

Law Enforcement Updates on Human Trafficking Crimes Through Monitoring of Social Media-Based Digital Recruitment and Online Platforms by the Indonesian Police

Zikri Muamar*, Syafruddin, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; zikrimuamar1991@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; syafruddin@stik-ptik.ac.id

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

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6324>

*Correspondence: Zikri Muamar

Email: zikrimuamar1991@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/>).

Abstract: *The development of digital technology has shifted the pattern of human trafficking crimes from conventional methods to anonymous, rapid, and cross-border recruitment based on social media and online platforms. This study aims to analyze the weaknesses of the Indonesian legal system in addressing digital recruitment in human trafficking crimes, examine the problems of law enforcement by the Indonesian National Police, and formulate an ideal legal reconstruction and reform in dealing with digital-based human trafficking. This study employs a normative juridical method that combines legislative and conceptual approaches by analyzing various regulations related to human trafficking crimes, information technology, cyber law enforcement, and legal protection. The results of the study indicate that national regulations, such as Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking and the Law on Information and Electronic Transactions, do not specifically regulate the supervision of digital recruitment, digital platform accountability, cyber patrols, digital surveillance, and cross-border enforcement mechanisms. In addition, the Indonesian National Police still faces limitations in cyber policing, minimal digital forensic capacity, difficulties in tracking anonymous accounts, and weak inter-agency coordination in handling digital-based human trafficking. Therefore, legal reconstruction and reform are needed through strengthening cyber policing, integrating cyber patrols and digital intelligence, optimizing electronic evidence, regulating digital platform obligations, and strengthening*

international cooperation to build a law enforcement system that is responsive, preventative, and adaptive to developments in digital technology.

Keywords: *human trafficking, digital recruitment, cyber policing, digital platforms*

Introduction

The development of digital technology has brought fundamental changes to the patterns of social interaction, economics, and communication in global society, including the transformation of the modus operandi of human trafficking crimes. The internet, social media, instant messaging applications, and digital platforms are no longer merely means of communication, but are also used as instruments of transnational crime that can reach victims quickly, anonymously, and across regions. (Danuri, 2019) Perpetrators of human trafficking crimes today no longer rely on conventional recruitment through field agents or

physical networks, but instead utilize platforms such as Facebook, Instagram, TikTok, Telegram, WhatsApp, and online job vacancy sites to recruit victims by offering jobs, scholarships, marriages, and even opportunities to work abroad with high economic rewards (Saputra, F. S., & Lawoleba, 2024). This phenomenon shows that cyberspace has developed into a new medium for human exploitation practices that are difficult for law enforcement to monitor. Normatively, Article 1, paragraph 1 of Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking defines human trafficking as the act of recruiting, transporting, harboring, sending, transferring, or receiving a person through threats of violence, fraud, abuse of power, or other forms of exploitation. However, this definition is still fundamentally oriented toward physical recruitment patterns and does not explicitly accommodate the rapidly evolving digital transformation (Nugroho, 2018). On the other hand, Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees the right to fair legal certainty, while Article 28G paragraph (1) guarantees personal protection and a sense of security for every citizen. Therefore, the state has a constitutional obligation to establish a legal system capable of protecting the public from the increasingly complex and organized threat of digital technology-based human trafficking.

The increase in human trafficking cases using digital recruitment methods in Indonesia demonstrates a correlation between the development of information technology and the increasing vulnerability of the public to cyber-based exploitation. Various empirical reports from the Indonesian National Police, the Ministry of Women's Empowerment and Child Protection, the Indonesian Migrant Workers Protection Agency, and international organizations such as the International Organization for Migration and the United Nations Office on Drugs and Crime show that social media is the dominant medium in recruiting victims of human trafficking, especially women, children, job seekers, and economically disadvantaged groups. (Elenta, R. S., & Waruwu, 2026) Victims are generally recruited through fake accounts that offer high-paying jobs, overseas jobs without official procedures, entertainment contracts, or online marriages. This condition is exacerbated by the low digital literacy of the community and the high unemployment rate, which causes people to easily fall into online fraud. Legally, this practice not only fulfills the elements of the crime of human trafficking as regulated in Article 2 of Law Number 21 of 2007, but also has the potential to fulfill the elements of the crime of electronic fraud and the dissemination of misleading information as regulated in Article 28 paragraph (1) in conjunction with Article 45A of Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions (Putra, R. R., Pratama, D. I., Kaloko, I. F., Niyobuhungiro, J., & Febriyanti, 2026). The problem is that the implementation of these provisions still faces various evidentiary obstacles because the legal relationship and communication between perpetrators and victims are conducted digitally, using anonymous accounts, fake identities, and encrypted communication applications that are difficult to trace. Thus, the development of digital recruitment methods indicates that human trafficking has evolved into a form of cyber-enabled crime that requires a technology-based and digital intelligence-based law enforcement approach.

The characteristics of digital recruitment in human trafficking crimes indicate the transformation of human trafficking into a form of organized cybercrime involving cross-

border networks, the use of virtual identities, and encrypted communication systems. Perpetrators generally utilize anonymous accounts, virtual private networks, overseas servers, and encryption-based applications to evade law enforcement (Kusuma, K. M., Assa, N. J., Mutasya, N., & Wulandari, 2025). The crime is no longer individualistic but involves an organized crime network with a systematic structure for recruitment, distribution of victims, control of communications, and money laundering. These conditions indicate that digital-based human trafficking (TPPO) shares characteristics with transnational cybercrime, making it impossible to address it solely through conventional approaches. (Wiguna, Z. P., Arifin, M. Y., & Muhdar, 2026) From an international legal perspective, the Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children, as an additional protocol to the United Nations Convention against Transnational Organized Crime, positions human trafficking as a transnational organized crime that requires cross-border cooperation and integration of law enforcement systems. Indonesia itself has ratified the United Nations Convention against Transnational Organized Crime through Law Number 5 of 2009, thus legally obligated to strengthen national legal instruments to address the development of digital-based human trafficking methods (Salsa, 2021). However, currently, the national legal system still lacks specific regulations regarding cyber trafficking, digital recruitment monitoring, or digital tracing mechanisms in human trafficking crimes. As a result, law enforcement officials often encounter jurisdictional obstacles, difficulty obtaining electronic data from foreign platforms, and limitations in conducting digital forensic investigations into transnational human trafficking networks.

The weakness of the Indonesian legal system in regulating digital recruitment for human trafficking is evident in the lack of harmonization of regulations specifically governing the supervision of digital platforms, the accountability of electronic service providers, cyber patrol mechanisms, and the deletion of illegal recruiter accounts. Law Number 21 of 2007 essentially only regulates elements of human trafficking in general, without anticipating the development of recruitment methods based on social media and digital platforms. Meanwhile, the Electronic Information and Transactions Law is more oriented towards regulating electronic transactions and the misuse of digital information in general, rather than specifically addressing digital recruitment for human trafficking. (Alhakim, 2024) Even the new Criminal Code, through Law Number 1 of 2023, does not provide a specific formulation regarding cyber trafficking or the responsibility of digital platforms that facilitate the spread of illegal recruitment. This is despite Article 15 of the ITE Law already regulating the obligation of electronic system providers to operate systems reliably and securely, while Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions also requires protection against misuse of electronic systems (Mulyati, D., Dewi, E., & Tamza, 2026) However, these regulations are still general in nature and do not explicitly require digital platforms to actively monitor human trafficking recruitment content. Due to this lack of norms, many digital platforms have, in fact, become a means of recruiting victims without having clear legal responsibility for the illegal activities taking place within their systems. This situation indicates a legal vacuum that prevents the national legal system from effectively addressing the complexities of digital-based human trafficking.

The challenges facing the Indonesian National Police (Polri) in handling digital recruitment of human trafficking (TPPO) are increasingly complex due to limited cyber policing capacity and weak digital forensic infrastructure. Law enforcement officers still face difficulties in tracking anonymous accounts, obtaining electronic data from foreign platforms, and identifying transnational crime networks that use encrypted communications. Furthermore, limited human resources competent in digital forensic investigation often result in suboptimal electronic evidence collection processes (Mustofa, A. A., Soekorini, N., & Aranggraeni, 2026). Although Article 5 of the ITE Law recognizes electronic information and electronic documents as valid legal evidence, the implementation of these provisions in digital-based TIP law enforcement practices still faces technical and procedural obstacles, particularly regarding the chain of custody of digital evidence, metadata validity, and access to foreign servers. Furthermore, coordination between the police, the Ministry of Communication and Information Technology, the National Cyber and Crypto Agency, the Indonesian Migrant Workers Protection Agency, and international institutions remains suboptimal (Wulandari, D. A., & Fitriyana, 2026). As a result, case handling processes are often sectoral and slow to respond to the rapid development of digital crime methods. This situation indicates a gap between the development of criminal technology and the capacity of national law enforcement institutions. If this situation persists, law enforcement against digital-based human trafficking will become increasingly ineffective and potentially increase the rate of human exploitation in cyberspace.

Based on these various problems, legal reforms to address digital recruitment and human trafficking are an urgent need within the Indonesian legal system. Legal reforms cannot focus solely on increasing criminal penalties but must also be directed at reconstructing a digital technology-based law enforcement system that is adaptive to the development of transnational cybercrime. The state needs to develop a cyber policing model integrated with cyber patrols, digital intelligence, artificial intelligence surveillance, and an early detection system for illegal recruitment activities on social media and online platforms. Furthermore, stricter regulations are needed regarding the obligations of digital platforms to monitor content, report suspicious activity, delete illegal recruiter accounts, and provide electronic data access to law enforcement officers based on due process of law. Legal reform must also strengthen international cooperation in digital tracing and cross-border data exchange, given the transnational nature of digital-based human trafficking. From a rule of law perspective, such reforms implement the principles of legal protection, legal certainty, and legal benefit, as fundamental objectives of the modern criminal justice system. Therefore, Indonesia needs a legal reconstruction that is not only repressive but also preventive, adaptive, and technology-based to effectively and sustainably address the challenges of law enforcement regarding digital recruitment in human trafficking.

Methodology

This study employs a normative juridical research method that focuses on the analysis of legal norms, legal principles, legal theories, and regulations related to digital recruitment-based human trafficking crimes from the perspective of law enforcement reforms by the Indonesian Police. Normative juridical research was chosen because this

study aims to examine the gaps in norms, regulatory disharmony, and weaknesses of the national legal system in addressing the development of human trafficking methods through social media and online platforms. The approaches used in this study are the statute approach and the conceptual approach. The legislative approach is carried out by examining various regulations related to the crime of human trafficking, information technology, cyber law enforcement, and human rights protection, including the 1945 Constitution of the Republic of Indonesia, Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions, Law Number 1 of 2023 concerning the Criminal Code, and various regulations related to the implementation of electronic systems and cyber law enforcement. Meanwhile, a conceptual approach is used to analyze the concept of the rule of law, legal protection, cyber policing, cybercrime, digital platform accountability, and criminal law reform as a theoretical basis in formulating an ideal legal construction to overcome digital recruitment regarding human trafficking. The legal materials used consist of primary, secondary, and tertiary legal materials, which are analyzed qualitatively using descriptive-analytical methods to produce systematic, comprehensive, and prescriptive legal arguments regarding the need for legal reform for enforcing digital-based human trafficking crimes in Indonesia.

Result and Discussion

Analysis of Weaknesses in the Indonesian Legal System in Combating Digital Recruitment in Human Trafficking

The development of digital technology has shifted the patterns and modus operandi of human trafficking from conventional forms to more complex, anonymous, and cross-border recruitment systems based on social media and online platforms. Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking regulates human trafficking through the concepts of recruitment, transportation, harboring, sending, transfer, or receipt of persons for exploitation, as stipulated in Article 1 number 1 and Article 2 paragraph (1). However, these provisions do not expressly regulate the technological modalities through which recruitment may be conducted, including recruitment through social media, encrypted messaging applications, anonymous accounts, algorithmically distributed advertisements, or online job platforms.

For the purpose of legal reconstruction, digital recruitment for human trafficking should be defined as any act of identifying, approaching, attracting, persuading, communicating with, or arranging the movement of a person through electronic systems, digital platforms, social media, messaging applications, or other information technologies, where such conduct is carried out by means of threats, deception, abuse of vulnerability, abuse of power, fraud, or other unlawful methods and is directed toward the exploitation of that person. This formulation preserves the essential elements of human trafficking while recognizing the use of digital technology as the means through which recruitment is initiated or facilitated.

This concept must be distinguished from ordinary online job advertising, which constitutes lawful recruitment when the identity of the recruiter, the employment

opportunity, contractual terms, and destination are genuine and legally verifiable. It is also distinct from ordinary electronic fraud because the legal focus is not merely financial deception, but the recruitment or control of a person for exploitation. Likewise, illegal migrant-worker recruitment may constitute a separate administrative or criminal violation, whereas digital recruitment becomes part of human trafficking when the recruitment process contains the legally relevant elements of coercion, deception, abuse of vulnerability, or other prohibited means directed toward exploitation. The absence of such a specific formulation currently makes it more difficult to identify the relationship between virtual recruitment activities and the substantive elements of trafficking when the perpetrator and victim never meet physically (Prameswari, 2025).

A further weakness is evident in the limitations of Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law in addressing digital-based human trafficking crimes. Normatively, the ITE Law regulates electronic systems, electronic information, and electronic documents, including the recognition of electronic evidence as stipulated in Article 5 paragraphs (1) and (2). Article 15 paragraph (1) further requires electronic system operators to operate electronic systems reliably and securely and to be responsible for the operation of their systems. However, these provisions do not specifically establish differentiated obligations for digital platforms where recruitment for human trafficking may occur.

Legal reconstruction should therefore establish proportionate platform due-diligence obligations based on the nature and risk level of the electronic service. Online job platforms should be required to conduct reasonable verification of the identity and legal status of recruiters or recruiting companies before high-risk overseas employment advertisements are published. Social media and messaging platforms should maintain accessible mechanisms for reporting suspected trafficking-related recruitment and should conduct risk-based detection of advertisements or accounts showing objectively suspicious indicators.

Where there is a sufficiently substantiated indication of trafficking-related recruitment, the platform should be required to preserve relevant electronic data, including account identifiers, available metadata, communication records within the legally authorized scope, and relevant transaction or advertising information. Removal or restriction of content should be conducted according to a legally defined notice-and-action procedure, while reporting to competent authorities should occur within a specified period based on the level of urgency. Platforms that intentionally facilitate trafficking activities, deliberately ignore lawful preservation or disclosure orders, or repeatedly fail to fulfill statutory due-diligence obligations may be subject to proportionate administrative or other legally prescribed sanctions. At the same time, platforms should not be required to determine criminal guilt independently; their role should be limited to risk management, lawful preservation, reporting, and cooperation based on due process of law.

Regulatory weaknesses are also evident in the National Criminal Code, through Law Number 1 of 2023, which currently has not provided comprehensive regulations regarding cyber trafficking and digital recruitment in human trafficking crimes. While the National

Criminal Code has accommodated developments in modern criminal law by recognizing information technology-based crimes, it has not yet established a specific legal framework for cyberspace-based human trafficking. Consequently, law enforcement officials still rely on conventional approaches in interpreting the elements of human trafficking crimes. Furthermore, there are no clear regulations regarding the accountability of digital corporations and electronic platforms that indirectly facilitate the recruitment of victims through their systems. While Article 46 of Law Number 21 of 2007 actually provides for corporate criminal liability in human trafficking crimes, this norm has not been extended to digital corporations or electronic platforms that profit economically from user traffic without adequately monitoring illegal recruitment content (Krisna, S. P., & Yudiantara, 2025). The regulatory vacuum has led to weak oversight of cyberspace and created legal uncertainty in determining the limits of digital platforms' responsibility for human trafficking activities occurring within their electronic systems.

The absence of a specific legal framework for preventive digital surveillance creates uncertainty regarding the limits of cyber policing in detecting human trafficking recruitment. Therefore, any future authority to conduct preventive digital surveillance should be expressly regulated by law and governed by the principles of legality, legitimate purpose, necessity, proportionality, data minimization, and accountability. General cyber patrols should primarily be limited to publicly accessible digital spaces and should not authorize unrestricted collection of private communications or personal data.

More intrusive measures, including targeted monitoring of non-public digital communications, covert digital infiltration, prolonged surveillance of identifiable persons, or access to protected account information, should require a higher evidentiary threshold and prior authorization from a legally designated judicial or independent authority, except in narrowly defined emergency circumstances where delay creates an immediate risk to the safety or freedom of a potential victim.

Every surveillance measure should be documented with its legal basis, purpose, scope, target where applicable, duration, categories of data collected, and grounds for continuation. Surveillance should be periodically reviewed, irrelevant data should be deleted or anonymized, and an independent oversight mechanism should have authority to audit the legality and proportionality of the use of surveillance powers. These safeguards are necessary to ensure that preventive cyber policing does not transform into unrestricted digital monitoring incompatible with privacy, personal-data protection, and due process of law.

Another significant weakness lies in the electronic evidence and cross-border tracking of digital human trafficking networks. Normatively, Article 5 of the ITE Law recognizes electronic information and electronic documents as valid legal evidence, while Article 44 of Law Number 21 of 2007 states that evidence in human trafficking crimes can take the form of electronic information and electronic documents. However, in practice, the electronic evidence process still faces numerous obstacles, such as metadata validity, digital account authentication, chain of custody of electronic evidence, and access to foreign servers. It is further complicated by the fact that most of the digital platforms used by

perpetrators are under foreign jurisdiction, preventing Indonesian law enforcement officials from directly accessing user data. As a result, the investigation process is often hampered by lengthy and bureaucratic mutual legal assistance mechanisms. Indonesia does have Law Number 1 of 2006 concerning Mutual Assistance in Criminal Matters and has ratified the United Nations Convention against Transnational Organized Crime through Law Number 5 of 2009. However, the implementation of cross-border cooperation in tracking digital-based human trafficking remains suboptimal due to weak technological integration, limited digital forensic capacity, and the absence of specific cooperation agreements with global digital platforms (Limadibrata, R. W., & Jamaludin, 2025). It has led many perpetrators to use overseas servers and anonymous accounts to evade law enforcement in Indonesia.

Legal reconstruction should therefore introduce a National Digital Evidence Standard applicable to investigations and prosecutions involving digital-based human trafficking. The standard should regulate the identification, acquisition, collection, preservation, examination, transfer, storage, and presentation of electronic evidence. Every item of electronic evidence should be accompanied by a documented chain of custody recording the source of the data, date and time of acquisition, responsible officer or institution, method of collection, subsequent transfers, forensic examination, and any technical processing performed.

To ensure forensic integrity, original electronic data should, where technically possible, be preserved, while forensic examination is conducted using verified copies. The standard should require integrity verification, preservation of relevant metadata, documentation of forensic tools and methods, and authentication procedures for digital accounts and communications. Where evidence is obtained from cloud infrastructure or foreign servers, the case file should additionally record the legal basis for access, the requesting and responding authorities, the method of transmission, and the continuity of preservation after the data enters the Indonesian criminal justice process.

These standards would complement, rather than replace, the recognition of electronic evidence under Article 5 of the ITE Law and Article 44 of Law Number 21 of 2007. Their purpose is to ensure that electronic evidence used in trafficking prosecutions satisfies requirements of authenticity, reliability, integrity, traceability, and procedural accountability.

It can be concluded that the Indonesian legal system is still lagging behind in responding to the transformation of digital-based human trafficking crimes. Existing regulations are still partial, sectoral, and have not yet established an integrated legal system capable of effectively anticipating the development of cyber-enabled trafficking. The lack of norms regarding digital platform accountability, cyberspace oversight, cyber patrols, digital surveillance, electronic evidence, and cross-border tracking demonstrates a legal gap between the development of criminal technology and national legal reforms. From the perspective of a state based on the rule of law, this situation contradicts the principles of legal certainty, legal protection, and effective law enforcement as guaranteed in Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia.

Problems of Law Enforcement by the Indonesian Police Regarding Digital Recruitment in Human Trafficking Crimes

The development of digital recruitment in human trafficking crimes has posed serious challenges to the Indonesian law enforcement system, particularly for the Indonesian National Police, the institution with primary authority in the investigation and prosecution of crimes. Recruitment methods through social media, instant messaging applications, and digital platforms create a far more complex crime pattern than conventional recruitment because perpetrators can operate anonymously, across regions, and across countries without having to make direct physical contact with the victim. In practice, many human trafficking cases begin through online job advertisements, illegal overseas job offers, and recruitment through closed social media groups that are difficult for law enforcement to monitor. Although Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police mandates the Indonesian National Police (Polri) to maintain public order and security, enforce the law, and provide protection to the public, the development of digital crime demonstrates that conventional law enforcement capacity is not yet fully capable of addressing cyber-based human trafficking patterns. Empirically, various human trafficking cases involving the illegal sending of migrant workers abroad demonstrate that perpetrators often utilize fake social media accounts and online communications to evade authorities' surveillance. This situation makes the process of identifying perpetrators much more difficult than with traditional recruitment patterns that have physical traces and direct relationships with victims. As a result, law enforcement is often delayed after victims have been moved or exploited outside of Indonesian jurisdiction.

One of the main problems facing the Indonesian Police is the limitations of the cyber policing system in dealing with digital-based human trafficking. Cyber policing essentially requires the capabilities of cyberspace surveillance, digital activity monitoring, cyber patrols, and digital intelligence that are integrated technologically and institutionally. However, empirically, these capabilities are still not evenly distributed throughout Indonesia due to limited technological infrastructure, budget, and human resources with digital competencies. In fact, Article 14, paragraph (1), letter g of the Police Law gives the National Police the authority to conduct inquiries and investigations into all criminal acts in accordance with the criminal procedure law and other laws and regulations. However, in practice, many regional police units do not yet have adequate cyber units to detect human trafficking recruitment activities through digital platforms. The limitation is exacerbated by the rapid development of encrypted communication technology used by perpetrators through Telegram, WhatsApp, or virtual private network applications, which complicates digital tracking. Empirically, police officers act more repressively after receiving a victim's report rather than conducting early detection and preventive supervision of illegal recruitment activities in cyberspace. It shows that the national cyber policing system is still reactive and has not yet developed into predictive policing based on information technology and digital data analysis.

The next problem relates to the lack of digital forensic capabilities and the difficulty of identifying anonymous accounts in the investigation of digital-based human trafficking

crimes. In many cases, perpetrators use fake identities, virtual numbers, anonymous social media accounts, and overseas servers to conceal their identities. This situation makes it difficult for investigators to conduct digital tracing and legally link digital accounts to the perpetrator's identity. Despite Article 5 paragraphs (1) and (2) of Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, which recognizes electronic information and electronic documents as valid legal evidence. Furthermore, Article 44 of Law Number 21 of 2007 concerning the Eradication of Human Trafficking Crimes also recognizes electronic evidence in the process of proving human trafficking cases. However, in empirical practice, the digital forensic capabilities of law enforcement officers still face various limitations, particularly in the processes of data extraction, account authentication, metadata analysis, recovery of deleted electronic data, and maintaining the chain of custody of digital evidence. Many digital-based human trafficking cases encounter evidentiary challenges because electronic evidence cannot be verified optimally or is deemed not to meet evidentiary standards in court. It indicates that the normative recognition of electronic evidence has not been accompanied by the technical and institutional readiness of law enforcement officials to manage digital evidence in a professional and modern manner.

Another very significant obstacle is the issue of transnational jurisdiction and limited access to electronic data from global digital platforms. The nature of digital-based human trafficking allows perpetrators, victims, communication servers, and financial transactions to be located in different countries, thus requiring complex cross-border cooperation. In practice, National Police investigators often face difficulties obtaining user data from digital platform companies such as Meta, Telegram, or other foreign applications because such data is under the jurisdiction of other countries and subject to the privacy policies of global companies. This is despite the fact that Article 43, paragraph (3) of the ITE Law authorizes investigators to request information from electronic system operators for law enforcement purposes. However, the implementation of this provision is often ineffective against foreign platforms that are not directly subject to Indonesian national jurisdiction. Empirically, the process of requesting electronic data often requires a lengthy mutual legal assistance mechanism, while perpetrators can quickly delete accounts, change digital identities, or move operations to other platforms. Indonesia does have Law No. 1 of 2006 concerning Mutual Assistance in Criminal Matters and ratified the United Nations Convention against Transnational Organized Crime through Law No. 5 of 2009. However, international cooperation in the context of cyber trafficking still faces technical and diplomatic obstacles, as well as differences in legal systems between countries. As a result, many digital human trafficking networks are difficult to comprehensively dismantle due to limited access to electronic data across jurisdictions.

Law enforcement challenges are also evident in the weak inter-agency coordination in handling digital recruitment-based human trafficking. Handling human trafficking essentially involves numerous institutions, such as the Indonesian National Police, the Ministry of Communication and Information Technology, the National Cyber and Crypto Agency, the Indonesian Migrant Workers Protection Agency, Immigration, the Prosecutor's

Office, and international institutions. However, in empirical practice, this coordination is often sectoral and not integrated into a single national digital surveillance system. The Ministry of Communication and Informatics, for example, has the authority to block access to negative content based on Article 40 paragraph (2b) of the ITE Law, but the information exchange mechanism with the police often does not occur quickly and systematically. On the other hand, the National Cyber and Crypto Agency has national cybersecurity authority, but does not yet have optimal operational integration with the digital-based human trafficking investigation process. Due to this weak coordination, monitoring of illegal recruitment accounts on social media is often ineffective, and case handling is slow. In fact, in several empirical cases, reported recruiter accounts remain active for long periods due to the lack of an integrated cyber patrol system between digital space monitoring agencies and law enforcement officials. The condition reveals that the problem of law enforcement lies not only in regulatory weaknesses but also in the lack of integration of institutional systems in dealing with the development of cyber-enabled trafficking.

In addition to these various obstacles, there is a significant mismatch between the development of digital crime methods and the capacity of the national law enforcement system. Human traffickers have now leveraged sophisticated digital technology through artificial intelligence, automated accounts, encrypted communications, cryptocurrency transactions, and even digital identity forgery to evade legal investigation. Meanwhile, the national law enforcement system still operates using a slow and bureaucratic, conventional procedural approach. Despite Article 28D paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees the public's right to legal certainty and fair legal protection. From the perspective of a state governed by the rule of law, the state should be able to implement a law enforcement system that adapts to technological developments and provides effective protection for the public from the threat of digital-based human trafficking. However, empirically, there remains a significant gap between the development of criminal technology and the ability of law enforcement officials to conduct digital surveillance, investigations, inquiries, and evidence collection. This situation has resulted in suboptimal law enforcement against digital recruitment in human trafficking crimes and the potential to expand the scope for impunity for organized cybercriminals.

Reconstruction and Reform of the Law Enforcement of Human Trafficking Crimes through Technology-Based Digital Recruitment Surveillance by the Indonesian National Police

Reconstruction and reform of the law enforcement of human trafficking crimes through technology-based digital recruitment surveillance must be directed toward establishing a modern, adaptive, and accountable cyber policing system. The Indonesian National Police may utilize artificial intelligence and machine-learning technology as a decision-support mechanism for detecting patterns associated with potentially unlawful recruitment. However, AI-assisted monitoring must not be treated as an autonomous system for determining that an account, advertisement, or individual is involved in human trafficking.

The identification of suspicious recruitment should be based on objective and legally relevant indicators, such as the use of unverifiable recruiter identities, repeated publication of employment offers inconsistent with verified business information, recruitment directed toward vulnerable persons through demonstrably deceptive representations, repeated use of previously identified trafficking infrastructure, abnormal migration of accounts following enforcement action, or combinations of digital indicators supported by verified contextual information. No single keyword, account characteristic, nationality, age group, or social characteristic should independently determine that an activity constitutes suspected trafficking.

To prevent false positives, algorithmic bias, and wrongful account classification, the system should be subject to periodic accuracy testing, bias assessment, documentation of the categories of data used, and independent technical auditing. AI-generated alerts should only trigger further verification by authorized human officers. Any blocking, investigation, disclosure request, or other adverse legal consequence must be based on independently verified evidence and human review. A correction mechanism should also be available where an account or advertisement has been wrongly classified.

Legal reform must also be directed at strengthening regulations regarding the obligations and responsibilities of digital platforms in preventing human trafficking recruitment through their electronic systems. Currently, Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law does not specifically regulate the responsibilities of digital platforms for online human trafficking activities. Therefore, a reformulation of legal norms is needed that requires electronic system operators to actively monitor, report suspicious activity, and delete accounts suspected of human trafficking recruitment. Specifically, the government needs to establish a specific Government Regulation concerning Digital Platform Supervision for the Prevention of Human Trafficking Crimes, which regulates the obligations of social media platforms, instant messaging applications, and online job sites to develop automated detection systems for illegal recruitment content. The regulation should also stipulate administrative and criminal sanctions for platforms that intentionally or negligently allow human trafficking activities to occur within their systems.

The establishment of a National Digital Trafficking Monitoring Center should be based on an integrated but clearly differentiated institutional model. Because human trafficking constitutes a criminal offense, the Indonesian National Police should exercise primary operational authority in relation to criminal intelligence, investigation, cyber patrols, and law-enforcement action. However, the Monitoring Center should not absorb or replace the statutory authority of other institutions.

The Ministry responsible for communication and digital affairs should retain authority concerning electronic-system governance, lawful coordination with platforms, and administrative measures relating to digital content or electronic systems. BSSN should provide cybersecurity and technical security support within its statutory competence. BP2MI should contribute data and risk indicators relating to migrant-worker recruitment

and protection, while Immigration should retain authority concerning immigration information, travel patterns, and legally authorized border-related measures.

To prevent institutional overlap, the proposed regulatory framework should establish a single coordination protocol identifying the lead institution for each operational stage, the categories of information that may be shared, the authorized purpose of data processing, access levels, retention periods, and audit trails for every inter-agency data request. The Monitoring Center should therefore function as an integration and early-warning mechanism, while criminal investigative decisions remain under the authority of legally competent investigators and sectoral institutions retain their respective statutory mandates.

Optimizing law enforcement against digital-based human trafficking also requires strengthening electronic evidence and digital forensics systems in the investigation and trial process. Although Article 5 of the ITE Law recognizes electronic information and electronic documents as valid legal evidence, the implementation of digital evidence in human trafficking cases still faces various technical and procedural obstacles. Therefore, it is necessary to revise the Criminal Procedure Code and establish specific regulations regarding digital evidence standards in cybercrime and digital-based human trafficking. Specifically, the Indonesian National Police (Polri) needs to establish a National Digital Forensic Laboratory integrated with all regional police forces and equipped with technology for metadata analysis, electronic data recovery, blockchain tracing, and an artificial intelligence forensic system. Furthermore, it is necessary to increase the capacity of investigators through regular specialized education in cyber investigation and digital forensic investigation. The government also needs to establish national standards for the chain of custody of electronic evidence to ensure the validity of digital evidence in court. Internationally, countries such as Singapore and the United States have developed integrated digital forensic systems that enable investigators to conduct rapid analysis of cross-platform electronic communications. The model can be adapted within the Indonesian legal system to strengthen the effectiveness of evidence against digital-based human trafficking perpetrators who use virtual identities and encrypted communications.

Subsequent legal reforms should focus on strengthening cross-border cooperation in tracking and prosecuting digital-based human trafficking networks. The transnational nature of cyber-enabled human trafficking means that law enforcement cannot be carried out partially within national jurisdictions alone. Therefore, Indonesia needs to strengthen the implementation of Law Number 1 of 2006 concerning Mutual Assistance in Criminal Matters and expand international cooperation in the areas of digital tracing, electronic data exchange, and cyber intelligence sharing. Specifically, the government needs to establish an ASEAN Cyber Trafficking Task Force to serve as a regional coordination center for addressing digital-based human trafficking in Southeast Asia. Likewise, Indonesia needs to establish direct cooperation agreements with global digital platform companies such as Meta, Telegram, Google, and TikTok to accelerate access to electronic data for law enforcement purposes. Internationally, the European Union has implemented the Digital Services Act, which requires digital platforms to actively cooperate with law enforcement

officials in addressing illegal content and human exploitation in cyberspace. The model can serve as a reference for Indonesia in developing more progressive regulations regarding digital platform obligations to support the eradication of technology-based human trafficking. With strong cross-border cooperation, the process of tracking perpetrators, freezing digital assets, and prosecuting international human trafficking networks can be carried out more effectively and expeditiously.

In addition to strengthening regulations and institutions, legal reforms must also be directed at establishing an early detection system and preventive protection for vulnerable communities becoming victims of digital recruitment. Currently, the law enforcement system tends to operate after victims experience exploitation, resulting in reactive legal protection. Therefore, a preventive cyber policing model is needed that places digital monitoring and education as an integral part of human trafficking eradication policies. Specifically, the government, in collaboration with the Indonesian National Police (Polri), needs to develop an artificial intelligence-based Early Warning System capable of automatically detecting illegal recruitment patterns through social media and digital applications. Furthermore, data integration between the police, the Population and Civil Registration Agency (Disdukcapil), the BP2MI (Indonesian Agency for the Protection of Migrant Workers), the Immigration Office (Immigration), and the Ministry of Communication and Information Technology (Kominfo) is needed to identify potential victims of human trafficking from the online recruitment stage. The government should also require digital job platforms to verify the identity and legality of recruiting companies before publishing advertisements to the public. In the education sector, the Indonesian National Police, along with the Ministry of Education and Communication and Information Technology, need to implement a national digital literacy program addressing the dangers of social media-based human trafficking, which targets schoolchildren, migrant workers, and rural communities. This preventative approach is crucial to reducing the public's vulnerability to increasingly widespread and systematic digital recruitment methods.

Reconstruction and reform of the law on human trafficking enforcement based on digital recruitment must be directed at establishing a legal system that is responsive to technological developments, based on human rights protection, and capable of ensuring legal certainty in cyberspace. The Indonesian legal system needs to move from a conventional approach to an integrated cyber law enforcement system that combines regulatory strengthening, digital technology, cross-border cooperation, cyber patrols, and preventive community protection. This reform must be realized through a revision of the Human Trafficking Law, an update of the Electronic Information and Transactions Law (ITE Law), strengthening the cyber policing authority of the Indonesian National Police (Polri), the establishment of regulations on digital platform responsibility, and the development of a national digital forensic infrastructure. Specifically, the government needs to include digital human trafficking as a national priority crime category in Indonesia's cybersecurity policy and establish a national anti-cyber trafficking command center that operates in an integrated 24-hour manner. Furthermore, the establishment of a specialized cyber court competent to handle cyber trafficking cases and electronic evidence professionally is

necessary. With this comprehensive and technology-based legal reconstruction, the Indonesian law enforcement system is expected to be able to address the development of digital human trafficking effectively, preventively, and sustainably, so that protection for the public from the threat of human exploitation in cyberspace can be optimally realized.

The proposed legal reconstruction should be implemented through an integrated regulatory model consisting of seven principal components. First, Law Number 21 of 2007 should be amended to expressly recognize digital recruitment as the use of electronic systems, digital platforms, or information technologies to recruit or facilitate the recruitment of persons through unlawful means for the purpose of exploitation. The amendment should clarify that the use of digital technology constitutes a method of committing or facilitating trafficking without altering the essential substantive elements of the offense.

Second, the Electronic Information and Transactions Law and related regulations should establish proportionate platform responsibilities concerning recruiter verification, risk-based detection of suspicious recruitment, accessible reporting mechanisms, preservation of relevant electronic evidence, lawful cooperation with competent authorities, and sanctions for intentional facilitation or serious non-compliance. Third, amendments to the Police Law or implementing legislation should establish the authority and limits of cyber patrols, AI-assisted analysis, and preventive digital surveillance based on legality, necessity, proportionality, human oversight, authorization requirements, and independent accountability.

Fourth, a National Digital Evidence Standard should regulate authentication, metadata preservation, forensic copying, integrity verification, chain of custody, cloud evidence, foreign-server evidence, and expert examination. Fifth, the National Digital Trafficking Monitoring Center should operate through a clear division of responsibilities between Polri as the primary law-enforcement authority and other participating institutions according to their respective statutory mandates.

Sixth, cross-border digital cooperation should establish procedures for emergency preservation requests, mutual legal assistance, authenticated digital-evidence exchange, account identification, asset tracing, and expedited cooperation in cases involving an immediate threat to victims. Finally, all digital monitoring, AI-assisted analysis, platform cooperation, and data exchange should be subject to safeguards concerning privacy, personal-data protection, data minimization, limited retention, access control, independent oversight, and effective remedies against unlawful or disproportionate action.

Through this structured regulatory model, legal reform would not merely expand cyber-policing powers but would establish a balanced system capable of addressing digital recruitment for human trafficking while maintaining constitutional rights, privacy, and due process of law.

Conclusion

The development of digital technology has shifted the pattern of human trafficking crimes from conventional recruitment systems to anonymous, rapid, organized, and transnational recruitment based on social media and online platforms. This situation

indicates that human trafficking can no longer be viewed solely as a conventional crime, but has evolved into a cyber-enabled transnational organized crime that exploits weaknesses in digital surveillance and low public digital literacy. However, the Indonesian legal system still faces various normative weaknesses and law enforcement problems in addressing digital recruitment in human trafficking crimes. Law Number 21 of 2007 on the Eradication of Human Trafficking, the Law on Information and Electronic Transactions, and other regulations on electronic systems still do not clearly regulate the responsibility of digital platforms, cyber patrol mechanisms, digital surveillance, or systems for monitoring illegal recruitment carried out through technology. At the same time, the Indonesian National Police continues to face several challenges, including limited cyber policing and digital forensic capabilities, difficulties in identifying anonymous accounts, weak coordination between agencies, and jurisdictional barriers in accessing electronic data from foreign digital platforms. As a result, law enforcement against digital human trafficking has not been optimal and tends to be reactive after victims experience exploitation. Therefore, legal reconstruction and reform are needed that are not only oriented toward repressive aspects, but also preventative and adaptive to technological developments. It includes strengthening cyber policing, integrating cyber patrol operations, regulating the obligations of digital platforms, improving the use of electronic evidence, and enhancing international cooperation to combat digital-based human trafficking.

The government and the House of Representatives of the Republic of Indonesia need to immediately reformulate and harmonize regulations related to digital-based human trafficking by revising Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, the Electronic Information and Transactions Law, and regulations related to the implementation of electronic systems to be more adaptive to technological developments and transnational cybercrime. These reforms should be directed at stricter regulations regarding digital platform accountability, mandatory monitoring of illegal recruitment content, due process-based digital surveillance, a national cyber patrol mechanism, and a modern and integrated electronic evidence system. Furthermore, the Indonesian National Police (Polri) needs to develop a cyber policing system based on artificial intelligence, digital intelligence, and predictive cyber patrol, supported by increased human resource capacity for digital forensics and the development of a national digital forensics laboratory integrated down to the regional level. The government also needs to establish a national digital-based anti-human trafficking monitoring center involving the Indonesian National Police (Polri), the Ministry of Communication and Information Technology (Kominfo), the National Civil Service Agency (BSSN), the Immigration Office (Immigration), the Indonesian Migrant Workers Association (BP2MI), and international institutions to strengthen coordination and early detection of illegal recruitment in cyberspace. At the international level, Indonesia needs to expand cross-border cooperation and establish special agreements with global digital platform companies to accelerate electronic data access for law enforcement purposes. With legal reforms and the strengthening of a comprehensive digital monitoring system, it is hoped that law enforcement against digital recruitment in human trafficking crimes will be more effective,

preventative, and provide optimal legal protection for the public in the era of digital transformation.

References

- Alhakim, A. (2024). Penanggulangan Tindak Pidana Perdagangan Orang Melalui Media Sosial Dalam Perspektif Kriminologi. *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, 471–490.
- Danuri, M. (2019). Perkembangan dan Transformasi Teknologi Digital. *Jurnal Ilmiah Infokam*.
- Elenta, R. S., & Waruwu, N. E. (2026). Perlindungan Hukum Terhadap Korban Tindak Pidana Perdagangan Orang dan Modus Rekrutmen Kerja Luar Negeri Melalui Media Sosial. *Jurnal Ilmiah Multidisiplin Ilmu*, 216–221.
- Frahma, E. A. (2025). Analisis Yuridis Peran Iom Dalam Mendukung Upaya Indonesia Dan Kamboja Dalam Penanggulangan Tindak Pidana Perdagangan Orang. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 9232–9241.
- Irawan, P. S., & Lestari, D. P. (2026). Kejahatan Transnasional Terorganisasi di Era Digital: Analisis Tren Kejahatan Siber dan Perdagangan Manusia Tahun 2025-2026. *Jurnal Pendidikan Masyarakat Indonesia Harapan*.
- Krisna, S. P., & Yudiantara, I. G. (2025). Pengaruh Teknologi Digital Dalam Modus Perdagangan Orang: Analisis Pidana Terhadap Kasus Online Scamming di Myanmar. *Kertha Desa: Journal Ilmu Hukum*, 1129–1146.
- Kusuma, K. M., Assa, N. J., Mutasya, N., & Wulandari, J. (2025). Analisis Tindak Pidana Perdagangan Orang (TPPO) WNI di Kamboja: Kronologi dan Penanganan Hukum. *Causa: Jurnal Hukum Dan Kewarganegaraan*, 71–80.
- Limadibrata, R. W., & Jamaludin, A. (2025). Menyoroti Kebijakan Hukum Pidana Terhadap Kasus Perdagangan Perempuan di Indonesia dengan Modus Rekrutmen Melalui Media Sosial. *Jurnal Hukum Lex Generalis*.
- Mulyati, D., Dewi, E., & Tamza, F. B. (2026). Human Trafficking di Dunia Maya: Perspektif Hukum Pidana Indonesia dalam Menjerat Rekrutmen Online dan Eksploitasi Digital. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 2082–2091.
- Mustofa, A. A., Soekorini, N., & Aranggraeni, R. (2026). Analisis Yuridis terhadap Pelaku Tindak Pidana Perdagangan Orang (Studi Kasus Putusan Nomor: 1172/Pid. Sus/2024/Pn. Sby). *RIGGS: Journal of Artificial Intelligence and Digital Business*, 6693–6700.
- Nugroho, O. C. (2018). Tanggung Jawab Negara dalam Penanganan Tindak Pidana Perdagangan Orang. *Jurnal Penelitian Hukum De Jure*.
- Prameswari, V. P. (2025). Pertanggungjawaban Hukum Pidana Terhadap Pelaku Tindak Pidana Perdagangan Orang Melalui Media Elektronik Berdasarkan Undang-Undang No 21 Tahun 2007 Tentang Pemberantasan Tindak Pidana Perdagangan Orang. *Lex Progressium: Jurnal Kajian Hukum Dan Perkembangan Hukum*.
- Putra, R. R., Pratama, D. I., Kaloko, I. F., Niyobuhungiro, J., & Febriyanti, N. (2026). Analisis Penegakan Hukum Terhadap Tindak Pidana Perdagangan Orang di Kamboja dalam Perspektif Hukum Pidana Nasional. *JURNAL USM LAW REVIEW*, 771–790.

-
- Salsa, S. N. (2021). Mutual Legal assistant Dalam Penyidikan Tindak Pidana perdagangan manusia melalui media sosial Sebagai Kejahatan terorganisasi transnasional. *Jurnal Yuridis*.
- Saputra, F. S., & Lawoleba, K. K. (2024). Modus Operandi Online Scam pada Tindak Pidana Perdagangan Orang dalam Perspektif Kejahatan Dimensi Baru. *National Conference on Law Studies (NCOLS)*.
- Wiguna, Z. P., Arifin, M. Y., & Muhdar, M. Z. (2026). Efektivitas Perlindungan Hukum terhadap Perdagangan Orang Online di BP2MI Sulsel. *LEGAL DIALOGICA*.
- Wulandari, D. A., & Fitriyana, L. (2026). Tindak Pidana Perdagangan Orang pada Kelompok Rentan di Aplikasi Online. *Wijaya Putra Law Review*, 183–206.