal framework in protecting children from online sexual abuse. Her analysis focuses on the insufficiency of criminal provisions in addressing technology-facilitated sexual crimes and highlights the need for stronger legal protection mechanisms for child victims. However, the study situates online sexual exploitation primarily within the framework of cybercrimeocation, without explicitly linking it to the legal construction of human trafficking or the trafficking-in-persons regime.

Similarly, (Wijakusumariasih, 2019), in *Jurnal Magister Hukum Udayana*, analyzes legal protection for children against online sexual exploitation and abuse through a human rights and child protection lens. This study underscores the state's obligation to safeguard children's rights and emphasizes victim protection, rehabilitation, and the prevention of secondary victimization. Nevertheless, the analysis remains focused on victim protection norms and does not address the structural role of digital technology, transnational networks, or the abuse of digital platforms as integral elements of trafficking practices.

Compared to these studies, the present research advances the existing scholarship by positioning cybersex trafficking as a specific form of technology-enabled human trafficking, rather than merely a cybercrime or a child protection issue. This study integrates victimology theory, the principle of legality, and modern criminal law concepts to examine how digital technology reshapes trafficking practices and exposes normative gaps in Indonesia's anti-trafficking legal framework. Furthermore, by incorporating a comparative and international legal perspective, this research extends beyond prior national studies to propose a more comprehensive regulatory approach that responds to the digital, cross-border, and corporate dimensions of cybersex trafficking.

2. RESEARCH METHOD

This research uses normative legal research, which is legal research conducted by examining legal materials as the main basis for examining legal problems that have been formulated (Taekema, 2018). This approach is used because the problem of cybersex trafficking in the context of technology abuse in Indonesia is closely related to the regulation of applicable positive legal norms, both in national laws and regulations and international legal instruments (Negara, 2023). Thus, the main focus of the research lies in the identification of norm gaps, regulatory disharmony, and the need for law reform to respond to the complexity of digital-based sexual crimes.

The types of legal materials used in this study include primary legal materials, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and its amendments, Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons (TPPO), Law Number 35 of 2014 concerning Child Protection, and the Criminal Code (KUHP). In addition, secondary legal materials are used, namely relevant legal literature, previous research results, academic journals, and documents from international institutions such as the Trafficking in Persons Report by the U.S. Department of State, as well as reports from ECPAT and ISEAS on digital human trafficking practices in Southeast Asia. Tertiary legal materials in the form of legal dictionaries, encyclopedias, and legal indexes are used as support for terminology clarification.

The approach used in the analysis includes a legislative approach, to systematically and critically examine the applicable legal provisions; conceptual approach, to review legal theories relevant to the problem of cybersex trafficking and technology abuse; and a comparative approach, in order to see how other countries—particularly in Southeast Asia such as the Philippines and Thailand organize and respond to similar crimes. The technique of collecting legal materials is carried out through library research, while data analysis is carried out qualitatively through the interpretation of applicable legal norms, general legal principles, and principles of justice.

The selection of comparison countries is based on several criteria. First, the Philippines and Thailand are chosen because both countries face similar challenges to Indonesia in dealing with cybersex trafficking, particularly in the context of Southeast Asia's digital economy and transnational organized crime networks. Second, these countries have developed more explicit regulatory and institutional responses to online sexual exploitation, including specialized cybercrime units and platform-related obligations, which provide relevant comparative insights for Indonesian legal reform. Third, the legal systems of these countries share structural similarities with Indonesia, especially in their reliance on statutory criminal law, making comparative analysis methodologically relevant.

The literature and legal materials analyzed in this study cover the period from 2015 to 2025. This timeframe is selected to capture the rapid development of digital technologies, the evolution of cyber-enabled sexual exploitation, and recent legal and policy responses at both national and international levels.

Through this method, it is hoped that the research will be able to provide a comprehensive overview of the condition of Indonesia's legal regulation on cybersex trafficking, as well as identify the challenges faced in the formation, implementation, and enforcement of laws that are responsive to the development of digital technology.

3. RESULTS AND DISCUSSIONS

Abuse of Technology in the Practice of Cybersex Trafficking in Indonesia

The development of information technology has brought serious implications for the dynamics of transnational crime, particularly in the form of human trafficking that metamorphoses into the digital space. One form of such crime is cybersex trafficking, which is the practice of sexual exploitation of individual especially children which is carried out online through social media, instant messaging applications, and other digital platforms. This phenomenon has become a crucial legal issue in Indonesia, considering the rapid penetration of the internet that has not been balanced with the readiness of the national legal system to respond to forms of technology-based crime.

In practice, various cases have shown that cybersex trafficking perpetrators take advantage of the vulnerability of children in the digital space to be used as objects of sexual exploitation. For example, in October 2024, the Metro Jaya Regional Police managed to uncover two Telegram groups named "Meguru Sensei" and "Acilsunda" respectively.(Viva.co.id, 2024) Both groups contain thousands of members and are used to trade child pornography content, which is produced by the victims themselves by force. The content is sold with an online subscription system for IDR 10,000 to IDR 15,000 for a period of three months. The main perpetrator can only be charged under the provisions of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and Law Number 44 of 2008 concerning Pornography, without being subject to Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons (TPPO Law), considering that the provisions in the law are still oriented towards the physical transfer of the victim.

A similar case occurred in June 2025, where the East Java Police Special Criminal Investigation Directorate arrested a perpetrator with the initials ASF who promoted child exploitation channels through Instagram and directed consumers to Telegram channels and the Potato Chat application. The suspect has made profits exceeding IDR 240 million since mid-2023. Based on data released by the National Police Criminal Investigation Agency (Bareskrim), during the period from May to November 2024, there were at least 47 cases of online child sexual exploitation, with the number of suspects reaching 58 people. In addition, more than 15,000 sites containing child pornography have been blocked by the government (Tempo, 2024a). Komnas HAM also noted that from December 2022 to May 2023, there were 5,111 reports of technology-based crimes that led to human trafficking, with 1,290 cases categorized as digital human trafficking, most of which were carried out through fictitious job recruitment modes (News, 2024).

The analysis of this phenomenon cannot be separated from the theoretical framework of victimology. The theory of victimology was first introduced by Benjamin Mendelsohn in 1947, which underscored the importance of the role and standing of the victim in the criminal justice system (Roy, 2023). Hans von Hentig, in his classic work "The Criminal and His Victim" (1948), emphasized certain sociological and psychological characteristics that make a person more susceptible to becoming a victim (Pratt & Turanovic, 2021). This idea was expanded by Nils Christie through the concept of the "ideal victim" (1986), namely victims who are morally and socially considered worthy of defense because of their weak position, such as children and women. In the context of cybersex trafficking, children from low-income families, with minimal levels of digital literacy, are in the ideal position of victim. A further development of this theory is known as structural victimology, which highlights how social structures, access inequality, and unresponsive legal regulations magnify the vulnerability of individuals to becoming victims of crime (McAulay, 2024).

From the perspective of legal principles, the provisions of nullum crimen sine lege, as contained in Article 1 paragraph (1) of the Criminal Code (KUHP), are an obstacle in law enforcement against cybersex trafficking perpetrators. Although the Anti-Trafficking Law normatively regulates sexual exploitation as a form of human trafficking, the emphasis is still limited

to the elements of movement or physical removal of victims, so it cannot be applied effectively to digital-based exploitation. As a result, law enforcement only relies on the criminal provisions in the ITE Law and the Pornography Law, which do not specifically regulate the complexity of cyber-based trafficking crimes.

In addition, the principle of legal protection as stipulated in Article 28D and Article 28I of the 1945 Constitution of the Republic of Indonesia states that everyone has the right to equal protection, security, and recognition before the law (Hanafi, 2025). But in practice, victims of cybersex trafficking have not received comprehensive legal protection. They rarely receive restitution, do not receive adequate psychological recovery services, and widespread exploitative content is difficult to remove thoroughly from the digital space. Therefore, a victim-centered justice approach that places the victim as the main subject in the judicial process, is an urgent need in the Indonesian criminal law system.

In the dimension of international law, cybersex trafficking is classified as a cyber-enabled crime, which is a conventional crime that is enhanced through the help of digital technology. The 2001 Budapest Convention on Cybercrime, which is the first and most comprehensive international legal instrument in the fight against cybercrime, provides a framework for cooperation between countries, the preservation of digital data, and cross-jurisdictional criminal mechanisms (Buckley et al., 2024). However, until now, Indonesia has not been a party to the convention, thus missing out on strategic opportunities to effectively conduct cross-border law enforcement cooperation through mutual legal assistance and cross-border digital surveillance (Brunhöber, 2022).

At the national level, some regulations have been updated. One of them is Government Regulation Number 17 of 2025 concerning Child Protection in the Online Realm which is a derivative of the results of the revision of the ITE Law in 2024. This regulation requires electronic system operators to implement a mechanism for verifying the age of users, classification of age groups, and the implementation of data protection impact assessments (Mardika & Prabaningrum, 2025). This PP also provides a two-year transition period for digital platform operators to adjust their systems. In addition, the government is preparing regulations restricting the age of social media users to prevent children's exposure to inappropriate digital content. Although this initiative shows progress in the administrative aspect, until now there is no special criminal regulation that expressly regulates cybersex trafficking perpetrators or the criminal liability of platform providers.

By paying attention to the overall description above, it can be concluded that the misuse of information technology in cybersex trafficking practices has created serious legal challenges in Indonesia. The victims, most of whom are children, are in a very vulnerable position and have not obtained adequate legal protection. Meanwhile, the existing regulatory system has not been able to reach digital-based crime modes comprehensively. Therefore, it is necessary to carry out regulatory reforms that include the explicit criminalization of cybersex trafficking, the ratification of international conventions such as the Budapest Convention, and the strengthening of the principle of victim-centered justice within the framework of national criminal law.

Based on the foregoing analysis, it is evident that the abuse of digital technology in cybersex trafficking practices in Indonesia has transformed conventional human trafficking into a covert, decentralized, and borderless crime. Existing criminal provisions remain fragmented and reactive, relying heavily on the ITE Law and the Pornography Law, while failing to capture the trafficking dimension inherent in online sexual exploitation. From a victimological perspective, this regulatory limitation perpetuates structural victimization, particularly against children who occupy a highly vulnerable position in the digital environment. These findings underline the urgency of examining the adequacy of Indonesia’s national legal framework in a broader comparative and international context, which will be further discussed in the following subsection.

For Indonesian policymakers, these findings indicate the need for immediate regulatory intervention. First, there is a pressing necessity to reformulate the Anti-Trafficking Law to explicitly include cybersex trafficking as a form of trafficking in persons, regardless of physical movement. Second, policymakers should integrate a victim-centered justice approach by mandating restitution, psychological rehabilitation, and mechanisms for the complete removal of exploitative digital content. Third, regulatory obligations for digital platform providers must be strengthened, including duties of prevention, monitoring, reporting, and cooperation with law enforcement agencies.

Without such reforms, Indonesia's legal system will remain structurally unprepared to respond to technology-enabled sexual exploitation.

Problems of National Legal Arrangements for Cybersex Trafficking in Comparative Perspectives and International Legal Instruments

Until now, Indonesia's national legal system does not have a regulation that explicitly and explicitly criminalizes digital-based forms of human trafficking or cybersex trafficking. Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons (UU TPPO) focuses more on the elements of physical transfer of victims through recruitment, transportation, or transfer, which is not always relevant in the context of sexual exploitation carried out through digital networks. As a result, many cybersex trafficking perpetrators are only ensnared by Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) or Law Number 44 of 2008 concerning Pornography, which does not have a comprehensive normative formulation in discussing the dimensions of human trafficking, especially in complex and hidden online forms.

This problem shows that there is a significant legal vacuum in national criminal regulations, especially in the aspect of the formulation of the crime. From the perspective of victimology theory, as developed by Benjamin Mendelsohn, Hans von Hentig, and Nils Christie, this kind of legal situation is at high risk of causing structural revitalization. Children and adolescents who are victims of online sexual exploitation often lack access to justice and redress due to the absence of norms that directly acknowledge their suffering as a form of victimization in a positive legal system. By not legally acknowledging the existence of victims of cybersex trafficking, the principle of victim-centered justice has not been implemented optimally in Indonesian criminal justice practice.

In principle, this problem is also closely related to the principle of legality as stated in Article 1 paragraph (1) of the Criminal Code (KUHP), which states that no act can be punished without legal provisions that regulate it first. Therefore, without expansion or adjustment to the elements in the Anti-Trafficking Law or the establishment of new norms that specifically regulate cybersex trafficking, law enforcement officials have no legal basis to take action against perpetrators proportionately. On the other hand, the principle of legal protection, as guaranteed in Articles 28D and 28I of the 1945 Constitution of the Republic of Indonesia, affirms the right of everyone, including children, to obtain protection from violence, exploitation, and violation of rights. If national regulations are not able to provide an effective framework and protect victims from this kind of cybercrime, then the state has failed to fulfill this constitutional mandate.

When studied comparatively, a number of countries have been more advanced in formulating legal instruments that are responsive to this form of crime. The Philippines, for example, passed Republic Act No. 11930 on Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) in 2022. This regulation explicitly categorizes acts of sexual exploitation of children through the internet as a criminal act of trafficking in persons, and establishes legal responsibilities for digital service providers who do not take preventive measures, removal, or reporting on content that contains exploitation (Bag-ao, 2025). Other countries such as the United Kingdom and Australia have also adjusted their child protection laws and criminalization of online sexual exploitation by incorporating elements of the use of digital technology and criminal provisions against negligent online platform providers (Hillman et al., 2014). This comparative approach suggests that these countries are not only expanding the criminal elements of national criminal law, but are also actively creating a cross-sectoral framework that involves cooperation between states, electronic system operators, and child protection agencies.

In the dimension of international law, the Budapest Convention on Cybercrime in 2001 is the main instrument that provides a legal framework for cybercrime across jurisdictions. This convention regulates data access, preservation of digital evidence, termination of illegal content, and law enforcement cooperation between countries. Although non-binding to non-member countries, the convention has become a global normative reference in the drafting of domestic regulations on digital crimes, including those related to the sexual exploitation of children (Bunga, 2019). By mid-2025, as many as 80 countries have ratified the convention. However, Indonesia is not yet a party state, so Indonesia's involvement in international cooperation and legal alignment with global standards is still very limited.

Meanwhile, Indonesia has sought to establish a mechanism for the protection of children through Government Regulation Number 17 of 2025 concerning Child Protection in the Online Realm. This regulation requires electronic system operators (PSEs) to classify content, verify age, and provide a rapid reporting mechanism for content containing child sexual violence (Tahir & Lestari, 2025). However, the regulation is still administrative and has not been equipped with provisions for criminal sanctions for violations that result in criminal consequences, such as the dissemination of child sexual exploitation content. In addition, there is no national legal provision that requires the complete removal of illegal content (right to be forgotten), as stipulated in the General Data Protection Regulation (GDPR) of the European Union (Zaltina & Nurtjahyo, 2024).

In the perspective of the modern criminal law concept, forms of crime such as cybersex trafficking should be placed in the category of cyber-enabled crime, which is a conventional crime that is expanded and facilitated by information technology (Natalis & Djohan, 2025). Therefore, the establishment of norms is not only sufficient to regulate its actions, but must also pay attention to forms of indirect participation, including digital service providers, social media platform owners, and individuals involved in the distribution and monetization of illegal content. This concept demands reform of the structure of criminal offenses, which has been individualistic, towards a system that also recognizes and ensnares digital corporations as the subject of criminal law.

In this context, Indonesia's absence in the ratification of the Budapest Convention and the absence of a national law that specifically regulates online-based trafficking in persons are urgent issues that need to be addressed immediately. National regulatory reform must also be accompanied by strengthening the capacity of law enforcement agencies, especially in the field of digital forensics, tracking the flow of funds (follow the money), and cross-border coordination. In addition, an ideal national framework should place victims as the main subjects through the granting of the right to restitution, psychological rehabilitation, and the complete removal of content that has a direct impact on the dignity and future of the victim.

The comparative and international analysis demonstrates that Indonesia’s national legal arrangements lag behind emerging global standards in addressing cybersex trafficking. The absence of explicit criminal norms, the limited scope of administrative regulations, and Indonesia’s non-ratification of the Budapest Convention collectively weaken the effectiveness of law enforcement and victim protection. Comparative experiences from countries such as the Philippines illustrate that explicit criminalization, coupled with corporate liability for digital platforms, can significantly enhance state capacity in combating online sexual exploitation. This condition confirms that Indonesia is facing not merely a technical enforcement problem, but a systemic regulatory deficit in responding to cyber-enabled crimes.

From a policy perspective, Indonesia must prioritize comprehensive legal reform through three strategic steps. First, the enactment of a specific legal framework on cybersex trafficking that incorporates digital elements, cross-border cooperation, and corporate criminal liability is essential. Second, Indonesia should consider ratifying the Budapest Convention on Cybercrime to strengthen international cooperation, digital evidence preservation, and cross-jurisdictional enforcement mechanisms. Third, national regulations should institutionalize victim-centered protection, including restitution schemes, long-term rehabilitation, and the adoption of the right to be forgotten for victims of online sexual exploitation. These measures are crucial to ensuring that Indonesia’s criminal law system remains responsive to technological developments while upholding justice and human dignity.

4. CONCLUSION

This study confirms that cybersex trafficking represents a distinct form of technology-enabled human trafficking, characterized by digital exploitation, the absence of physical victim movement, and transnational operations. These features expose the inadequacy of Indonesia’s existing legal framework, which remains fragmented and largely oriented toward conventional trafficking and cybercrime models.

By integrating victimology, legality principles, and modern criminal law, this research reveals a condition of structural victimization in which victims particularly children are insufficiently

recognized and protected due to normative gaps in trafficking regulation. The principle of legality further limits effective enforcement when digital exploitation is not explicitly criminalized within anti-trafficking law.

The principal contribution of this study lies in repositioning cybersex trafficking as a core trafficking-in-persons issue rather than a derivative cybercrime or child protection concern. Through comparative and international analysis, this research demonstrates the urgency of legal reform that incorporates digital modalities, corporate criminal liability, and victim-centered justice. Such reform is essential to ensure that Indonesia's criminal law remains responsive to technological developments and aligned with evolving global standards on trafficking and human rights protection.

REFERENCES

Abast, B. R., Damanik, D. C., Fahmi, G. J., Hutagalung, J. M. N., & Siahaan, M. T. P. (2025). Cybercrime as a threat to national security: A review of the role and preparedness of the Indonesian Police. *Proceedings of Police Academy*, *1*(1), 119–131.

Ali, M., Muliyono, A., Sanjaya, W., & Wibowo, A. (2022). Compensation and restitution for victims of crime in Indonesia: Regulatory flaws, judicial response, and proposed solution. *Cogent Social Sciences*, *8*(1). https://doi.org/10.1080/23311886.2022.2069910

Bag-ao, B. V. C. (2025). 'In number there is strength': Multi-agency collaborative strategies for combating online sexual abuse and exploitation of children (OSAEC) in Cagayan de Oro City, Philippines. *Social Inquiry into Well-Being*, *23*(1), 26–57.

Brunhöber, B. (2022). *Criminal law of global digitality: Characteristics and critique of cybercrime law BT - The Law of Global Digitality* (pp. 223–249). Routledge.

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1).

Bunga, D. (2019). Legal response to cybercrime in global and national dimensions. *Padjadjaran Jurnal Ilmu Hukum*, *6*(1), 10–27.

Hanafi, H. (2025). The dialectics of freedom of expression and legal restrictions on digital platforms: An analysis of human rights principles, the Electronic Information and Transactions Law, and Constitutional Court Decision Number 105/PUU-XXII/2024. *International Journal of Law, Environment, and Natural Resources*, *5*(1), 57–75.

Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, *30*(6), 687–698. https://doi.org/10.1016/j.clsr.2014.09.003

Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights*, *3*(1), 20–29.

Lisanawati, G. (2013). Cyber Child Sexual Exploitation dalam Perspektif Perlindungan atas Kejahatan Siber. *Pandecta Research Law Journal*, *8*(1), 1–14. https://doi.org/10.15294/pandecta.v8i1.2348

Mardika, N. Y., & Prabaningrum, D. R. (2025). Child protection in the digital age: A review of the preventive law child pornography. *Jurnal Ius Constituendum*, *10*(2), 211–223.

McAulay, J. P. (2024). Less than ideal victims: Understanding barriers to queer men's recognition of male-perpetrated intimate partner violence through Christie's Ideal Victim framework. *International Review of Victimology*, *30*(2), 282–297. https://doi.org/10.1177/02697580231185545

Natalis, A., & Djohan, N. H. (2025). Cybersex trafficking: Legal challenges and protection for women and children in Indonesia. *International Cybersecurity Law Review*, 1–36.

Negara, T. A. S. (2023). Normative Legal Research in Indonesia: Its Originis and Approaches. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855

News, A. (2024). *Online scams new trend in human trafficking cases: Komnas HAM*. https://en.antaranews.com/news/317097

Pratt, T. C., & Turanovic, J. J. (2021). *Revitalizing Victimization Theory*. Routledge.

Roy, A. (2023). Understanding of victimology on the lens of criminal law. *Indian Journal of Law & Legal Research*, *5*(1), 1–15.

Rozanova-Smith, M., Oddsdóttir, E. E., & Petrov, A. N. (2025). Women's perspectives on progress and setbacks in gender equality in Northern Iceland during times of crisis. *Societies*, *15*(7), 191.

Rusfiana, Y., & Kurniasih, D. (2024). The role of civil society organizations in promoting social and political change in Indonesia. *Journal of Ethnic and Cultural Studies*, *11*(3), 187–207.

Sarkar, G., & Shukla, S. K. (2024). Bi-directional exploitation of human trafficking victims: Both targets and perpetrators in cybercrime. *Journal of Human Trafficking*.

Sriyai, S. (2025). *Global inequality and digital vulnerability: Unpacking online scams and human trafficking*.

ISEAS–Yusof Ishak Institute.
Taekema, S. (2018). Theoretical and normative frameworks for legal research: Putting theory into practice. *Law and Method*, *2018*(2), 1–17.
Tahir, R., & Lestari, T. Y. (2025). Children's digital rights: An in-depth analysis of Indonesia, Europe, and the US. *Eduvest – Journal of Universal Studies*, *5*(2), 1942–1964.
Tempo. (2024a). *Indonesian police block over 10,000 child sexual abuse materials on internet*.
Tempo. (2024b). *Ministry finds 5,111 online scam cases involving Indonesians abroad*.
Viva.co.id. (2024). *Sindikat ACIL Sunda terbongkar jualan pornografi anak di grup Telegram berbayar*.
Wijakusumariasih, N. P. I. (2019). Legal Protection for Children Against Sexual Exploitation and Abuse of Children Online. *Jurnal Magister Hukum Udayana*, *8*(1), 1–12. https://doi.org/10.24843/JMHU.2019.v08.i01.p01
Zaltina, P., & Nurtjahyo, L. I. (2024). Right to be forgotten as a legal protection for the victims of electronic sexual violence cases. *The Indonesian Journal of Socio-Legal Studies*, *3*(2), 1–14.