

A Model for Preventing Indonesian Migrant Workers from Human Trafficking Under the Guise of Digital Job Placement in Cambodia Based on Human Rights Protection

Komang Saptapramana*, Zulkarnein Koto, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; komangsaptapramana@yahoo.com

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

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

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6319>

*Correspondence: Komang

Saptapramana

Email:

komangsaptapramana@yahoo.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 given rise to a transformation in the crime of human trafficking against Indonesian migrant workers through the mode of illegal digital job placement to Cambodia, integrated with cybercrime, scam centers, and online gambling. This study aims to analyze the crime of human trafficking under the guise of digital job placement against Indonesian migrant workers in Cambodia, examine the problems and weaknesses of legal policies in its prevention, and formulate the reconstruction and legal reform of the prevention model based on human rights protection. This study uses a normative juridical method with a legislative approach and a conceptual approach through an analysis of Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers, the Law on Information and Electronic Transactions, and international legal instruments related to human trafficking and human rights. The results of the study indicate that the national legal system still faces various weaknesses in the form of regulatory disharmony, weak supervision of digital recruitment, suboptimal cross-agency coordination, minimal cyber surveillance, and the absence of a digital technology-based early warning system for trafficking. Therefore, legal reconstruction and reform are needed through strengthened cyber patrols, AI-based recruitment monitoring, cross-agency data integration, digital platform oversight, increased public digital literacy, and strengthened bilateral cooperation between Indonesia and Cambodia to create an adaptive, responsive, and human rights-based protection system for*

Indonesian migrant workers against the threat of modern digital human trafficking.

Keywords: *human trafficking; Indonesian migrant workers; digital job placement*

Introduction

The development of globalization and the transformation of digital technology have significantly changed the patterns of social, economic, and employment relations, including the mechanisms for recruiting migrant workers across borders. (Danuri, 2019) The advancement of social media and digital platforms such as Telegram, Facebook, TikTok, WhatsApp, and various online job sites has created new spaces that facilitate labor mobility

(Sidik, I. A., Suherman, 2024), but at the same time has also given rise to a new form of transnational crime in the form of digital-based human trafficking. The mode of human trafficking, which was previously carried out conventionally through direct recruitment, has now evolved into digital exploitation through fake job advertisements offering positions in customer service, cryptocurrency administration, digital marketing operators, and information technology jobs, with the lure of high salaries abroad, particularly in Cambodia. In practice, victims are then forced to work in scam centers, illegal online gambling, or organized cybercrime activities across borders (Saputra, F. S., & Lawoleba, 2024). This phenomenon shows that the crime of human trafficking has evolved into a technology-based transnational organized crime that moves faster than the development of national legal regulations.

From the perspective of Ulrich Beck's risk society theory, technological modernization has given rise to new, abstract global risks that are difficult to control with conventional legal instruments. Furthermore, cybercriminology theory explains that the development of cyberspace has created new crime patterns that exploit digital anonymity to exploit victims across borders, while Roscoe Pound's law as a tool of social engineering theory emphasizes that the law must adapt to social change and technological developments to protect society from modern forms of crime. (Sundari, 2024) In national law, Article 28D paragraph (1) of the 1945 Constitution affirms the guarantee of legal protection and certainty for every citizen, while Article 28G paragraph (1) of the 1945 Constitution provides the right to self-protection, a sense of security, and protection from the threat of fear. However, the development of digital-based human trafficking crimes demonstrates that national law still faces limitations in addressing the complexity of modern human trafficking, which utilizes information technology as a primary instrument of human exploitation.

The emergence of cases involving Indonesian citizens who travel to Cambodia and subsequently become involved in exploitation within scam centers or other forms of transnational digital crime has raised significant legal concerns regarding the protection of prospective Indonesian migrant workers. Government information, documented case reports, and academic studies have identified patterns in which individuals are attracted through overseas employment offers and subsequently experience confinement, intimidation, passport confiscation, threats, and forced involvement in digital fraud activities (Hidayat, R., Syahnan, M., & Rokan, 2026). These sources provide an important contextual basis for examining how digital recruitment may function as an initial stage in a broader trafficking process, although this study does not independently measure the national scale or statistical prevalence of such recruitment.

Normatively, the state has a constitutional obligation to protect citizens as stipulated in the fourth paragraph of the Preamble to the 1945 Constitution and Article 27 paragraph (2) of the 1945 Constitution, which guarantees the right of citizens to obtain decent work and a living. In addition, Article 4 of Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers affirms the right of migrant workers to receive protection before, during, and after employment. However, the existing legal framework does not yet provide a sufficiently specific preventive mechanism for identifying and responding to recruitment activities conducted through social media, messaging applications, and other

digital platforms. Therefore, the issue examined in this study is primarily a normative gap concerning whether existing legal instruments are sufficiently capable of preventing digitally facilitated recruitment that may develop into trafficking and transnational exploitation (Nugroho, 2018).

The weakness of Indonesia's migrant worker placement prevention system is a fundamental issue that demonstrates the suboptimal national legal policy in addressing digital human trafficking. Supervision of online recruitment remains very weak due to the lack of an integrated cyber surveillance system capable of detecting illegal recruitment patterns through social media and digital platforms. Furthermore, cross-agency coordination between the Ministry of Manpower, the Indonesian Migrant Workers Protection Agency (BP2MI), the police, immigration, the Ministry of Communication and Digital, and the Ministry of Foreign Affairs remains sectoral and not effectively integrated. (Hidayat, 2021) This situation is exacerbated by the public's lack of digital literacy, a weak early warning system for trafficking, and the lack of a unified database on recruitment agencies and worker migration patterns to countries prone to digital exploitation, such as Cambodia. Consequently, the state tends to use a repressive approach through criminal prosecution after victims are identified, rather than developing a digital technology-based preventive system. This is despite Article 69 of Law Number 18 of 2017, which affirms that the central and regional governments have the responsibility to protect migrant workers through monitoring and preventing non-procedural placement. Furthermore, Article 70 stipulates the government's obligation to provide education and training for prospective Indonesian migrant workers (Indah Rohmawati, Amir Junaidi, 2024). However, these provisions have not been optimally implemented in the context of modern digital crime developments. From the perspective of Lawrence Friedman's legal system theory, legal effectiveness is influenced by legal substance, legal structure, and legal culture. Weak institutional coordination and the lack of adaptation of society's digital legal culture indicate that the national legal system is still unable to respond to the transformation of information technology-based human trafficking (Sari, F. R., & Adityo, 2024).

The problematic legal regulations in preventing human trafficking against Indonesian migrant workers also indicate disharmony and a lack of legal norms. Law Number 21 of 2007 concerning Human Trafficking in Persons (TPPO) does not specifically regulate cross-border digital labor recruitment or the accountability of digital platforms used as a means of illegal recruitment. Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law does not comprehensively regulate the obligations of digital platforms to prevent the dissemination of fake job vacancies that could become human trafficking tool. Furthermore, the Personal Data Protection Law does not specifically protect against the misuse of victim data in digital trafficking recruitment (Shaliha, R., 2023). This condition creates a legal vacuum in combating employment trafficking scams that exploit cross-jurisdictional cyberspace. Overlapping authority between institutions also weakens the effectiveness of oversight and law enforcement. Gustav Radbruch's theory of legal certainty saw the law must provide certainty, justice, and benefit in a balanced manner. However, unclear regulation of digital recruitment oversight generates legal uncertainty and undermines the protection of migrant workers. In this regard, Philipus M. Hadjon's theory of legal protection underscores the

state's obligation to ensure both preventive and repressive protection of citizens' rights. However, in reality, preventive protection for Indonesian migrant workers remains very limited because positive law has not yet adapted to the development of digital technology-based trafficking (Ismail, M. M., Ismail, Y., & Humiati, 2025).

Conventional approaches used to prevent human trafficking have also proven ineffective in the face of the complexities of modern digital human trafficking. Administrative action and raids on illegal agents are unable to reach online recruitment networks that operate anonymously through social media and encrypted communication apps. Manual surveillance systems also lag behind advances in digital technology, which allows syndicates to operate across borders quickly. Modern human trafficking crimes are even integrated with cybercrime, online gambling, money laundering, and international digital fraud involving organized transnational networks (Fikri, 2022). This situation indicates that the state is still using traditional approaches to this highly complex form of modern digital crime. This is despite Article 71 of Law Number 18 of 2017, which authorizes the government to comprehensively supervise the placement and protection of Indonesian migrant workers. Similarly, Article 13 of the Human Trafficking Law emphasizes the importance of international cooperation in preventing human trafficking. However, the implementation of cross-border cooperation and cybersurveillance remains suboptimal, particularly in detecting digital platform-based migrant worker recruitment (Istiqomah, I., Tarmudi, T., Yusuf, H., Dewi, R., & Umboh, 2023). Therefore, a new legal paradigm is needed that positions digital technology as a primary instrument for preventing human trafficking, not merely an administrative tool. Updating preventive legal policies is urgently needed to enable the state to adapt to the transformation of cyber-based human trafficking crimes.

The urgency of establishing a prevention model based on human rights protection is crucial because Indonesian migrant workers are essentially legal subjects and human rights subjects who must be protected by the state. Article 28I paragraph (4) of the 1945 Constitution affirms that the protection, promotion, enforcement, and fulfillment of human rights are the responsibility of the state, particularly the government. Furthermore, Indonesia has ratified the United Nations Convention against Transnational Organized Crime and the Palermo Protocol through Law Number 14 of 2009, thus giving the state an international obligation to prevent and eradicate human trafficking, particularly of women and children. The principle of due diligence in international human rights law also emphasizes that states are obligated to take preventive measures to prevent human rights violations committed by non-state actors, including digital human trafficking syndicates. Thus, a security approach alone is insufficient to resolve the problem of human trafficking against Indonesian migrant workers in Cambodia. A prevention model is needed that places human rights protection as a primary foundation through strengthened cyber patrols, cross-agency data integration, digital platform monitoring, the establishment of an early warning system for trafficking, the use of artificial intelligence to detect illegal recruitment patterns, and strengthening bilateral cooperation between Indonesia and Cambodia in protecting migrant workers. This legal reconstruction is crucial for creating a preventive protection system that adapts to developments in digital technology while providing legal certainty

and human rights protection for Indonesian migrant workers from the threat of modern digital-based human trafficking.

Methodology

This study employs a normative juridical research method with a statutory approach and a conceptual approach. The statutory approach is carried out by examining various laws and regulations related to the prevention of human trafficking crimes against Indonesian migrant workers, including the 1945 Constitution of the Republic of Indonesia, Law Number 21 of 2007 concerning the Eradication of Criminal Acts of Human Trafficking, Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers, Law Number 1 of 2024 concerning Electronic Information and Transactions, the Criminal Code, immigration regulations, employment, personal data protection, and various international legal instruments such as the Palermo Protocol and the United Nations Convention against Transnational Organized Crime. This approach is used to analyze the synchronization, harmonization, and effectiveness of legal norms in preventing human trafficking practices under the guise of digital job placement in Cambodia. Meanwhile, a conceptual approach examines the doctrines, theories, and views of legal experts related to human rights protection, cybercriminology, migrant worker protection, and legal reform theories as a basis for formulating a prevention model that is adaptive to the development of transnational digital crime. The legal materials used consist of primary, secondary, and tertiary legal materials that are analyzed prescriptively through legal interpretation, legal argumentation, and legal construction techniques to produce a legal reform formulation that provides legal certainty, justice, and human rights protection for Indonesian migrant workers from the threat of digital-based human trafficking crimes.

Result and Discussion

Legal Analysis of Human Trafficking Crimes Under the Guise of Digital Job Placement for Indonesian Migrant Workers in Cambodia

The development of digital technology has transformed the pattern of human trafficking from conventional forms to digital-based human trafficking, utilizing social media and online platforms as the primary means of victim recruitment. This transformation demonstrates that human trafficking is no longer perpetrated through direct physical violence, but rather through information manipulation, job identity theft, and digital technology-based economic exploitation. In practice, perpetrators utilize Facebook, Telegram, TikTok, WhatsApp, Instagram, and various online job sites to offer high-paying jobs abroad, particularly in Cambodia, in positions such as customer service, cryptocurrency administrators, digital marketers, online game operators, and information technology operators. However, in reality, victims are forced to work in scam centers, international online fraud, illegal online gambling, and other cybercrime activities. This situation demonstrates that human trafficking has evolved into a transnational organized crime that exploits advances in information technology across borders. From the perspective of Ulrich Beck's risk society theory, globalization and technological modernization create new risks

that are cross-border and difficult to control with traditional legal instruments. Therefore, the development of modern digital crime demands an updated legal system that adapts to the transformation of human exploitation patterns in cyberspace. Constitutionally, Article 28G paragraph (1) of the 1945 Constitution guarantees the right of every person to personal protection, a sense of security, and protection from the threat of fear, while Article 28I paragraph (4) of the 1945 Constitution emphasizes that the protection and enforcement of human rights is the responsibility of the state. Therefore, the state has a legal obligation to prevent the development of digital-based human trafficking practices that threaten the human rights of Indonesian migrant workers (Nugroho, B., & Roesli, 2017).

The phenomenon of Indonesian migrant workers becoming victims of human trafficking in Cambodia demonstrates a structured and systematic pattern of digital exploitation. Many victims are recruited non-procedurally through fake job advertisements with promises of legal employment opportunities and high incomes, but then experience confinement, violence, threats, economic exploitation, and confiscation of travel documents upon arrival in their destination countries. In practice, victims are forced to work at scam centers that carry out international digital fraud targeting victims across borders. This mode fulfills the elements of the crime of human trafficking as regulated in Article 1, number 1 of Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, which states that human trafficking includes the recruitment, transportation, shelter, sending, transfer, or receipt of a person with the threat of violence, fraud, abuse of power, or debt bondage for exploitation. In addition, Article 2, paragraph (1) of the TPPO Law emphasizes that anyone who recruits or sends a person for exploitation can be punished. In the context of Indonesian migrant workers in Cambodia, the elements of fraud and exploitation are very dominant because victims are recruited through digital manipulation and forced to carry out illegal activities under the threat of violence. This condition shows that modern human trafficking is no longer only related to conventional sexual exploitation or forced labor, but has developed into digital exploitation based on cybercrime. From a cyber criminology perspective, cyberspace has become the main medium for modern crime because it provides anonymity, speed of communication, and ease of mobilization of victims across countries without adequate legal supervision (Shabrina'Ishmah, D., Aqimuddin, E. A., & Izadi, 2023).

The characteristics of modern human trafficking also demonstrate a close link between human trafficking, cybercrime, online gambling, money laundering, and transnational organized crime networks. Human trafficking syndicates exploit Indonesian migrant workers as instruments in international online scam operations that generate substantial economic profits through digital fraud. Thus, victims not only experience labor exploitation but are also forced to participate in transnational cybercrime activities. This situation demonstrates that human trafficking has expanded into forms of exploitation previously unanticipated in national legal regulations. Although Law Number 1 of 2024 concerning Electronic Information and Transactions prohibits the dissemination of false information, electronic manipulation, and the misuse of electronic systems, this regulation does not specifically address the link between digital platforms and human trafficking

crimes. Likewise, Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers also does not comprehensively regulate the oversight mechanism for social media-based and digital application-based labor recruitment. This is despite Article 5 of Law Number 18 of 2017, which affirms that every prospective Indonesian migrant worker has the right to obtain accurate information regarding the labor market, placement procedures, and working conditions abroad. Weak oversight of the digital space often leads to violations of these rights through the dissemination of false job information that misleads prospective migrant workers. Therefore, the development of digital-based human trafficking demonstrates a gap between technological developments and the ability of national law to provide preventive protection for Indonesian migrant workers.

From a legal perspective, the digital recruitment of Indonesian migrant workers to Cambodia is also related to violations of provisions for non-procedural placement of migrant workers. Article 81 of Law Number 18 of 2017 stipulates that everyone is prohibited from placing Indonesian migrant workers without official government permission. However, in practice, much recruitment is carried out by informal agents or individuals utilizing social media without state oversight. As a result, migrant workers depart via tourist routes, transit through third countries, or use documents that do not align with their actual work destination. This situation demonstrates the weak state oversight of digital-based migrant worker mobility. Furthermore, acts of passport confiscation, communication restrictions, threats of violence, and forced labor in scam centers also fulfill the elements of forced labor as prohibited by various international legal instruments, including the Palermo Protocol and the International Labour Organization Forced Labor Convention. Indonesia itself has ratified the United Nations Convention against Transnational Organized Crime through Law Number 5 of 2009 and the Palermo Protocol through Law Number 14 of 2009, thus having an international obligation to prevent, prosecute, and protect victims of transnational human trafficking. Therefore, the exploitation of Indonesian migrant workers in Cambodia is not only a violation of national law but also a violation of the country's binding international legal commitments (Ardanya, C., & Wulandari, 2025).

From the perspective of Roscoe Pound's theory of law as a tool of social engineering, the law should function as a social engineering instrument capable of adapting to societal changes and technological developments. However, the development of digital human trafficking demonstrates that national law still tends to be reactive and lags behind developments in modern crime modes. Legal regulations focus more on taking action after the crime has occurred rather than on developing a digital technology-based prevention system. This is despite the fact that Article 69 of Law Number 18 of 2017 assigns responsibility to the central and regional governments to protect migrant workers by preventing non-procedural placement. Furthermore, Article 13 of Law Number 21 of 2007 emphasizes the importance of national and international cooperation in preventing human trafficking. However, the implementation of this norm has not been optimal due to the lack of integrated digital surveillance systems, cyber patrols for online recruitment, or early detection mechanisms for illegal job advertisements on social media. This situation demonstrates that the legal substance, legal structure, and legal culture have not been

effective in addressing the digital-based transformation of human trafficking (Pangestu, 2025).

A legal analysis of human trafficking crimes under the guise of digital job placement for Indonesian migrant workers in Cambodia shows that advances in information technology have created increasingly complex and transnational forms of human exploitation. Modern human trafficking is no longer solely perpetrated through overt physical violence, but has evolved through digital manipulation, misuse of technology platforms, and cybercrime-based economic exploitation. National legal regulations have provided a normative basis through the 1945 Constitution, the Human Trafficking Law, the Law on the Protection of Indonesian Migrant Workers, and various international legal instruments. However, their implementation and legal substance have not kept pace with the development of transnational digital crime. Weak oversight of online recruitment, suboptimal inter-agency coordination, and the absence of a digital technology-based prevention system demonstrate the urgent need for comprehensive legal reform. Therefore, a reconstruction of legal policy is needed that focuses not only on criminal prosecution but also on developing a preventative protection model based on digital technology and human rights to prevent Indonesian migrant workers from becoming victims of human trafficking in the era of global digital transformation.

Problems and Weaknesses of Legal Policy in Preventing Human Trafficking of Indonesian Migrant Workers Under the Guise of Digital Job Placement in Cambodia

Human trafficking, previously conducted conventionally, may now involve social media, instant messaging applications, and digital job platforms as instruments for communication and recruitment. However, the use of a digital medium does not automatically transform every illegal overseas recruitment activity into human trafficking. Therefore, the concept of digital human trafficking recruitment should be understood as the use of electronic systems, digital platforms, social-media accounts, messaging applications, or other information technologies to recruit, transport, transfer, harbor, or otherwise facilitate the movement of a person through means or circumstances that satisfy the legal elements of trafficking and are connected to an intended or actual purpose of exploitation.

This concept must be distinguished from ordinary violations of migrant-worker placement regulations. A non-procedural placement may occur when a person works abroad without fulfilling applicable administrative or placement requirements, but such a violation does not necessarily involve deception, coercion, abuse of vulnerability, or exploitation. Likewise, online fraud may involve deception through digital communication but does not automatically constitute trafficking unless the fraudulent conduct is connected to the recruitment or movement of a person for exploitation. Digital human trafficking recruitment therefore occupies a distinct legal category: the digital medium constitutes the recruitment instrument, while the existence of trafficking depends on the presence of legally relevant acts, means, and purposes associated with exploitation under Law Number 21 of 2007.

Article 2 paragraph (1) of Law Number 21 of 2007 already provides a normative basis for addressing recruitment conducted for exploitative purposes. However, the provision

does not specifically regulate the characteristics of recruitment conducted through electronic systems, the preventive monitoring of digital recruitment content, or the corresponding responsibilities of electronic service providers. The legal reconstruction proposed in this study therefore does not seek to criminalize all informal overseas job advertisements but to establish clearer criteria for identifying digital recruitment that presents a legally recognizable connection to deception, abuse of vulnerability, organized recruitment networks, or a substantial risk of exploitation.

Weaknesses in legal policy are also evident in the suboptimal state oversight of online migrant worker recruitment. Article 69 of Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers stipulates that the central and regional governments are responsible for protecting Indonesian migrant workers through the supervision and prevention of non-procedural placements. However, implementation of this norm remains very weak, as oversight focuses more on conventional administrative channels than on digital recruitment activities. In practice, many informal agents and illegal recruiters utilize anonymous social media accounts to recruit prospective migrant workers without official permits. Some recruiters even use fictitious company identities and encrypted messaging apps to evade law enforcement scrutiny. This situation is exacerbated by the public's low digital literacy, which makes many prospective migrant workers easily fall prey to fake job postings offering high salaries without understanding the risks of exploitation and human trafficking. Besides, the government lacks a cybersurveillance and digital monitoring system capable of detecting illegal recruitment patterns in real time. As a result, the state tends to act after victims have been identified and cases have gone viral in the media, rather than taking preventative measures from the early stages of digital recruitment.

Another fundamental problem is the weak inter-agency coordination in handling digital-based human trafficking. Handling Indonesian migrant workers involves various institutions such as the Ministry of Manpower, the Indonesian Migrant Workers Protection Agency (BP2MI), the Indonesian National Police (Polri), the Directorate General of Immigration, the Ministry of Foreign Affairs, and the Ministry of Communication and Digital. However, coordination between these institutions remains sectoral and has not been effectively integrated. This is despite Article 40 of Law Number 21 of 2007 mandating cross-sectoral cooperation in the prevention and handling of human trafficking crimes. Empirically, this weak coordination has led to many non-procedural migrant workers escaping to Cambodia using tourist visas or transit routes through third countries without being detected initially.

Furthermore, the lack of data integration between agencies makes it difficult for the government to map the migration patterns of migrant workers at high risk of becoming victims of digital trafficking. In some cases, victims are only identified after being detained and seeking assistance through social media or Indonesian embassies abroad. This situation demonstrates the weakness of the early warning system for trafficking, which should be the primary instrument in preventing digital-based human trafficking. The government still uses an administrative and repressive approach that lags behind the rapid and organized developments of transnational cybercrime.

Regulatory disharmony is also a serious issue in protecting Indonesian migrant workers from the threat of digital human trafficking. Law Number 1 of 2024 concerning Electronic Information and Transactions does not specifically regulate the obligations of digital platforms to monitor illegal job recruitment content that could potentially become a means of human trafficking. This is even though digital platforms play a crucial role in the dissemination of fake job postings and the mobilization of victims across borders. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection also does not specifically regulate the protection of prospective migrant worker data, which is often misused by illegal recruiters for exploitation and human trafficking. This situation demonstrates a lack of norms regarding the accountability of digital platforms and the protection of users from the risks of information technology-based trafficking. From the perspective of Gustav Radbruch's theory of legal certainty, the law should provide certainty, justice, and benefit to society. However, the lack of clarity regarding the oversight of digital recruitment actually creates legal uncertainty and weakens protection for Indonesian migrant workers. Empirically, many illegal recruiter accounts remain active on social media despite public reports due to the lack of an effective legal mechanism to swiftly and coordinately prosecute and block digital trafficking recruitment networks.

From the perspective of Lawrence Friedman's legal system theory, legal effectiveness is influenced by three main elements: legal substance, legal structure, and legal culture. From a legal substance perspective, national regulations do not yet comprehensively regulate digital trafficking and the oversight of online platforms. From a legal structure perspective, law enforcement officials still face limited cyber investigation capabilities and minimal integration of cross-agency oversight. Meanwhile, from a legal culture perspective, low digital literacy makes prospective migrant workers susceptible to illegal social media-based recruitment practices. Furthermore, a societal culture that views working abroad as a quick way to earn a high income also increases vulnerability to digital manipulation by trafficking syndicates. From the perspective of Philipus M. Hadjon's legal protection theory, the state should provide citizens with a balance of preventive and repressive protection. However, empirical reality shows that state protection still places more emphasis on handling victims after exploitation occurs than on building a digital technology-based preventive protection system. As a result, Indonesian migrant workers remain vulnerable to exploitation and cross-border human trafficking.

The weaknesses in legal policies in preventing human trafficking of Indonesian migrant workers under the guise of digital job placement in Cambodia indicate a multidimensional problem, including regulatory weaknesses, weak digital oversight, suboptimal cross-agency coordination, and the national legal system's inability to adapt to the development of transnational cybercrime. Existing regulations still focus on conventional human trafficking patterns, thus failing to address the complexities of modern digital exploitation, which utilizes social media, online platforms, and electronic communication applications as instruments for victim recruitment. Empirically, the increasing number of Indonesian migrant workers falling victim to scam centers and human trafficking in Cambodia demonstrates that the state has not yet succeeded in establishing an

effective and responsive prevention system to the development of digital technology. Therefore, comprehensive legal reform is needed through regulatory harmonization, strengthening cyber surveillance, integrating data across agencies, establishing an early warning system for trafficking, and strengthening the accountability of digital platforms in preventing electronic-based illegal labor recruitment. These steps are crucial for achieving legal certainty, protecting human rights, and adapting a human trafficking prevention system to the transformation of modern digital crime.

Reconstruction and Legal Update of the Model for Preventing Indonesian Migrant Workers from Human Trafficking Under the Guise of Digital Job Placement in Cambodia Based on Human Rights Protection

Reconstruction and legal reform of the model for preventing human trafficking in Cambodia for Indonesian migrant workers under the guise of digital job placement must be directed toward establishing a digital technology- and human rights-based preventive protection system capable of addressing the transformation of modern trafficking. Legal reform is therefore needed through amendments to Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking and Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers by introducing specific norms concerning digital trafficking recruitment, digital recruitment monitoring, and the responsibilities of electronic platforms used in overseas recruitment. Derivative regulations in the form of Government Regulations or Presidential Regulations may establish a National Anti-Trafficking Digital Surveillance System coordinated through a legally defined institutional framework.

The system may use artificial intelligence to conduct an initial risk assessment of publicly available recruitment content and lawfully obtained digital information. However, AI should not determine that an advertisement constitutes trafficking or automatically trigger punitive action. Instead, the system should identify a combination of risk indicators, including the absence of verifiable recruiter or company identity, inconsistency between the advertised employer and official placement information, recruitment for destinations associated with identified trafficking risks, unrealistic remuneration, requests for unofficial payments, instructions to travel using inappropriate visa arrangements, repeated use of anonymous or newly created accounts, recruiter links to previously verified suspicious networks, and language indicating concealment of the actual nature of the work.

No single indicator should be sufficient to classify a recruitment activity as trafficking-related. The system should use a multi-factor risk assessment, generate a risk score or alert, and require human verification by an authorized officer before any investigation, content restriction, or other legal action is initiated. The algorithm should be periodically evaluated for accuracy and false-positive rates, while legitimate recruiters should have access to a correction or review mechanism if their content is incorrectly flagged. In this way, AI functions as an early-warning and prioritization tool rather than an autonomous mechanism for determining criminality. This approach remains consistent with the state's responsibility under Article 28I paragraph (4) of the 1945 Constitution to protect human rights while maintaining proportionality and legal certainty.

Legal reform must also be directed at strengthening cyber patrols and digital monitoring to prevent trafficking-related recruitment conducted through electronic systems. However, the authority to conduct such monitoring must be expressly limited by the principles of legality, necessity, proportionality, purpose limitation, and accountability. The National Anti-Trafficking Digital Surveillance System should primarily analyze publicly available recruitment content and other data lawfully obtained for a specific statutory purpose. Access to private communications, non-public account information, or other protected electronic data should remain subject to the authorization procedures required under applicable law. Monitoring should therefore not amount to unrestricted surveillance of citizens or generalized profiling based solely on personal characteristics.

A specialized Anti-Digital Human Trafficking Task Force may be established through a clear regulatory framework involving the Indonesian National Police, BP2MI, Immigration, the Ministry of Communication and Digital, PPATK, the Ministry of Foreign Affairs, and other legally relevant institutions. Each institution should exercise authority according to its statutory function, while access to information must be role-based and limited to the data necessary for a defined prevention or investigation purpose. The system should maintain audit logs, establish data-retention limits, conduct periodic security assessments, and provide supervisory mechanisms for alleged misuse of surveillance authority or personal data.

Legal reform should also establish due-diligence obligations for digital platforms that host or distribute overseas job advertisements. These obligations may include: first, reasonable verification of recruiter or advertiser identity for designated high-risk overseas recruitment categories; second, verification against official lists or registries of authorized placement entities where technically and legally feasible; third, a notice-and-review mechanism for suspicious recruitment content; fourth, temporary restriction or removal of content that has been verified as unlawful or presents a substantial trafficking risk; fifth, a dedicated reporting channel for users and government authorities; sixth, preservation of relevant recruitment records and account metadata for a legally limited period when a lawful preservation request is issued; and seventh, periodic transparency reporting regarding content actions related to trafficking and illegal overseas recruitment. Failure to comply with clearly established obligations after lawful notice or verification may result in proportionate administrative sanctions. These obligations should be directed at risk-based due diligence and not impose a general obligation to monitor every private communication or automatically censor legitimate employment advertisements.

In addition to strengthening digital oversight, legal reform must also create cross-agency data integration to build an effective early warning system for trafficking. Weak inter-agency coordination has resulted in many undocumented migrant workers entering Cambodia on tourist visas without being detected. Therefore, the government needs to establish an Integrated Migrant Protection System that connects data from the Indonesian Migrant Workers Association (BP2MI), Immigration, the Police, the Ministry of Foreign Affairs, the Population and Civil Registration Agency (Disdukcapil), and the Ministry of Manpower into a single national digital system. Specifically, every citizen traveling to a

country with a high trafficking risk, such as Cambodia, must undergo a digital verification process regarding their departure destination, employment contract, company sponsorship, and the legality of their placement. The system even needs to be equipped with an AI-based risk assessment to detect suspicious departure patterns based on age, travel purpose, recruiter history, and the type of job offered. If any indication of trafficking risk is found, the system automatically notifies relevant authorities for further investigation. This model implements Article 69 of Law Number 18 of 2017, which requires the government to protect migrant workers through monitoring and preventing undocumented placement. Furthermore, the establishment of an early detection system aligns with the due diligence principle in international human rights law, which requires states to take preventive measures to prevent human rights violations by non-state actors.

Legal reconstruction based on human rights protection must also be realized through strengthening digital education and legal literacy for prospective Indonesian migrant workers. Many human trafficking victims are trapped due to a lack of understanding of the risks of online recruitment and a lack of access to legal information regarding overseas job placement. Therefore, the government needs to mandate anti-trafficking digital literacy education as part of the administrative process for placing Indonesian migrant workers. Specifically, the Indonesian Migrant Workers Association (BP2MI), in collaboration with the Ministry of Education and local governments, can establish a Digital Anti-Trafficking Education Program that provides training on identifying fake job vacancies, digital security, reporting mechanisms, and migrant workers' rights under national and international law. Furthermore, the government needs to develop an official national application that provides a database of legal placement companies, overseas job vacancy verification services, an emergency panic button, and rapid access to complaints for migrant workers abroad. This program is crucial because Article 5 of Law Number 18 of 2017 affirms that Indonesian migrant workers have the right to receive accurate information regarding the job market and overseas placement procedures. Thus, the protection of migrant workers is not only carried out through a repressive approach, but also through strengthening community capacity to protect themselves from the risks of digital exploitation.

Internationally, legal reconstruction must also strengthen bilateral cooperation between Indonesia and Cambodia in combating digital human trafficking. The proposed Bilateral Digital Anti-Trafficking Agreement should not merely contain a general commitment to cooperate but should establish specific operational mechanisms. First, the Agreement should provide procedures for joint investigations involving designated Indonesian and Cambodian authorities, including the designation of contact points and procedures for urgent cross-border coordination. Second, it should regulate the preservation, authentication, and exchange of digital evidence, including recruitment communications, account information, electronic transaction records, platform data, and other electronically stored information, subject to the applicable laws of each State.

Third, the Agreement should establish a joint mechanism for victim identification and referral, including procedures for identifying Indonesian citizens found in scam centers or other suspected exploitation sites and for ensuring that victims are not automatically

treated as immigration offenders or criminal perpetrators before an appropriate assessment is conducted. Fourth, it should regulate rapid repatriation, temporary shelter, access to consular assistance, medical and psychological support, and the secure return of identity and travel documents. Fifth, the Agreement should provide mechanisms for asset tracing, freezing, and recovery where proceeds of trafficking or digital exploitation are located in either jurisdiction. Sixth, the parties should establish coordinated procedures for identifying and disrupting scam-center networks and trafficking-related recruitment infrastructure.

The Agreement should also provide for periodic information exchange, designated emergency contact points, joint training, annual implementation reviews, and cooperation with relevant international or regional mechanisms, including Interpol and ASEANAPOL where appropriate. The proposed joint cyber trafficking task force should therefore operate under clearly defined authority, information-sharing safeguards, and accountability mechanisms rather than as an informal coordination arrangement. The strengthening of the Indonesian Embassy in Cambodia through a Crisis Response Digital Center can complement this framework by providing rapid reporting, victim referral, consular assistance, and emergency protection in accordance with the Palermo Protocol and applicable human rights obligations.

The reconstruction and legal reform of the model for preventing human trafficking in Cambodia for Indonesian migrant workers under the guise of digital job placement must be directed toward establishing an adaptive, integrated, and human rights-oriented preventive protection system. Legal reform cannot simply be achieved through increasing criminal sanctions, but must address the digital recruitment stage through a combination of clearer substantive norms, platform due diligence, risk-based monitoring, institutional data coordination, victim protection, and effective international cooperation. The proposed model therefore shifts the legal policy orientation from an exclusively reactive response after exploitation has occurred toward an early-warning and prevention framework capable of identifying legally relevant trafficking indicators while maintaining privacy, freedom of movement, and due process.

The reconstruction should be implemented through amendments to Law Number 21 of 2007, Law Number 18 of 2017, and relevant provisions governing electronic systems and electronic information, followed by implementing regulations that define institutional authority, technical standards, data-protection safeguards, and accountability mechanisms. In this manner, digital technology is not treated merely as an instrument of surveillance but as a legally controlled mechanism for prevention, verification, victim protection, and coordinated intervention. Such reconstruction is consistent with the constitutional obligation to protect citizens, the Palermo Protocol, and the principle of state due diligence in preventing human rights violations by non-state actors.

Conclusion

Based on the discussion, the development of digital technology has transformed the pattern of human trafficking against Indonesian migrant workers from conventional forms to digital-based human trafficking that utilizes social media, online platforms, and

electronic communication applications as the primary means of recruiting victims to Cambodia. This practice has developed as part of a transnational organized crime integrated with cybercrime, scam centers, online gambling, and digital labor exploitation. The recruitment method is carried out through fake job offers with the lure of high salaries, but in reality, victims experience confinement, intimidation, violence, passport confiscation, and forced work in an international digital fraud network. Legally, this practice fulfills the elements of the crime of human trafficking as stipulated in Law Number 21 of 2007 concerning the Eradication of the Crime of Human Trafficking and is contrary to Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers. However, national legal policies still face various weaknesses, such as regulatory disharmony, weak oversight of digital recruitment, suboptimal cross-agency coordination, minimal cyber surveillance, and the absence of a digital technology-based early warning system for trafficking. Furthermore, positive law does not yet comprehensively regulate the accountability of digital platforms in preventing illegal cross-border labor recruitment. This condition shows that the national legal system is still repressive and not yet adaptive to the development of modern digital human trafficking, so that human rights protection for Indonesian migrant workers has not been implemented optimally.

Based on this finding, a reconstruction and legal update of the human trafficking prevention model for Indonesian migrant workers is needed, based on human rights protection through a digital technology-based preventive approach. The government needs to revise regulations related to human trafficking, migrant worker protection, and electronic systems by including specific norms regarding digital trafficking recruitment, digital platform oversight, and the accountability of electronic service providers in preventing illegal recruitment. In addition, the state needs to build an integrated digital surveillance system by strengthening cyber patrols, establishing AI-based recruitment monitoring, integrating data across agencies, and establishing an early warning system for trafficking that can detect high-risk migrant worker recruitment patterns early on. The government also needs to strengthen public digital literacy through information technology-based anti-trafficking education and develop an official overseas job vacancy verification application to prevent the spread of fake job information. Internationally, bilateral cooperation between Indonesia and Cambodia is needed to strengthen digital data exchange, joint cyber investigations, victim protection, and eradicating cross-border scam centers. With this legal reconstruction, it is hoped that a protection system for Indonesian migrant workers will be created that is more adaptive, responsive, and progressive to the development of modern digital crimes while being able to provide legal certainty, justice, and effective human rights protection against the threat of digital technology-based human trafficking.

References

- Ardanya, C., & Wulandari, M. E. (2025). Diplomasi Indonesia Dalam Menangani Kasus Perdagangan Manusia Di Kamboja. *Jurnal Ilmu Sosial Dan Humaniora*, 1702–1715.
- Danuri, M. (2019). Perkembangan dan Transformasi Teknologi Digital. *Jurnal Ilmiah Infokam*.
- Fikri, S. (2022). Perlindungan Dan Pemenuhan Hak Asasi Manusia Bagi Pekerja Migran Indonesia Di Luar Negeri. *Jurnal Upgriplk*.

- Hidayat, R., Syahnan, M., & Rokan, M. K. (2026). Optimalisasi Calling Visa, E-Visa, Dan Sanksi Pidana Dalam Pencegahan Pekerja Migran Indonesia Ilegal Ke Kamboja. *Rechtsnormen Jurnal Komunikasi Dan Informasi Hukum*, 85–91.
- Hidayat, I. D. (2021). Perlindungan Pekerja Migran Indonesia/Tenaga Kerja Indonesia Oleh Pemerintah Daerah. *Mizan: Jurnal Ilmu Hukum*, 71–80.
- Indah Rohmawati, Amir Junaidi, dan A. K. (2024). Urgensi Regulasi Penyalahgunaan Deepfake sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO). *Innovative: Journal of Social Science Research*, 4(6), 1779–1794.
- Ismail, M. M., Ismail, Y., & Humiati, H. (2025). Tinjauan Yuridis Terhadap Pelindungan Pekerja Migran Indonesia. *Interdisciplinary Explorations In Research Journal*.
- Istiqomah, I., Tarmudi, T., Yusuf, H., Dewi, R., & Umboh, N. K. (2023). Analisis Yuridis Perlindungan Hukum Terhadap Pekerja Migran Indonesia Di Luar Negeri. *Action Research Literate*.
- Nugroho, B., & Roesli, M. (2017). Analisa Hukum Tindak Pidana Perdagangan Orang (Human Trafficking). *Jurnal Bina Mulia Hukum*.
- Nugroho, O. C. (2018). Tanggung Jawab Negara Dalam Penanganan Tindak Pidana Perdagangan Orang. *Jurnal Penelitian Hukum De Jure*.
- 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)*.
- Sari, F. R., & Adityo, R. D. (2024). Efektivitas Alat Bukti Elektronik Pada Praktik Beracara Perspektif Teori Sistem Hukum Lawrence M. Friedman. *Sakina: Journal Of Family Studies*.
- Shabrina'Ishmah, D., Aqimuddin, E. A., & Izadi, F. F. (2023). Perlindungan Tenaga Kerja Wanita Indonesia Dalam Kasus Perdagangan Manusia Di Kamboja. *Jurnal Riset Ilmu Hukum*.
- Shaliha, R., & U. (2023). Tinjauan Yuridis Perlindungan Hukum Jaminan Sosial Bagi Pekerja Migran Berdasarkan Undang–Undang Nomor 18 Tahun 2017 Tentang Perlindungan Pekerja Migran Indonesia. *Indonesia Berdaya*.
- Sidik, I. A., Suherman, A. (2024). Efektivitas Penerapan Hukum Perlindungan Perempuan Dan Anak Dalam Mencegah Kekerasan. *Jurnal Kajian Hukum Dan Kebijakan Publik* | E-ISSN : 3031-8882, 2(1), 174–182.
<https://jurnal.kopusindo.com/index.php/jkhkp/article/view/351>