

Reconstruction of Police Legal Policy in Preventing Human Trafficking Crimes through Digital Platforms as a Transnational Crime in Indonesia

M. Reza Pranata*, Sutrisno, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; rezapranata594@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; sutrisnosuki18@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6320>

*Correspondence: M. Reza Pranata

Email: rezapranata594@gmail.com

Received: 08/08/2026

Accepted: 27/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

strengthening cyber policing, establishing an integrated early warning system, utilizing artificial intelligence and big data, and strengthening international cooperation to create a more effective, adaptive, and human rights-oriented digital-based human trafficking prevention system in Indonesia.

Abstract: Human trafficking through digital platforms has evolved into a modern transnational crime that utilizes social media, instant messaging applications, online job platforms, and digital technology to recruit and exploit victims across borders. This study aims to analyze police legal policies in preventing digital platform-based human trafficking crimes in Indonesia, identify regulatory weaknesses and empirical obstacles faced by the Indonesian National Police, and formulate a reconstruction of cyber-policing-based legal policies in preventing human trafficking as a transnational crime. This study employs a normative juridical method compared a legislative and a conceptual approaches through an analysis of various national regulations and international legal instruments related to human trafficking and digital law enforcement. The results show that applicable legal policies are not yet adaptive to the development of digital technology-based human trafficking because they are still oriented towards a repressive approach and do not specifically regulate digital trafficking, platform liability, cyber surveillance, and preventive cyber policing. In addition, the Indonesian National Police face structural, substantial, and technological obstacles such as limited digital forensics, the use of anonymous accounts and foreign servers, weak inter-agency coordination, and a suboptimal early detection system for human trafficking in cyberspace. Therefore, a reconstruction of police legal policy is needed through regulatory reformulation,

Keywords: human trafficking, cyber policing, digital platforms, transnational crime

Introduction

Human trafficking in the era of globalization and digital transformation has undergone a very complex development from conventional patterns to digital technology-based patterns that are transnational, organized, and difficult to detect by conventional law enforcement systems. (Irawan, 2026) While previously human trafficking crimes were carried out through direct recruitment, falsification of physical documents, or traditional agent networks, currently the modus operandi has developed through social media, instant messaging applications, online job vacancy platforms, and even digital payment systems and cryptocurrencies that allow perpetrators to disguise their identities and move the proceeds of crime quickly across national jurisdictions (Nuraeny, 2022). From an

international legal perspective, the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (the 2000 Palermo Protocol), classifies human trafficking as a transnational organized crime. Indonesia ratified this protocol through Law Number 14 of 2009. Article 3 of the Palermo Protocol defines human trafficking as the recruitment, transportation, transfer, harboring, or receipt of persons through threats, deception, abuse of power, or other forms of exploitation. In addition, the United Nations Office on Drugs and Crime (UNODC) places human trafficking as one of the fastest-growing crimes in the world because it exploits the development of information technology and weak cross-border supervision. At the regional level, the ASEAN Convention Against Trafficking in Persons, Especially Women and Children, ratified through Law Number 12 of 2017, also emphasizes the importance of regional cooperation in preventing digital technology-based human trafficking (Nugroho, 2018). This situation demonstrates that digital globalization has expanded the operational space of human trafficking syndicates while weakening the effectiveness of traditional oversight mechanisms by law enforcement, which remain territorially and administratively oriented.

The phenomenon of human trafficking through digital platforms in Indonesia is a highly worrying development, as victim recruitment is now systematically conducted through Facebook, Instagram, TikTok, Telegram, WhatsApp, and online job sites, with the modus operandi of offering high-paying jobs abroad without formal migrant worker placement procedures. In practice, many victims are recruited to work as online scam operators, online gambling administrators, engage in sexual exploitation, and even forced labor in Cambodia, Myanmar, and Laos, all controlled by transnational crime syndicates. According to Article 1, point 1 of Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, human trafficking includes the recruitment, transportation, harboring, sending, transfer, or receipt of a person by means of threats of violence, fraud, abuse of power, debt bondage, or payment for exploitation (Elenta, 2026). However, the development of digital modes has caused the implementation of these norms to face new challenges because recruitment is carried out through anonymous and cross-border cyberspace. Data from the BP2MI (Indonesian Agency for the Protection of Human Resources and Migrant Workers), the Indonesian National Police, and the Ministry of Foreign Affairs show an increase in the number of Indonesian citizens who are victims of human trafficking in Cambodia and Myanmar, most of whom are recruited through social media and instant messaging applications. In fact, many victims come from vulnerable groups such as women, migrant workers, young people of productive age, and low-income communities who are easily influenced by digital job advertisements (Krisna, 2025). This situation shows that the transformation of digital-based human trafficking has developed faster than the detection, monitoring, and prevention capabilities of the police, posing a serious threat to the protection of human rights and national security in Indonesia.

In response, the Indonesian National Police (Polri) faces significant complexity due to the use of digital-based human trafficking systems, encrypted communication systems, anonymous accounts, fake identities, virtual private networks, overseas servers, and cryptocurrency payments, which complicate the process of tracing the perpetrators' identities and the flow of criminal funds. This situation creates structural, substantial, and

technological obstacles in Indonesia's law enforcement system. Based on Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police, the main duties of the Polri include maintaining public security and order, law enforcement, and community protection and service. However, in practice, the Polri's institutional capacity to address cyber-enabled trafficking still faces various limitations, particularly in digital forensics, cyber intelligence, international data exchange, and cross-jurisdictional electronic evidence (Wiguna, 2026). Furthermore, mutual legal assistance mechanisms and international cooperation are often hampered by differences in legal systems between countries, jurisdictional issues, and limited access to digital data located outside of Indonesia. From a criminal procedural law perspective, electronic evidence is recognized through Article 5 of Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024. However, this regulation does not specifically address the mechanisms for proving the relationship between digital platform-based human trafficking, which involves cross-border and anonymous technology. Consequently, law enforcement officials often encounter difficulties in proving the link between digital recruiters, international syndicates, and victim exploitation, thus suboptimal enforcement and prevention effectiveness (Saputra, 2025).

This problem is further exacerbated by weaknesses in legal policy and disharmony in regulations in Indonesia. Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking is still fundamentally structured within the conventional human trafficking paradigm and therefore does not explicitly regulate digital recruitment, platform liability, artificial intelligence-based trafficking, cybersurveillance, or digital technology-based preventive policing systems. Furthermore, there is disharmony between the Anti-Trafficking Law and the Electronic Information and Transactions Law, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 6 of 2011 concerning Immigration, Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers, and the Police Law, resulting in the handling of digital-based human trafficking not being normatively integrated (Adnan, 2024). From the perspective of the formation of legislation, this condition indicates a normative vacuum, normative ambiguity, and normative conflict that impacts the weakness of legal certainty and the effectiveness of prevention. For example, there are no clear regulations regarding the responsibility of digital platforms for illegal recruitment content, the mechanism for blocking human trafficking syndicate accounts, or the authority of the National Police to conduct preventive cyber surveillance without violating the public's right to privacy (Andriani, 2024). As a result, existing legal policies still tend to be repressive after the victim occurs and have not been able to build a prevention system that is adaptive to developments in digital technology and the character of modern transnational crime.

On the other hand, the police's prevention system and preventive approach in handling digital-based human trafficking are still conventional and have not fully utilized developments in information technology. Tackling human trafficking is still predominantly carried out through repressive action rather than developing a prevention system based on cyber patrol, predictive policing, digital intelligence, artificial intelligence monitoring, and real-time mapping of trafficking networks. In fact, Article 14 paragraph (1), letter i of the Police Law gives the National Police the authority to protect the safety of life, body,

property, society, and the environment from disturbances of order and disasters, including digital crimes that develop in cyberspace (Limadibrata, 2025). However, in practice, there is no integrated early warning system capable of detecting digital human trafficking recruitment patterns from an early stage. In addition, weak coordination between agencies such as the Ministry of Communication and Digital, Immigration, BP2MI, Interpol, and ASEANAPOL often causes data exchange and handling responses to be slow and sectoral. Low digital literacy in the community also increases the vulnerability of victims to information manipulation and online job vacancy fraud (Wulandari, 2026)

. This situation indicates that Indonesia's human trafficking prevention system still lags behind the rapid, flexible, and internationally digital network-based developments in cyber-enabled transnational crime.

Based on these various issues, the reconstruction of police legal policy is an urgent need to address the development of digital platform-based human trafficking as a modern transnational crime. This reconstruction must be directed at reformulating regulations that are more adaptive to technological developments, strengthening the authority of the National Police in cyber policing, optimizing international cooperation, and integrating big data and artificial intelligence into early detection systems for human trafficking. Furthermore, legal reforms are needed to regulate the responsibilities of digital platforms, implement human rights-based cyber oversight mechanisms, and implement a preventive policing model that is not solely repressive but also victim-centered and provides restorative justice for victims of human trafficking. From the perspective of a modern rule of law, as affirmed in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, the state has a constitutional obligation to protect human rights and ensure the safety of its citizens from the increasingly complex threat of human trafficking due to digital transformation. Therefore, a futuristic policing and smart law enforcement model is needed that can integrate digital technology, cross-border cooperation, data protection, and a human rights approach in a balanced manner so that police legal policies in Indonesia can be more effective, preventive, and responsive in dealing with human trafficking as a digital platform-based transnational crime.

Methodology

This research employs a normative juridical research method under a statutory approach and a conceptual approach. The statutory approach is used to examine various regulations related to the crime of human trafficking and the authority of the police in preventing digital-based transnational crimes, including Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, Law Number 2 of 2002 concerning the Indonesian National Police, Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers, as well as various international legal instruments such as the Palermo Protocol and the ASEAN Convention Against Trafficking in Persons Especially Women and Children. Meanwhile, a conceptual approach is used to examine legal concepts related to human trafficking as a transnational organized crime, cyber-enabled trafficking, cyber policing, preventive law enforcement, futuristic policing,

and human rights protection in a digital law enforcement system. The types and sources of legal materials in this study consist of primary legal materials in the form of laws and international legal instruments, secondary legal materials in the form of books, scientific journals, research results, and doctrines of legal experts, and tertiary legal materials in the form of legal dictionaries and legal encyclopedias. The technique of collecting legal materials is carried out through literature studies with the methods of inventory, classification, and systematization of legal materials relevant to the research object. Furthermore, the analysis of legal materials is carried out prescriptively-analytically using deductive reasoning to find legal arguments, identify gaps and weaknesses in norms, and formulate the reconstruction of adaptive, preventive, and digital technology-based police legal policies in preventing the crime of human trafficking as a transnational crime in Indonesia.

Result and Discussion

Police Legal Policy in Preventing Human Trafficking Crimes through Digital Platforms as a Transnational Crime in Indonesia

The police's legal policy in preventing human trafficking crimes through digital platforms is essentially part of the national law enforcement policy in dealing with the development of information technology-based transnational crimes. Human trafficking is currently no longer carried out conventionally, but has utilized social media, instant messaging applications, online job vacancy platforms, and digital transaction systems to recruit, control, and exploit victims across countries. In the context of international law, human trafficking is categorized as a transnational organized crime, as emphasized in the Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children Supplementing the United Nations Convention against Transnational Organized Crime of 2000 or the Palermo Protocol, which has been ratified through Law Number 14 of 2009. Article 3 of the Palermo Protocol states that human trafficking includes the recruitment, transportation, transfer, harboring, or receipt of a person by means of threats of violence, fraud, abuse of power, or other forms of exploitation. At the national level, regulations regarding the crime of human trafficking are stipulated in Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, specifically Article 1, number 1, which stipulates that human trafficking is the act of recruiting, transporting, harboring, sending, transferring, or receiving a person through threats of violence, abduction, confinement, fraud, abuse of power, debt bondage, or the payment of payment for exploitation. This provision demonstrates that human trafficking is a serious crime that threatens human rights and requires police legal policies that adapt to developments in digital technology (Mardan, 2025).

Within the national legal system, the Indonesian National Police (Polri) has strategic authority in preventing the crime of human trafficking, as stipulated in Law Number 2 of 2002 concerning the Indonesian National Police. Article 13 of the Police Law stipulates that the main duties of the Polri include maintaining public security and order, law enforcement, and protecting, serving, and providing services to the community. Furthermore, Article 14 paragraph (1) letter g and letter i emphasize that the Indonesian National Police is tasked

with conducting investigations and inquiries into all criminal acts in accordance with criminal procedural law and protecting the safety of life, body, and property of the public from security disturbances. In the context of digital-based human trafficking, this authority provides a legal basis for the Indonesian National Police to take preventive measures through cyberspace surveillance, cyber patrols, mapping digital trafficking networks, and international cooperation in exchanging information on transnational crimes. In addition, Article 15 paragraph (1) letter a of the Police Law gives the Indonesian National Police the authority to receive public reports and complaints, while Article 15 paragraph (2) letter k provides other authorities in accordance with relevant laws and regulations in handling technology-based crimes (Noval, 2022). Thus, the police's legal policy in preventing digital platform-based human trafficking has strong normative legitimacy in the Indonesian legal system.

The development of human trafficking through digital platforms is also closely related to the use of information and communication technology, so its regulation cannot be separated from Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. Article 27A and Article 28 of the ITE Law, in principle, provide a legal basis for the dissemination of misleading, detrimental, or manipulated electronic information that can be used in the recruitment mode of human trafficking victims through digital media. In addition, Article 5 paragraph (1) of the ITE Law recognizes electronic information and electronic documents as valid legal evidence so that they can be used in the process of investigating and investigating digital-based human trafficking. In practice, human trafficking syndicates often use anonymous accounts, fake identities, and encrypted messaging applications to recruit victims through fake job advertisements with the lure of high salaries abroad. This condition requires the National Police to develop a cyber policing policy that is not only repressive in orientation, but also preventive through proactive digital surveillance. However, cyber surveillance by law enforcement officers must still adhere to the protection of privacy and human rights as guaranteed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which affirms the right of every person to protection of themselves, their families, their honor, their dignity, and their sense of security (Harahap, 2025).

In addition to digital law enforcement, police legal policies in preventing human trafficking also relate to the protection of Indonesian migrant workers, the group most vulnerable to becoming victims of cross-border human trafficking. Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers stipulates in Article 5 that the state is obliged to guarantee the protection of Indonesian migrant workers before, during, and after employment. Furthermore, Article 68 regulates the importance of monitoring the recruitment of illegal migrant workers, which could potentially become a method of human trafficking. In practice, many victims are recruited through social media and digital platforms, posing as customer service representatives, online casino operators, or digital company administrators in Cambodia, Myanmar, and Laos, resulting in forced labor exploitation and torture. Therefore, the Indonesian National Police (Polri) must not only

function as a repressive force after a crime has occurred, but must also play an active role in prevention through digital education, cyber patrols, identification of illegal recruiter accounts, and cross-agency coordination with the Ministry of Communication and Digital, BP2MI (Indonesian Agency for the Protection of Human Resources), the Directorate General of Immigration, and international organizations such as Interpol and ASEANAPOL. This approach is necessary because the character of modern human trafficking has evolved into a cyber-enabled transnational crime that moves very quickly and exploits gaps in the public's weak digital literacy (Pasaribu, 2025).

From a criminal law policy perspective, preventing digital platform-based human trafficking is not sufficient through a penal or repressive approach alone; it must also be integrated with non-penal policies and information technology-based prevention systems. It aligns with the provisions of Article 58 of Law Number 21 of 2007, which emphasizes the importance of cooperation between the government, regional governments, communities, families, and social institutions in preventing the crime of human trafficking. Furthermore, Article 59 stipulates that the government is obliged to take preventative measures through education, outreach, and monitoring of potential human trafficking cases. In the digital context, the implementation of these norms should be realized through the development of an integrated digital prevention system that allows the Indonesian National Police (Polri) to monitor online recruitment patterns, analyze suspicious activity in big data, and use artificial intelligence to detect trafficking networks more quickly and accurately. However, currently, applicable legal policies tend to be conventional and do not specifically regulate platform liability, the responsibilities of social media providers, or oversight mechanisms for the digital algorithms used by human trafficking syndicates to seek out victims systematically. As a result, the effectiveness of prevention still depends heavily on the pattern of action taken after victims are found or after public reports are received by law enforcement (Kamilah, 2026).

Police legal policy in preventing human trafficking through digital platforms requires normative, institutional, and technological strengthening to meet the challenges of modern transnational crime. This strengthening should be directed at reformulating regulations that explicitly govern cyber trafficking, expanding the National Police's preventive authority in digital surveillance based on due process of law, strengthening international cooperation, and integrating a national cyber intelligence system to detect transnational human trafficking networks. Furthermore, it is necessary to develop a futuristic policing and smart law enforcement model that utilizes artificial intelligence, cyber intelligence, digital forensics, and international data exchange in an integrated manner while upholding the principle of human rights protection. It aligns with the objectives of a state based on the rule of law, as affirmed in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, which positions the law as an instrument for community protection and a guarantor of social justice. Therefore, police legal policy in preventing human trafficking through digital platforms must be reconstructed to be more adaptive, preventative, humane, and technology-based to effectively protect the public from the threat of human trafficking as a transnational crime in Indonesia.

Regulatory Weaknesses and Police Obstacles in Preventing Digital Platform-Based Human Trafficking in Indonesia

Regulatory weaknesses in preventing digital platform-based human trafficking in Indonesia are fundamentally rooted in the national legal system's lack of adaptation to the development of transnational cybercrime, which utilizes digital technology as the primary means of recruiting and exploiting victims. Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking regulates a general prohibition on human trafficking through Article 2 paragraph (1), which states that anyone who recruits, transports, harbors, sends, transfers, or receives a person through threats of violence, fraud, abuse of power, or debt bondage for exploitation shall be subject to imprisonment and a fine. However, this regulation is still formulated within the conventional human trafficking paradigm and therefore does not specifically address digital platform-based human trafficking, such as recruitment through social media, the use of artificial intelligence to manipulate victim identities, exploitation through cyber scam systems, or the use of cryptocurrency in criminal transactions. As a result, there is a lack of norms regarding digital platform oversight mechanisms, the responsibilities of electronic service providers, and the authority of law enforcement officers to conduct preventive cyber surveillance against illegal recruitment activities in cyberspace. Empirically, this condition is evident in the rampant recruitment of victims through Facebook, Telegram, TikTok, and WhatsApp, using the modus operandi of high-paying overseas job vacancies that are difficult to reach by conventional legal oversight due to the use of anonymous accounts, overseas servers, and rapidly changing fake identities.

The issue of disharmony between laws and regulations has resulted in digital-based human trafficking efforts not being implemented effectively and in an integrated manner. Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law does recognize electronic evidence through Article 5 paragraph (1), but does not specifically regulate the obligations of digital platforms to detect, report, or close accounts used by human trafficking syndicates. On the other hand, Law Number 27 of 2022 concerning Personal Data Protection provides strict protection for access to personal data, so that, in practice, law enforcement officers often experience difficulty in quickly obtaining digital platform user data for prevention and investigation purposes. This situation is exacerbated by the lack of synchronization of regulations between the Human Trafficking Law, the Electronic Information and Transactions Law, Law Number 6 of 2011 concerning Immigration, Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers, and Law Number 2 of 2002 concerning the Indonesian National Police. Empirically, this disharmony has led to weak inter-agency coordination in addressing digital human trafficking cases, for example, in cases involving the illegal sending of migrant workers to Cambodia and Myanmar, which involve online recruitment, falsified travel documents, and even forced labor exploitation in online scams and cross-border online gambling. Many victims are ultimately rescued too late due to slow data exchange and the lack of an integrated inter-agency system.

Regulatory weaknesses are also evident in the lack of clear regulations regarding platform liability, or the legal responsibility of social media and digital application providers for human trafficking activities occurring within their systems. Currently, national regulations have not explicitly mandated digital platform companies to conduct active monitoring, remove illegal recruitment content, or automatically report suspicious activity related to human trafficking. Yet, in empirical practice, human trafficking syndicates systematically exploit social media algorithms to target vulnerable groups such as young women, migrant workers, and low-income communities by offering fake jobs that appear legitimate and convincing. Many recruiters even use paid advertising and fake accounts that are difficult for law enforcement to track. The absence of regulations regarding digital platform liability means that prevention efforts rely more on public reports or repressive action after victims are identified. This shows that the national legal system is still lagging behind the rapid and flexible development of digital crime methods. In fact, Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees the right of every citizen to fair legal certainty, so the state should be able to establish regulations that provide effective protection against the threat of digital technology-based human trafficking.

In addition to regulatory issues, the Indonesian National Police (Polri) faces legal and institutional challenges in preventing digital platform-based human trafficking. Pursuant to Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police, Polri is responsible for maintaining public order and security, enforcing the law, and providing protection to the community. However, the normative framework governing this authority does not yet provide a specific and integrated mechanism for addressing trafficking activities facilitated through anonymous accounts, encrypted communication, foreign-based digital infrastructure, cryptocurrency transactions, and cross-border electronic platforms. These characteristics, as reflected in documented cases and academic discussions concerning cyber-enabled trafficking, create legal and operational complexities in identifying perpetrators, preserving electronic evidence, and coordinating investigations across jurisdictions.

Therefore, the issue identified in this study is not intended as an independent empirical measurement of national forensic capacity or institutional performance. Rather, the normative analysis demonstrates that existing regulations do not yet comprehensively establish a specialized legal framework concerning cyber-enabled trafficking investigations, cross-border digital evidence, AI-assisted monitoring, or coordinated data exchange. This regulatory gap provides the basis for reconstructing police legal policy toward a more integrated cyber policing model capable of responding to the characteristics of digitally facilitated transnational trafficking.

Another empirical problem is the weak preventive approach and the lack of an early detection system for digital human trafficking in Indonesia. To date, prevention efforts are still predominantly carried out through repressive tactics after victims report cases or cases go viral on social media. However, Article 14 paragraph (1) letter i of the National Police Law authorizes the Indonesian National Police (Polri) to protect public safety from various

forms of security threats, including transnational digital crime. In practice, cyber patrols and digital space monitoring remain suboptimal due to limited human resources, monitoring technology, and budget. Furthermore, there is no integrated early warning system capable of detecting human trafficking recruitment patterns in real time through social media and digital applications. This situation is exacerbated by the public's low digital literacy, which causes many victims to believe foreign job advertisements without official verification. Empirical data show that the majority of digital human trafficking victims come from low-income communities and those of productive age who are tempted by offers of high-paying jobs. Due to the weak prevention system, many victims only realize they are being exploited after arriving in their destination country and experiencing confinement, torture, or forced labor within an international online scam network.

Understandably, the legal system and police policies in Indonesia are not fully prepared to address the transformation of human trafficking into a cyber-enabled transnational crime based on digital platforms. Existing legal policies still tend to be reactive and repressive, while technological developments demand a more preventative, adaptive, and digitally integrated approach. Therefore, regulatory reform is needed to explicitly regulate digital platform-based human trafficking, strengthen the preventive authority of the Indonesian National Police in cyber policing, establish a platform liability mechanism, and develop a faster and more effective international cooperation system based on digital data exchange. In addition, the state needs to build an integrated digital prevention system that utilizes artificial intelligence, big data analysis, cyber intelligence, and predictive policing to detect human trafficking activities from the digital recruitment stage. This step is crucial to realizing the protection of human rights as guaranteed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which affirms the right of every person to personal protection, a sense of security, and freedom from the threat of fear. Therefore, regulatory reform and strengthening police capacity are fundamental requirements in building an effective digital-based human trafficking prevention system in Indonesia.

Reconstruction of Cyber Policing-Based Police Legal Policy in Preventing Human Trafficking as a Transnational Crime in Indonesia

The reconstruction of police legal policies based on cyber policing in preventing human trafficking as a transnational crime in Indonesia must begin with regulatory updates capable of addressing the transformation of trafficking activities through digital technology. Law Number 21 of 2007 already criminalizes trafficking through a formulation that covers recruitment, transportation, transfer, harboring, or receipt of persons through legally prohibited means for the purpose of exploitation. However, the Law does not specifically regulate the legal consequences arising when digital platforms, electronic communication systems, algorithmic targeting, cryptocurrency transactions, anonymous accounts, or other digital infrastructures function as the primary instruments for recruitment, coordination, concealment, financial transactions, or exploitation.

For this purpose, digital platform-based human trafficking or cyber-enabled trafficking should be legally defined as trafficking conduct in which an electronic system,

digital platform, online communication service, automated technology, or other digital infrastructure is knowingly used as a substantial instrument for the recruitment, facilitation, coordination, control, transfer, concealment, financing, or exploitation of a person, provided that the underlying conduct fulfills the constituent elements of human trafficking under Law Number 21 of 2007. The digital element therefore does not create a separate offense independent from trafficking but constitutes a specific modality requiring additional rules concerning prevention, evidence, platform responsibility, and investigation.

This concept must be distinguished from online fraud, illegal migrant-worker recruitment, and ordinary cybercrime. Online fraud may involve deception through electronic systems without the purpose of exploiting a person through the legally relevant elements of trafficking. Illegal migrant-worker recruitment concerns violations of placement procedures but does not necessarily involve exploitation or trafficking. Likewise, a cybercrime may involve unlawful access or manipulation of electronic systems without involving trafficking in persons. The proposed concept therefore requires a legally identifiable connection between the digital conduct and the act, means, and purpose of trafficking.

In addition to regulatory reform, the reconstruction of police legal policy must also be directed toward strengthening cyber policing through the establishment of a Cyber Anti-Trafficking Center within the Indonesian National Police as a specialized national coordination and analytical unit. Its legal basis should be established through legislation or implementing regulations that clearly define its functions, institutional position, scope of authority, relationship with existing cybercrime and trafficking units, and accountability mechanisms. The Center should function as a hub for digital intelligence, risk analysis, electronic evidence coordination, inter-agency referral, and cross-border cooperation, while coercive investigative measures remain subject to the authority and procedural requirements applicable under criminal procedure law.

The Center may employ artificial intelligence, machine learning, big-data analytics, and cyber patrols to analyze publicly available information and other lawfully obtained data. AI-assisted analysis may identify combinations of risk indicators, including unverifiable recruiter identities, repeated use of fraudulent accounts, inconsistencies in employment information, links to previously identified trafficking networks, suspicious payment patterns, and recruitment communications associated with documented trafficking methods. However, no single keyword, destination, personal characteristic, or communication pattern should automatically classify an individual or recruitment activity as trafficking-related.

To control false positives and algorithmic bias, AI systems must operate through multi-factor risk assessment, periodic accuracy testing, independent bias evaluation, documented model updates, and mandatory human review before an alert results in an investigative or restrictive action. Individuals should not be profiled solely on the basis of ethnicity, gender, age, economic status, nationality, or other protected personal characteristics. AI-generated findings should function as analytical leads rather than autonomous determinations of criminality.

The operational authority of the Cyber Anti-Trafficking Center must also comply with Article 28G paragraph (1) of the 1945 Constitution and Law Number 27 of 2022 concerning Personal Data Protection. Monitoring should be based on legality, necessity, proportionality, purpose limitation, and accountability. Publicly available content may be analyzed within the scope of statutory authority, whereas access to private communications, non-public account data, or other protected electronic information must follow legally authorized procedures. The system should apply data minimization, role-based access, encryption, audit logs, defined retention periods, cybersecurity testing, and external or internal oversight mechanisms to prevent misuse.

Reconstruction of police legal policy must also prioritize a preventative approach through the establishment of a national anti-trafficking early-warning and integrated data-exchange system. The proposed system should connect legally relevant information held by Polri, BP2MI, Immigration, PPATK, the Ministry of Communication and Digital, and the Ministry of Foreign Affairs. To prevent institutional overlap, Polri, through the Cyber Anti-Trafficking Center, should function as the primary operational coordinator for criminal intelligence and trafficking-risk analysis, while data governance should be regulated through a multi-agency framework in which each institution remains the controller and responsible authority for data originating from its statutory functions.

The national anti-trafficking dashboard should not provide unrestricted access to a centralized database. Instead, it should operate through role-based access, purpose limitation, data minimization, authentication, encryption, access logging, and differentiated retention periods. Access to financial information, immigration data, migrant-worker records, or personal data must be limited to authorized personnel and legally defined purposes. Every data request and transfer should be recorded and auditable, while cybersecurity standards and incident-response procedures must be established to address unauthorized access, data breaches, or misuse.

The dashboard should primarily display risk trends, aggregated patterns, verified network connections, case coordination status, and other information necessary for prevention and investigation. Personally identifiable information should only be accessible where necessary and authorized by law. AI-based predictive analysis may generate early-warning indicators, but those indicators must be subject to human verification and must not automatically result in arrest, travel restriction, account blocking, or other measures affecting fundamental rights.

In addition to strengthening technological systems, the reconstruction of police legal policy must also be carried out through strengthening international cooperation in addressing human trafficking as a transnational crime. Cooperation with Interpol, ASEANAPOL, Cambodia, Myanmar, Laos, and other relevant jurisdictions should be translated into specific operational mechanisms. First, designated contact points should be established for urgent preservation and exchange of digital evidence, including recruitment communications, account information, electronic transaction records, cryptocurrency-related information, platform metadata, and other electronically stored information.

Second, Indonesia should establish procedures for joint cyber investigations involving coordinated case analysis, synchronized investigative measures, and legally documented transfers of electronic evidence to preserve evidentiary integrity and chain of custody. Third, cooperation should include mechanisms for cross-border asset tracing, freezing, confiscation, and recovery where trafficking proceeds are held through conventional financial institutions, digital payment systems, or virtual assets.

Fourth, cooperation should provide clear procedures for identifying victims, conducting coordinated rescue operations, facilitating emergency consular access, securing temporary protection, and carrying out safe repatriation. Fifth, extradition and mutual legal assistance mechanisms should be strengthened for suspects operating across jurisdictions, while cross-border requests to digital platforms should be processed through legally recognized preservation, disclosure, and evidentiary procedures. These mechanisms should be implemented through bilateral or multilateral arrangements that establish response timelines, competent authorities, data-protection safeguards, and accountability for cross-border information sharing.

The reconstruction of police legal policy must also be oriented towards victim protection and increasing public digital literacy as part of a long-term prevention strategy. In this context, the Indonesian National Police (Polri) acts not only as a law enforcement officer but also as a community protection institution that actively provides digital education to vulnerable groups. Specifically, the Indonesian National Police (Polri) needs to implement a national digital anti-trafficking campaign through social media, schools, campuses, villages, and migrant worker communities, with a focus on educating about digital human trafficking methods, verifying overseas job vacancies, and the dangers of international cyber scams. Furthermore, authorities should establish an integrated digital complaint service through a mobile application and a national hotline, enabling the public to report suspicious recruiter accounts quickly and anonymously. Regarding victim protection, the Indonesian National Police (Polri) must strengthen its victim-centered approach by providing psychological support, legal aid, social rehabilitation, and digital identity protection for victims of human trafficking. This step is crucial to realizing the protection of human rights as guaranteed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which affirms the right of every person to a sense of security and protection from the threat of fear.

The reconstruction of police legal policy based on cyber policing must be directed toward developing a futuristic policing and smart law enforcement model that is adaptive to digital technology and the dynamics of modern transnational crime while remaining subject to due process of law and human rights protection. The proposed model should therefore combine substantive legal reform, platform due diligence, AI-assisted early warning, regulated digital surveillance, integrated data governance, international cooperation, and victim protection within a single normative framework.

Legal reform should not treat technology merely as an instrument of surveillance. Instead, technology should function as a legally controlled instrument for identifying risk, preserving evidence, coordinating institutions, protecting potential victims, and supporting

proportionate law-enforcement action. The proposed reconstruction therefore requires amendments to substantive legislation and the adoption of implementing regulations that clearly define authority, authorization procedures, institutional responsibility, technological standards, data-protection safeguards, oversight, complaint mechanisms, and sanctions for misuse of authority or failure to comply with statutory obligations.

To provide a concrete normative direction, the proposed reconstruction should be translated into specific model provisions. First, Law Number 21 of 2007 should recognize digital platform-based or cyber-enabled trafficking as trafficking conduct in which electronic systems or digital infrastructures constitute a substantial instrument for recruitment, facilitation, coordination, control, financing, or exploitation, while retaining the essential legal elements of trafficking. Second, relevant provisions of the Electronic Information and Transactions Law should establish proportionate due-diligence obligations for platforms hosting designated high-risk recruitment content, including identity verification, notice-and-review procedures, lawful content restriction, preservation of electronic evidence, and cooperation with authorized authorities.

Third, regulations concerning the Indonesian National Police should provide a legal basis for the Cyber Anti-Trafficking Center, define its institutional authority, limit surveillance activities according to legality, necessity, and proportionality, and require judicial or other legally prescribed authorization for access to protected communications or data. Fourth, AI-assisted analysis should be subject to human oversight, accuracy testing, bias assessment, auditability, and a prohibition against solely automated decisions affecting fundamental rights. Fifth, inter-agency data sharing should be governed by purpose limitation, data minimization, role-based access, retention limits, encryption, cybersecurity requirements, audit logs, and sanctions for unauthorized disclosure or misuse.

Finally, implementing regulations should establish early-warning procedures, victim referral mechanisms, emergency cross-border coordination, preservation of digital evidence, complaint mechanisms, institutional accountability, and proportionate administrative or other applicable sanctions for officials or electronic service providers that intentionally violate clearly established legal obligations. Through these provisions, the reconstruction becomes a concrete legal architecture rather than a general policy recommendation.

Conclusion

The study reveals that the development of human trafficking through digital platforms has changed the character of human trafficking crimes from conventional crimes to cyber-enabled transnational crimes that are complex, organized, and cross-border, utilizing advances in information technology as the primary means of recruitment and exploitation of victims. Current modes of human trafficking are carried out through social media, instant messaging applications, online job platforms, and digital transaction systems, which complicate detection and monitoring by law enforcement officials. In this context, police legal policies in Indonesia have not been fully adaptive to the development of digital technology-based human trafficking because applicable regulations, particularly Law

Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, are still oriented towards conventional human trafficking patterns and do not specifically regulate digital trafficking, platform liability, cyber surveillance, or preventive cyber policing. In addition, there is disharmony between the Human Trafficking Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, the Police Law, and the Law on the Protection of Indonesian Migrant Workers, which prevents the digital-based human trafficking prevention system from being implemented in an integrated manner. Empirically, the Indonesian National Police (Polri) also faces various structural and technological obstacles, such as limited digital forensics, the use of anonymous accounts and foreign servers, weak international data exchange, and suboptimal cyber patrol and early detection systems for human trafficking in cyberspace. Therefore, the reconstruction of police legal policies based on cyber policing is an urgent need through regulatory updates, strengthening the National Police's preventive authority, integrating artificial intelligence and big data technology, strengthening international cooperation, and developing a digital prevention system oriented towards protecting human rights and public safety.

The study recommended that the government and the House of Representatives (DPR) immediately reform Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking by including specific provisions regarding digital platform-based human trafficking, the responsibilities of electronic platform providers, cyber surveillance mechanisms based on due process of law, and strengthening the preventive approach within the law enforcement system. Furthermore, the Indonesian National Police (Polri) needs to develop a modern cyber policing model through the establishment of a Cyber Anti-Trafficking Center, the development of an integrated early warning system, the optimization of artificial intelligence-based cyber patrols, and the enhancement of human resource capacity in the fields of cyber intelligence and digital forensics. Strengthening coordination between institutions such as the Ministry of Communication and Digital, BP2MI, the Directorate General of Immigration, PPATK, and the Ministry of Foreign Affairs must also be carried out through an integrated digital data exchange system to accelerate the detection and prevention of transnational human trafficking. At the international level, the government needs to strengthen cooperation with Interpol, ASEANAPOL, and trafficking destination countries such as Cambodia, Myanmar, and Laos in the form of joint cyber investigations and digital data exchange on transnational human trafficking networks. Furthermore, it is necessary to increase the digital literacy of the public through national education on the dangers of digital human trafficking and verification of overseas job vacancies to prevent people from easily becoming victims of digital exploitation. Thus, the reconstruction of police legal policies based on cyber policing is expected to be able to create a human trafficking prevention system that is more adaptive, preventative, effective, and equitable in addressing the dynamics of modern transnational crime in Indonesia.

References

- Andriani, N. A. (2024). Penggunaan Media Elektronik Dalam Perdagangan Manusia Lintas Negara. *Aladalah: Jurnal Politik, Sosial, Hukum Dan Humaniora*.
- Elenta, R. S. (2026). Perlindungan Hukum Terhadap Korban Tindak Pidana Perdagangan Orang Dan Modus Rekrutmen Kerja Luar Negeri Melalui Media Sosial. *Jurnal Ilmiah Multidisiplin Ilmu*.
- Harahap, A. E. (2025). Pengaruh Perdagangan Digital Terhadap Peningkatan Ekonomi Masyarakat. *Jurnal Intelek Insan Cendikia*.
- Irawan, P. S. (2026). Kejahatan Transnasional Terorganisasi Di Era Digital: Analisis Tren Kejahatan Siber Dan Perdagangan Manusia Tahun 2025-2026. *Jurnal Pendidikan Masyarakat Indonesia Harapan*.
- Kamilah, A. R. (2026). Janji Manis Berujung Tragis: Modus Operandi Perdagangan Orang Terhadap Perempuan. *Legal Dialogica*.
- Krisna, S. P. (2025). Pengaruh Teknologi Digital Dalam Modus Perdagangan Orang: Analisis Pidana Terhadap Kasus Online Scamming Di Myanmar. *Kertha Desa: Journal Ilmu Hukum*.
- Limadibrata, R. W. (2025). Menyoroti Kebijakan Hukum Pidana Terhadap Kasus Perdagangan Perempuan Di Indonesia Dengan Modus Rekrutmen Melalui Media Sosial. *Jurnal Hukum Lex Generalis*.
- Mardan, A. A. (2025). Diplomasi Negara Terhadap Maraknya Perdagangan Manusia Di Balik Industri Judi Online Di Kamboja. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 1148–1154.
- Noval, S. M. (2022). Modus Operandi Dan Strategi Pencegahan Kejahatan Perdagangan Seksual Anak Secara Daring. *Undang: Jurnal Hukum*, 419–451.
- Nugroho, O. C. (2018). Tanggung Jawab Negara Dalam Penanganan Tindak Pidana Perdagangan Orang. *Jurnal Penelitian Hukum De Jure*.
- Nuraeny, H. (2022). Tindak Pidana Perdagangan Orang Kebijakan Hukum Pidana Dan Pencegahannya. *Jakarta: Sinar Grafika*.
- Pasaribu, A. O. (2025). Legal Analysis Of Human Trafficking Through Platforms Based On Indonesian Laws And Regulations. *Jurnal Hukum Sehasen*, 1–8.
- Saputra, R. (2025). *Reformasi Hukum Acara Pidana: Menyongsong KUHAP Baru*. Jakarta: Langgam Pustaka.
- Wiguna, Z. P. (2026). Efektivitas Perlindungan Hukum Terhadap Perdagangan Orang Online Di Bp2mi Sulsel. *Legal Dialogica*.
- Wulandari, D. A. (2026). Tindak Pidana Perdagangan Orang Pada Kelompok Rentan Di Aplikasi Online. *Wijaya Putra Law Review*, 183–206.