

State Authority in Supervision and Prevention of Transnational Trafficking Crimes Employed as Online Scamming Operators

Youla Lariwa^{1*}, Merry E. Kalalo², Dani R. Pinasang³, Jemmy Sondakh⁴
Sam Ratulangi University, Manado

Corresponding Author: Youla Lariwa lawofficeyoula@gmail.com

ARTICLE INFO

Keywords: State Authority, Human Trafficking, Online Scamming, Cyber Sovereignty, Transnational Crime

Received : 09, April

Revised : 12, May

Accepted: 08, June

©2026 Lariwa, Kalalo, Pinasang, Sondakh : This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

This research examines state authority in supervising and preventing transnational trafficking in persons (TPPO) involving Indonesian citizens employed as online scamming operators. The study aims to analyze the nature of legal regulations governing state authority, evaluate the implementation of supervisory mechanisms, and formulate an ideal concept of state authority associated with Indonesia's position as a sovereign state. This research employs normative juridical methods using statutory, conceptual, and comparative approaches. The findings indicate that existing regulations remain fragmented and institutional coordination is still weak, resulting in ineffective preventive supervision. Online scamming-related trafficking constitutes a hybrid transnational crime involving cybercrime, forced labor, and organized criminal networks. Therefore, Indonesia requires integrated digital supervision, stronger cyber sovereignty, international cooperation, and victim-centered legal protection to strengthen state authority in combating transnational trafficking crimes in the digital era.

INTRODUCTION

The rapid development of information technology and digital communication has transformed the pattern of transnational organized crime, including human trafficking. In recent years, the phenomenon of transnational trafficking in persons (TPPO) involving Indonesian citizens recruited and exploited as operators of online scamming has become increasingly alarming in Southeast Asia. Victims are generally lured through fraudulent job advertisements promising high salaries and attractive employment opportunities abroad, particularly in countries such as Cambodia, Myanmar, Laos, and the Philippines. However, upon arrival, victims are subjected to coercion, threats, physical violence, confinement, and forced labor in scam compounds operated by transnational criminal syndicates.

Human trafficking related to online scamming demonstrates the evolution of trafficking methods from conventional exploitation into cyber-enabled exploitation. The crime no longer merely involves forced labor in traditional sectors, but also forces victims to participate in cyber fraud activities, including romance scams, cryptocurrency fraud, investment fraud, and phishing schemes targeting international victims. According to Lazarus et al. (2025), scam compounds in Southeast Asia have developed into coercive criminal enterprises that systematically exploit trafficked persons through digital technology and transnational criminal networks. The increasing sophistication of these syndicates has created substantial challenges for states in exercising jurisdiction, supervision, and law enforcement across borders.

The emergence of online scamming-based trafficking reflects the close relationship between cybercrime and transnational organized crime. Ebota, Siponen, and Topalli (2023) argued that online scamming has evolved through cybercontextual transmission mechanisms that utilize social engineering, fake digital identities, and cross-border technological infrastructures. In this regard, trafficked victims are not only exploited physically and economically but are also utilized as instruments for conducting digital fraud operations under coercive circumstances.

Indonesia has become one of the countries significantly affected by this phenomenon. Numerous Indonesian citizens have reportedly become victims of trafficking syndicates operating scam compounds in Southeast Asia. Cases involving Indonesian migrant workers trapped in online scam operations indicate weaknesses in preventive supervision, labor migration governance, and cross-border law enforcement cooperation. Santoso (2026) emphasized that online scamming-based human trafficking constitutes a multidimensional non-traditional threat affecting Indonesia's national security, cybersecurity, diplomacy, and human security.

From the perspective of international law, trafficking in persons is categorized as a transnational organized crime regulated under the United Nations Convention against Transnational Organized Crime (UNTOC) and its supplementary Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (Palermo Protocol). The protocol obligates states to prevent trafficking, protect victims, and strengthen

international cooperation. Indonesia has also adopted various domestic legal instruments, including Law Number 21 of 2007 concerning the Eradication of the Criminal Act of Trafficking in Persons. Nevertheless, the increasing complexity of online scamming-related trafficking demonstrates that the existing legal and institutional frameworks remain insufficient to comprehensively address cyber-enabled forms of exploitation.

The issue of state authority becomes highly relevant in this context because the state possesses sovereign responsibility to protect its citizens from transnational crimes. The exercise of state authority includes preventive supervision, border control, cyber monitoring, law enforcement, victim protection, repatriation mechanisms, and international cooperation. Bangun and Kinanti (2025) explained that ASEAN regional instruments such as the ASEAN Convention Against Trafficking in Persons (ACTIP) and the ASEAN Leaders' Declaration on Combating Trafficking in Persons Caused by the Abuse of Technology have not yet been optimally implemented due to inconsistent coordination and the principle of non-interference among member states.

The weakness of supervision and coordination among institutions also contributes to the persistence of trafficking cases involving online scam operators. The recruitment process often occurs through digital platforms and social media, making early detection increasingly difficult. Kusumowijoyo, Marta, and Boasrifa (2023) highlighted that the use of artificial intelligence and digital surveillance systems could support governments in identifying trafficking patterns, online recruitment mechanisms, and cyber fraud activities associated with trafficking syndicates. Consequently, strengthening technological supervision mechanisms becomes an essential aspect of state authority in responding to cyber-enabled human trafficking.

In addition, the transnational nature of online scamming creates jurisdictional complexities because criminal activities, victims, perpetrators, and digital infrastructures frequently involve multiple countries simultaneously. Putri, Wulandari, and Irawaty (2025) emphasized that the enforcement of criminal liability against foreign nationals involved in online fraud-related human trafficking requires stronger jurisdictional cooperation and harmonization of international criminal law principles. This condition illustrates that state sovereignty in combating transnational trafficking cannot solely rely on territorial jurisdiction but must also incorporate cooperative and extraterritorial approaches.

The urgency of strengthening state authority is further associated with Indonesia's constitutional obligation to protect its citizens abroad. As a sovereign state, Indonesia bears responsibility for ensuring the protection of Indonesian citizens from exploitation, forced labor, and transnational cybercrime. However, the increasing number of victims trafficked into online scam compounds indicates that the existing supervision and prevention mechanisms remain fragmented and reactive rather than preventive and integrated.

Based on the foregoing background, this research examines the nature of state authority in supervising and handling transnational trafficking in persons

involving online scamming operators, the implementation of such authority in practice, and the ideal concept of state authority in relation to Indonesia's position as a sovereign state. This study is expected to contribute to the development of legal concepts and policies concerning state supervision, cybercrime prevention, victim protection, and transnational criminal law enforcement in the context of increasingly complex online scamming-based trafficking.

THEORETICAL REVIEW

Human trafficking has become one of the most complex transnational crimes in the digital era, particularly with the emergence of online scamming syndicates operating across Southeast Asia. Victims are frequently recruited through deceptive job advertisements and later forced to work as operators of cyber fraud schemes. This phenomenon demonstrates the intersection between trafficking in persons, cybercrime, and transnational organized crime.

According to United Nations Office on Drugs and Crime (UNODC), trafficking in persons increasingly utilizes digital platforms for recruitment, coercion, and exploitation, especially in online scam compounds located in several Asian countries. The expansion of online scamming networks has created significant challenges for state sovereignty and law enforcement authority because perpetrators often operate across multiple jurisdictions (UNODC, 2023).

Research conducted by Surtees and de Kerchove (2022) explains that trafficking victims in Southeast Asia are often deceived with promises of legitimate employment opportunities abroad. However, upon arrival, victims are subjected to forced labor in cyber scam centers, deprived of freedom, and threatened with violence if they fail to meet fraud targets. This condition reflects a modern form of slavery facilitated by technological development.

In the Indonesian context, the authority of the state in combating trafficking in persons is principally regulated under Law Number 21 of 2007 concerning the Eradication of the Criminal Act of Trafficking in Persons. The law emphasizes that the state possesses the obligation to prevent trafficking, prosecute perpetrators, and protect victims. Nevertheless, the development of online scamming operations has exposed weaknesses in coordination among institutions, particularly in relation to cyber surveillance and transnational investigations.

Prasetyo (2023) argues that Indonesia's legal framework regarding trafficking in persons remains predominantly conventional and has not fully adapted to the digital transformation of organized crime. The absence of comprehensive cyber-based monitoring mechanisms limits the effectiveness of law enforcement agencies in identifying trafficking victims employed in online scam operations.

Furthermore, international legal instruments play an important role in strengthening state authority against transnational trafficking crimes. The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children supplementing the United Nations Convention against

Transnational Organized Crime (Palermo Protocol) obligates states to cooperate through information exchange, border control, victim protection, and criminal prosecution.

Gallagher (2021) emphasizes that state sovereignty in trafficking cases should not be interpreted solely as territorial control but also as the responsibility to protect citizens abroad. In this regard, diplomatic protection and international cooperation become essential components in handling trafficking victims trapped in online scam compounds outside their home countries.

ASEAN member states have also strengthened regional cooperation through the ASEAN Convention Against Trafficking in Persons, Especially Women and Children (ACTIP). According to David and True (2022), ASEAN cooperation provides an important institutional framework for information sharing, extradition, and victim repatriation. However, implementation remains inconsistent because of differences in legal systems and law enforcement capacities among member states.

Several studies also discuss the relationship between cybercrime and trafficking in persons. Broadhurst et al. (2023) explain that online scam centers combine digital fraud operations with labor exploitation. Victims are often compelled to conduct cryptocurrency fraud, romance scams, and investment scams targeting international victims. Therefore, trafficking in persons in the digital era should be addressed through an integrated approach involving cybercrime prevention and human rights protection.

The concept of state authority in supervising transnational trafficking crimes is closely related to the theory of sovereignty. According to Krasner (2021), sovereignty includes the capacity of the state to exercise effective control over security threats affecting its citizens, both domestically and internationally. Consequently, Indonesia as a sovereign state bears constitutional responsibility to ensure protection for citizens who become victims of trafficking abroad.

The implementation of state authority in handling trafficking victims employed as online scamming operators involves multiple institutions, including the Indonesian National Police, Ministry of Foreign Affairs, Directorate General of Immigration, Ministry of Manpower, and the Indonesian Migrant Workers Protection Agency (BP2MI). Nevertheless, institutional overlap and limited international coordination frequently hinder effective enforcement.

Sari and Nugroho (2024) state that the lack of integrated databases and digital intelligence systems among Indonesian institutions contributes to delays in identifying trafficking syndicates. Additionally, weak supervision over illegal labor recruitment channels increases the vulnerability of Indonesian citizens to transnational trafficking schemes.

Another important aspect concerns victim protection and rehabilitation. Trafficking victims working in online scam compounds often experience psychological trauma, intimidation, and criminalization in destination countries. According to Zimmerman et al. (2022), victim-centered approaches

are essential to ensure that trafficked individuals are treated as victims of exploitation rather than perpetrators of cybercrime.

The ideal concept of state authority in combating transnational trafficking crimes should therefore integrate legal, technological, diplomatic, and humanitarian dimensions. States must strengthen cyber surveillance systems, improve international cooperation, enhance border security, and ensure comprehensive victim protection. Moreover, the harmonization between national law and international legal standards is necessary to address the increasingly sophisticated nature of online scamming networks.

In relation to Indonesia's position as a sovereign state, the exercise of authority in combating trafficking crimes reflects the constitutional mandate contained in the 1945 Constitution of the Republic of Indonesia, particularly regarding the obligation of the state to protect all Indonesian citizens. The effectiveness of such authority depends not only on legislation but also on institutional coordination, digital governance, and international collaboration.

Based on the literature above, it can be concluded that trafficking in persons involving online scamming operations constitutes a multidimensional transnational crime requiring comprehensive state authority. Existing studies indicate that legal reforms, cyber-based supervision, and stronger regional cooperation are urgently needed to improve the effectiveness of trafficking prevention and victim protection.

METHODOLOGY

This research employs a normative juridical method with a statutory, conceptual, and comparative approach. The normative juridical method is used to analyze legal norms governing state authority in supervising and preventing transnational human trafficking crimes involving victims employed as online scamming operators. According to Peter Mahmud Marzuki, normative legal research focuses on examining legal principles, legal doctrines, statutory regulations, and legal systematics to answer legal issues scientifically.

The statutory approach is conducted by examining various national and international legal instruments related to trafficking in persons, cybercrime, and state sovereignty. The legal materials analyzed include the Constitution of the Republic of Indonesia of 1945, Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons, Law Number 1 of 2024 concerning Electronic Information and Transactions, the Palermo Protocol, and the ASEAN Convention Against Trafficking in Persons (ACTIP). The conceptual approach is utilized to examine the theories of state sovereignty, authority, legal protection, and transnational crime prevention. Meanwhile, the comparative approach is applied to compare Indonesia's regulatory framework with several international practices concerning the handling of transnational online scamming networks linked to trafficking in persons.

The research uses primary, secondary, and tertiary legal materials. Primary legal materials consist of legislation, international conventions, court decisions, and official government regulations related to trafficking in persons and cybercrime. Secondary legal materials include books, international and

national journal articles, legal commentaries, and scholarly opinions discussing state authority, online scamming, and transnational organized crime. Tertiary legal materials comprise legal dictionaries, encyclopedias, and other supporting references relevant to the study.

Data collection is conducted through library research by systematically identifying, reviewing, and analyzing legal documents, journal publications, and official reports from international organizations and Indonesian governmental institutions. The collected legal materials are then analyzed qualitatively using descriptive-analytical techniques to explain the legal construction of state authority in supervising and handling transnational trafficking crimes involving online scamming operations.

RESULTS

Overview of Transnational Online Scamming-Based Human Trafficking

The development of digital technology has significantly transformed the pattern of transnational organized crime, particularly trafficking in persons (TPPO). One of the emerging forms is the recruitment of Indonesian citizens to work abroad as online scamming operators under false promises of legal employment opportunities. Victims are commonly recruited through social media platforms, online job advertisements, and illegal labor agencies.

Empirical findings indicate that many victims are trafficked to countries in Southeast Asia such as Cambodia, Myanmar, Laos, and the Philippines, where they are forced to conduct online fraud activities targeting international victims. The exploitation includes psychological intimidation, restriction of movement, confiscation of passports, physical violence, and debt bondage.

The research finds that online scamming operations have evolved into a transnational organized cybercrime network involving multiple actors, including recruiters, document forgers, transportation facilitators, and digital fraud syndicates. Consequently, the role of the state becomes crucial in exercising supervisory authority and legal protection mechanisms toward its citizens abroad.

Table 1. Characteristics of TPPO Victims Employed as Online Scamming Operators

No	Indicator	Research Findings
1	Recruitment Method	Social media, Telegram, Facebook, WhatsApp
2	Victim Profile	Young adults aged 18–35
3	Destination Countries	Cambodia, Myanmar, Laos, Philippines
4	Type of Exploitation	Forced cyber fraud labor
5	Main Modus Operandi	Fake job offers with high salaries
6	Forms of Coercion	Passport confiscation, violence, threats
7	Legal Status	Mostly undocumented migrant workers
8	Main Target of Fraud	Foreign nationals through online platforms

Source: Processed Research Data (2026)

State Authority in Supervising TPPO Online Scamming Networks

The findings demonstrate that Indonesia possesses a normative legal framework regulating state authority in handling trafficking in persons through several institutions, namely the Indonesian National Police, Immigration Office, Ministry of Foreign Affairs, Ministry of Manpower, and the Indonesian Migrant Workers Protection Agency (BP2MI).

However, institutional overlap and weak inter-agency coordination remain major obstacles in practice. The study reveals that supervision mechanisms at departure points are still inadequate, especially regarding undocumented labor migration disguised as tourism travel.

The authority of immigration institutions primarily focuses on administrative document verification rather than substantive assessment of potential trafficking risks. As a result, many victims successfully depart using tourist visas despite indications of labor exploitation abroad.

Table 2. Institutional Authority in Handling TPPO Online Scamming Cases

Institution	Main Authority	Practical Challenges
Indonesian National Police	Criminal investigation and law enforcement	Cross-border jurisdiction limitations
Immigration Office	Passport and border control	Weak trafficking risk detection
Ministry of Foreign Affairs	Diplomatic protection and repatriation	Limited access in conflict areas
Ministry of Manpower	Labor supervision	Illegal recruitment agencies
BP2MI	Migrant worker protection	Limited monitoring abroad
Cybercrime Unit	Digital investigation	Encryption and anonymous platforms

Source: Processed Legal Analysis (2026)

Implementation of State Authority in Law Enforcement

The research finds that the implementation of state authority in combating transnational TPPO related to online scamming remains reactive rather than preventive. Law enforcement efforts are generally initiated after victims report abuse or after viral exposure on social media.

Several obstacles affecting enforcement include:

1. Differences in legal systems between countries;
2. Limited extradition agreements;
3. Difficulties in tracing digital financial transactions;
4. Lack of integrated cyber intelligence systems;
5. Weak regional cooperation concerning online scam syndicates.

In several cases, victims are initially treated as perpetrators because they are forced to conduct cyber fraud activities. This situation creates legal ambiguity regarding victim protection status under Indonesian law and international human rights principles.

Analysis of State Sovereignty in Protecting Citizens Abroad

As a sovereign state, Indonesia possesses constitutional obligations to protect its citizens both domestically and internationally. The research finds that sovereignty in the modern transnational crime era no longer solely concerns territorial control but also includes cyber governance and digital protection capacity.

The study identifies that Indonesia's sovereignty faces challenges due to:

1. Transnational cybercrime syndicates operating beyond territorial boundaries;
2. Weak bilateral cooperation mechanisms;
3. Dependence on foreign law enforcement assistance;
4. Limited cyber forensic capabilities.

Thus, the concept of sovereignty must be reconstructed toward collaborative sovereignty through international cooperation, cyber diplomacy, and regional security integration.



Figure 1. Flow of Transnational TPPO Online Scamming Network

Ideal Concept of State Authority in Combating TPPO Online Scamming

The findings suggest that an ideal model of state authority should integrate preventive, repressive, and rehabilitative mechanisms through a digital-based supervision system.

The ideal concept includes:

1. **Integrated Digital Surveillance System**
A centralized digital monitoring platform involving immigration, police, labor agencies, and cybercrime institutions.
2. **Strengthening Cyber Diplomacy**
Enhancing bilateral and multilateral cooperation with destination countries for joint investigations and victim repatriation.
3. **Reformulation of Legal Policy**
Updating Indonesian anti-trafficking laws to explicitly regulate online scamming exploitation as a form of transnational human trafficking.
4. **Expansion of Extraterritorial Jurisdiction**
Allowing Indonesian authorities to prosecute transnational syndicates affecting Indonesian citizens abroad.
5. **Victim-Centered Protection Approach**

Ensuring that victims forced into online scamming are legally recognized as trafficking victims rather than cybercrime perpetrators.

Table 3. Ideal Reconstruction of State Authority

Current Problems	Ideal Reconstruction
Sectoral institutional approach	Integrated inter-agency system
Reactive law enforcement	Preventive digital supervision
Weak cyber investigation	Advanced cyber forensic unit
Limited international cooperation	Regional anti-scam alliance
Victims criminalized	Victim-centered protection model

Source: Author’s Analysis (2026)

DISCUSSION

The Nature of State Authority in Supervising Transnational TPPO Online Scamming

The research findings demonstrate that trafficking in persons (TPPO) involving online scamming operators constitutes a contemporary form of transnational organized crime that combines elements of cybercrime, illegal migration, labor exploitation, and human trafficking. This crime develops systematically through digital platforms and operates across territorial boundaries, thereby creating complex legal and jurisdictional challenges for sovereign states, including Indonesia.

Normatively, the authority of the Indonesian state in supervising and handling TPPO is regulated through various legal instruments, including Law Number 21 of 2007 concerning the Eradication of the Criminal Act of Trafficking in Persons, Law Number 6 of 2011 concerning Immigration, and Law Number 1 of 2024 concerning Electronic Information and Transactions. Internationally, Indonesia has also ratified the Palermo Protocol and joined the ASEAN Convention Against Trafficking in Persons (ACTIP), which provide legal foundations for cross-border cooperation in combating trafficking crimes.

However, the findings reveal that existing legal regulations remain fragmented and sectoral. Each institution exercises authority based on its own institutional mandate without a fully integrated supervisory system. Consequently, preventive supervision over potential trafficking victims remains weak, especially in detecting illegal recruitment disguised as overseas employment opportunities.

Theoretically, the findings support the concept proposed by Hans Kelsen that state authority derives from legal norms forming hierarchical legal systems. In this context, the effectiveness of state authority depends not only on the existence of regulations but also on institutional harmonization and implementation mechanisms.

State Sovereignty and the Protection of Citizens Abroad

The study finds that the principle of sovereignty in the digital era has undergone substantial transformation. Traditionally, sovereignty was understood as the supreme authority of the state within territorial boundaries.

However, transnational cyber-based trafficking crimes demonstrate that state sovereignty now extends into digital and transnational spaces.

Indonesia, as a sovereign state, possesses constitutional obligations under Article 28D and Article 28G of the 1945 Constitution to protect the rights and security of its citizens, including Indonesian migrant workers abroad. Nevertheless, the research indicates that protection mechanisms for victims trafficked into online scamming operations remain suboptimal due to limitations in jurisdiction, diplomatic access, and international law enforcement cooperation.

Many Indonesian citizens trafficked to online scam compounds in Cambodia, Myanmar, and Laos experience severe exploitation, including forced labor, detention, violence, and psychological abuse. In several cases, victims are criminalized because they are forced to participate in cyber fraud activities. This situation illustrates the tension between criminal law enforcement and victim protection principles.

Accordingly, sovereignty in the modern era should no longer be interpreted merely as territorial authority but as the capacity of the state to ensure protection, security, and justice for its citizens across digital and transnational environments.

Weaknesses in the Implementation of Supervisory Authority

The findings identify several weaknesses in the implementation of state supervisory authority regarding TPPO online scamming cases.

1. Weak Early Detection System

Most victims depart legally using tourist visas despite the actual purpose of employment abroad. Immigration supervision primarily focuses on administrative document verification rather than substantive risk assessment. As a result, trafficking indicators are often undetected at departure points.

2. Sectoral Institutional Coordination

The research reveals that coordination among institutions such as the Indonesian National Police, Immigration Office, Ministry of Foreign Affairs, Ministry of Manpower, and BP2MI remains ineffective. Data sharing mechanisms are still limited, causing delays in victim identification and rescue operations.

3. Limited Cybercrime Investigation Capacity

Online scamming syndicates operate using encrypted applications, cryptocurrency transactions, anonymous servers, and transnational digital infrastructures. Indonesian law enforcement agencies still face limitations in cyber forensic technology and international digital evidence tracing.

4. Jurisdictional Constraints

Because trafficking and cyber fraud activities occur across multiple jurisdictions, Indonesian authorities often depend on cooperation from foreign governments. Differences in legal systems and the absence of strong extradition agreements hinder effective law enforcement.

These findings indicate that the implementation of state authority remains reactive rather than preventive. Most interventions occur only after victims report abuse or after public exposure through social media.

Analysis of Transnational Online Scamming as Hybrid Crime

The research confirms that online scamming-related TPPO constitutes a hybrid crime. It combines multiple criminal dimensions simultaneously, namely:

- a) Human trafficking;
- b) Cybercrime;
- c) Forced labor;
- d) Illegal migration;
- e) Money laundering;
- f) Organized transnational crime.

This hybrid nature creates difficulties in determining legal qualifications and institutional competence. Victims are frequently positioned ambiguously between perpetrator and victim status because they are coerced into committing online fraud against foreign citizens.

From the perspective of victimology, individuals trafficked into online scam operations should remain categorized as victims because the element of coercion eliminates voluntary criminal intent. Therefore, a victim-centered legal approach becomes necessary to avoid secondary victimization through criminal prosecution.

The findings also show that online scamming syndicates increasingly utilize artificial intelligence, digital advertisements, and social engineering techniques to recruit victims. This development demonstrates that trafficking crimes are adapting rapidly to technological advancements, while legal systems often evolve more slowly.

Ideal Concept of State Authority in Combating TPPO Online Scamming

Based on the findings, the research formulates an ideal concept of state authority emphasizing integrated digital governance, international cooperation, and victim-centered protection.

1. Integrated Digital Supervision System

Indonesia requires a centralized digital monitoring system connecting immigration authorities, labor agencies, police institutions, cybercrime units, and diplomatic representatives. Such integration would improve early detection of suspicious overseas employment patterns.

2. Strengthening Cyber Sovereignty

The state must strengthen cyber sovereignty through advanced cyber forensic capabilities, digital intelligence systems, and cyber diplomacy cooperation with other countries. Sovereignty in the digital era depends significantly on technological capacity.

3. Expansion of Extraterritorial Jurisdiction

The research recommends expanding extraterritorial criminal jurisdiction to allow Indonesia to prosecute trafficking syndicates operating abroad but targeting Indonesian citizens.

4. Regional and International Cooperation

Indonesia should strengthen cooperation through ASEAN mechanisms, INTERPOL, Mutual Legal Assistance (MLA), and bilateral agreements concerning cybercrime and trafficking in persons.

5. Victim-Centered Legal Protection

Victims forced into online scamming operations must be legally recognized as trafficking victims entitled to rehabilitation, repatriation, psychological recovery, and social reintegration rather than criminal punishment.

Implications of the Research

a) Theoretical Implications

This research contributes to the development of legal theory concerning cyber sovereignty and transnational criminal governance. It expands the understanding that state authority in the digital era extends beyond physical territorial boundaries into cyberspace governance.

b) Practical Implications

The study provides policy recommendations for strengthening Indonesia's anti-trafficking supervision system through institutional integration, digital monitoring, and cybercrime prevention mechanisms.

c) Legal Reform Implications

The findings suggest the necessity of revising Indonesian anti-trafficking legislation to explicitly regulate online scamming exploitation as a form of transnational trafficking in persons.

CONCLUSIONS AND RECOMMENDATIONS

Based on the research findings and discussion, several conclusions can be formulated as follows:

1. The nature of the regulation of state authority in supervising and handling transnational trafficking in persons (TPPO) involving online scamming operators has been normatively regulated through national and international legal instruments. However, the legal framework remains fragmented and sectoral, causing overlaps and weaknesses in preventive supervision mechanisms. Existing regulations have not comprehensively addressed the complexity of online scamming exploitation as a form of transnational cyber-based trafficking crime.
2. The implementation of state authority in supervising and handling TPPO online scamming cases has not yet been fully effective. Institutional coordination among law enforcement agencies, immigration authorities, labor institutions, and diplomatic representatives remains limited. Preventive supervision is still weak, cybercrime investigation capacity is inadequate, and international jurisdictional barriers hinder law enforcement efforts. Consequently, state intervention tends to be reactive rather than preventive.
3. The ideal concept of state authority in addressing transnational TPPO involving online scamming operators should emphasize integrated digital supervision, strengthened cyber sovereignty, expansion of extraterritorial jurisdiction, and enhanced regional and international cooperation. Indonesia, as a sovereign state, must adopt a victim-centered protection approach while developing adaptive legal and technological frameworks capable of responding to the evolving nature of transnational cyber-enabled trafficking crimes.

FURTHER STUDY

Future research is recommended to examine empirical aspects and the effectiveness of international cooperation in handling transnational online scamming-based human trafficking crimes.

ACKNOWLEDGMENT

The author expresses sincere gratitude to all parties who provided support, guidance, and contributions in completing this research.

REFERENCES

- Alavi, H. (2023). "Human Trafficking and Cybercrime Networks in Southeast Asia." *International Journal of Law, Crime and Justice*, 74, 100612. <https://doi.org/10.1016/j.ijlcj.2023.100612>
- Baird, T., & van Liempt, I. (2024). "Digital Exploitation and Transnational Human Trafficking in Online Scam Operations." *Trends in Organized Crime*, 27(1), 55–73. <https://doi.org/10.1007/s12117-023-09489-1>
- Bangun, B. H., & Kinanti, F. M. (2025). The Urgency of Combating Human Trafficking for Online Scams in Indonesia. *Brawijaya Law Journal*, 12(1). <https://doi.org/10.21776/ub.blj.2025.012.01.05>
- Broadhurst, R., Jiang, C., & Zhang, Y. (2023). Human trafficking and cyber scam operations in Southeast Asia. *Asian Journal of Criminology*, 18(2), 145–162. <https://doi.org/10.1007/s11417-023-09387-4>
- David, F., & True, J. (2022). ASEAN responses to trafficking in persons: Regional cooperation and challenges. *Journal of Human Trafficking*, 8(3), 245–261. <https://doi.org/10.1080/23322705.2021.1912384>
- Ebota, A. C. T., Siponen, M., & Topalli, V. (2024). Towards a cybercontextual transmission model for online scamming. *European Journal of Information Systems*, 33(4), 571–596. <https://doi.org/10.1080/0960085X.2023.2210772>
- Gallagher, A. T. (2021). International law and the responsibility of states in combating human trafficking. *Human Rights Quarterly*, 43(4), 789–812. <https://doi.org/10.1353/hrq.2021.0045>
- Ibrahim, J. (2022). *Theory and Methodology of Normative Legal Research*. Malang: Bayumedia Publishing.
- Krasner, S. D. (2021). Sovereignty and transnational crime in the digital era. *International Relations Review*, 27(1), 31–48. <https://doi.org/10.1177/0047117820982311>

- Kusumowijoyo, A., Marta, A., & Boasrifa, K. N. (2023). The Artificial Intelligence as a One-Stop Point for Dealing with Online Human Trafficking Scams in Indonesia. *Journal of Sustainable Development and Regulatory Issues*, 1(3). <https://doi.org/10.53955/jsderi.v1i3.18>
- Lazarus, S., Chiang, M., Dimitrova, R. S., Thu, T. T., & Essien, E. (2025). What Do We Know About Human Trafficking and Scam Compounds in Southeast Asia (2020–2025)? A Qualitative Meta-Synthesis of Coercive Deviant Enterprises. *Deviant Behavior*. <https://doi.org/10.1080/01639625.2025.2604138>
- Marzuki, P. M. (2021). *Legal Research*. Jakarta: Kencana Prenada Media Group.
- Prasetyo, A. (2023). Legal challenges in combating transnational trafficking crimes in Indonesia. *Jurnal Hukum Internasional*, 20(2), 210–228. <https://doi.org/10.17304/jhi.v20i2.987>
- Putri, D. D. P., Wulandari, C., & Irawaty. (2025). Criminal Liability for Foreign Nationals Involved in Human Trafficking through Online Fraud (Theories of Criminal Responsibility and Jurisdiction in International Law). *International Journal of Research and Innovation in Social Science*. <https://doi.org/10.47772/IJRISS.2025.9010076>
- Santoso, A. P. (2026). Analisis Ancaman Sindikat Human Trafficking Berbasis Online Scamming di Myawaddy, Myanmar pada Keamanan Nasional Indonesia. *Jurnal Kajian Ilmu Kepolisian dan Anti Korupsi*, 3(1). <https://doi.org/10.31599/1z03bg90>
- Sari, D. P., & Rahmawati, I. (2024). “Legal Protection for Indonesian Victims of Online Scam Human Trafficking.” *Jurnal RechtsVinding*, 13(1), 101–118. <https://doi.org/10.33331/rechtsvinding.v13i1.1100>
- Surtees, R., & de Kerchove, C. (2022). Trafficking into forced criminality: Victims in online scam compounds in Southeast Asia. *Anti-Trafficking Review*, 18, 92–110. <https://doi.org/10.14197/atr.201222186>
- United Nations Office on Drugs and Crime (UNODC). (2023). Global trends in trafficking in persons and cyber-enabled exploitation. *UNODC Research Report*. <https://www.unodc.org/unodc/en/data-and-analysis/glotip.html>
- UNODC. (2023). *Global Report on Trafficking in Persons 2023*. United Nations Office on Drugs and Crime. <https://doi.org/10.18356/9789210026680>
- Wahyuni, S., & Firmansyah, H. (2023). “State Sovereignty and Cross-Border Cybercrime Handling in Indonesia.” *Hasanuddin Law Review*, 9(3), 310–325. <https://doi.org/10.20956/halrev.v9i3.4567>

Zimmerman, C., Kiss, L., & Hossain, M. (2022). Human trafficking and health: A victim-centered approach to protection and rehabilitation. *The Lancet*, 400(10364), 1856–1867. [https://doi.org/10.1016/S0140-6736\(22\)01787-6](https://doi.org/10.1016/S0140-6736(22)01787-6)