



LICS 2026

Topic: Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children

Criminal Law Formulation in Indonesia in Addressing New Modes of Human Trafficking Based on The Digital Sector

Wagiyo

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: w4giyo86@gmail.com

Abstract. *The era of digital disruption has brought about a radical transformation not only in the economic and communication sectors but also in the landscape of organized transnational crime. One of the most tangible threats today is the evolution of conventional Human Trafficking Crimes (TPPO) into cyber-trafficking or digital-based human trafficking. This phenomenon is characterized by a massive shift in modus operandi, where recruitment is carried out through social media, online job scams, and the exploitation of victims who are forced to become operators of online gambling, investment fraud, and other cybercrimes (cyber-slavery) in various Southeast Asian countries. Amid this massive shift in criminal methods, Indonesia's criminal law instruments, particularly Law Number 21 of 2007 on the Eradication of Human Trafficking Crimes, are considered to have begun lagging behind and experiencing technological inadequacy. Current positive law remains heavily oriented toward conventional physical and sexual exploitation, thereby creating legal gaps in prosecuting the intellectual actors behind these cybercrime networks. This study aims to examine and analyze the weaknesses within Indonesia's current positive criminal law system and to propose a comprehensive criminal law policy formulation for addressing cyber-trafficking. This research employs a normative legal research doctrinal legal research method using statutory and conceptual approaches. The study examines the conflicts among the Human Trafficking Law, the Electronic Information and Transactions Law (ITE Law), and the Criminal Procedure Code. As a solution, this study formulates the urgency of regulatory reform through the harmonization and integration of substantive and procedural criminal law. The proposed formulation includes expanding the meaning of "exploitation" to accommodate virtual exploitation and forced cybercrime, implementing the concept of strict liability for digital service provider corporations that act negligently, and strengthening extraterritorial instruments and Mutual Legal Assistance mechanisms. This criminal law reform is*

Criminal Law Formulation in Indonesia...
(Wagiyo)



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

essential to protect Indonesian citizens from the threat of modern slavery while creating a criminal justice system that is adaptive, responsive, and just in the digital era.

Keywords: *Digital Sector; Electronic Transactions; Human Trafficking.*

1. Introduction

The development of information and communication technology (ICT) in the 21st century has created a new living space for human civilization known as cyberspace. This digitalization has undeniably brought efficiency, unlimited global connectivity, and the democratization of information, which have driven exponential global economic growth. Unfortunately, like a double-edged sword, technological advancement has also introduced new threats. Cyberspace, which is borderless, anonymous, and instantaneous, has been exploited by transnational criminal syndicates to modernize their operations, giving rise to forms of cybercrime that are far more complex, organized, and difficult for conventional law enforcement authorities to trace.¹

One form of transnational crime that has undergone the most alarming transformation due to technological advancement is Human Trafficking (TPPO). Historically, human trafficking has been associated with physical abduction, smuggling across land and sea borders, and exploitation centered on forced prostitution or manual labor in domestic and plantation sectors. Today, however, this crime has evolved into cyber-trafficking (cyber-based human trafficking). International syndicates no longer need to travel directly to villages to find victims; they simply exploit social media algorithms, instant messaging applications, and fake job vacancy websites to ensnare victims remotely at minimal operational cost.²

The phenomenon of cyber-trafficking has become increasingly prominent and has developed into a regional crisis in Southeast Asia, particularly after the COVID-19 pandemic. Economic downturns, high unemployment rates, coupled with increasing basic digital literacy but low digital security awareness among young people, have made Indonesian citizens (WNI) prime targets. Thousands of technologically literate Indonesians have been deceived by offers of high-paying jobs as customer service representatives or marketing staff abroad, only to be trafficked into heavily guarded scam compounds in countries such as Cambodia, Myanmar,

¹ Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar* (Jakarta: Kencana, 2013), hlm. 24

² Barda Nawawi Arief, *Kebijakan Hukum Pidana (Penal Policy)* (Jakarta: Kencana, 2011), hlm. 55-58.



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

and the Philippines.³ There, they are forced to work long hours under threats of physical abuse, carrying out online fraud, cryptocurrency theft (pig butchering scams), and online gambling operations.

In facing the complexity of these new methods, Indonesia's criminal justice system is required to provide responses that are swift, accurate, and deterrent. The primary legal instrument currently used to combat human trafficking is Law Number 21 of 2007 concerning the Eradication of Human Trafficking Crimes (Human Trafficking Law). When enacted nearly two decades ago, this law was recognized as one of the most progressive legislative products in Asia. However, static criminal law has gradually fallen behind the rapidly evolving dynamics of crime. The normative formulation of the Human Trafficking Law still relies heavily on physical dimensions, both in terms of recruitment processes and the definition of forms of exploitation.⁴

Its most crucial weakness lies in the elaboration of the element of "exploitation." Lawmakers at the time did not anticipate the emergence of "digital slavery" (cyber-slavery), where victims are not exploited for manual labor in bridge construction or factory work but are instead forced to use their minds to deceive others through computer screens in air-conditioned rooms locked from the outside. This has created debates in courtrooms: does forcing someone to become an online scammer fulfill the element of exploitation in the same way as conventional forced labor? This ambiguity in legal norms often complicates prosecutors' efforts to draft solid indictments, potentially allowing perpetrators to escape prosecution under human trafficking provisions that carry severe criminal penalties.⁵

To address this weakness, law enforcement officers often attempt to combine the Human Trafficking Law with Law Number 11 of 2008, as most recently amended by Law Number 1 of 2024 concerning Electronic Information and Transactions (ITE Law). Although the ITE Law regulates cybercrime, its approach primarily focuses on crimes against electronic systems (such as hacking and data manipulation) or illegal content (such as defamation, obscenity, and hoaxes). The ITE Law contains no normative provisions specifically designed to regulate

³ Diana Yusyanti, "Pelindungan Hukum Terhadap WNI Korban Tindak Pidana Perdagangan Orang di Era Digital," *Jurnal Penelitian Hukum De Jure* 21, no. 3 (2021): 392

⁴ Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang, Penjelasan Umum

⁵ Eddy O.S. Hiarij, "Evolusi Kejahatan Transnasional dan Kesiapan Hukum Pidana Indonesia," *Jurnal Hukum Pidana dan Kriminologi* 1, no. 2 (2020): 115



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

cybercrimes involving the exploitation of human bodies, freedom, and dignity as found in human trafficking cases.⁶ Consequently, law enforcement becomes partial and fragmented.

Another equally complex challenge in cyber-trafficking concerns jurisdiction and evidentiary procedural law. Indonesia's Criminal Procedure Code (KUHP) was drafted in 1981, long before the internet existed. The investigation and prosecution of crimes whose, locus delicti is abroad, while the servers used are located in a third country and victims are recruited in Indonesia, create extraordinarily complicated jurisdictional conflicts. Digital evidence, such as conversations on Telegram that can be automatically deleted, along with financial transactions using decentralized cryptocurrencies, is extremely difficult to seize and present as valid evidence in court without a modern legal framework for digital forensics.⁷

Furthermore, current legal instruments have yet to adequately address corporate criminal liability in the technology sector. Digital platforms, social media companies, and internet service providers often shield themselves behind the Safe Harbor Policy, claiming that they merely serve as neutral intermediaries and are therefore not responsible for user-generated content. In reality, however, their algorithms frequently facilitate systematic connections between human trafficking recruiters and prospective victims. Future criminal law policy must begin formulating stringent liability mechanisms for technology corporations that negligently or deliberately ignore human trafficking advertisements and activities on their platforms.⁸

The need to reform (reconstruct) both substantive and procedural criminal law has become increasingly urgent considering the vulnerability of cyber-trafficking victims to secondary victimization. It is not uncommon for Indonesian citizens who have been rescued and repatriated to instead be arrested and prosecuted under the ITE Law for committing online fraud, without considering that they acted under coercion, death threats, and duress. Indonesia's current positive law does not yet contain a firm and comprehensive non-punishment clause for human trafficking victims who are forced to commit crimes, particularly cybercrimes.⁹

Based on this highly critical background, this scientific article has both academic and practical urgency in examining the deadlock within Indonesia's current criminal justice system. This study aims to map the anatomy of cyber-trafficking methods in Indonesia, highlight the

⁶ Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 27-29

⁷ Romli Atmasasmita, *Sistem Peradilan Pidana Kontemporer* (Jakarta: Kencana, 2010), hlm. 77.

⁸ Eddy O.S. Hiarij, *Op.Cit.*, hlm. 120

⁹ Diana Yusyanti, *Loc.Cit.*, hlm. 400



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

regulatory gaps in existing positive law, and construct an ideal formulation of future criminal law policy. Through this study, it is hoped that a prescriptive recommendation can be developed for policymakers in designing laws that are precise, adaptive, and fully oriented toward protecting victims of human trafficking in the digital era.

2. Research Methods

This study is a normative legal research (doctrinal legal research) focusing on the examination of legal rules, norms, and principles within the criminal justice system. The primary approach employed is the statutory approach, involving a comprehensive analysis of the consistency and weaknesses of existing positive legal instruments. The legislation examined includes: the 1945 Constitution of the Republic of Indonesia, Law Number 21 of 2007 concerning the Eradication of Human Trafficking Crimes, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, Law Number 8 of 1981 concerning Criminal Procedure (KUHP), and Law Number 1 of 2023 concerning the Criminal Code (New Criminal Code).¹⁰ In addition, this research employs a conceptual approach to explore the views of scholars and modern criminal law doctrines concerning transnational cybercrime. All primary, secondary (journals and academic literature), and tertiary legal materials are analyzed using a prescriptive method to produce ideas for criminal law reform.

3. Results and Discussion

3.1. Characteristics and Modus Operandi of Cyber-Trafficking in Indonesia

The metamorphosis of human trafficking into cyber-trafficking is marked by a dramatic shift in the initial recruitment stage. Whereas in traditional trafficking in persons (TIP), brokers (recruiters) visited impoverished villages, they now invade people's private spaces through smartphone screens. The recruitment process (cyber-recruitment) is carried out on a massive scale by creating fake accounts and community groups on Facebook, Telegram, and TikTok. Recruiters post highly professional-looking international job advertisements, offering prestigious positions such as customer service representatives or IT staff abroad with promises of salaries worth thousands of dollars, free airfare, and luxurious accommodation, all without requiring high educational qualifications. This strategy of visual manipulation quickly captivates job seekers facing economic hardship.¹¹

¹⁰ Undang-Undang No. 1 Tahun 2023 Tentang KUHP Nasional

¹¹



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

This shift in characteristics has also changed the demographic profile of trafficking victims in Indonesia. Cyber-trafficking syndicates no longer target illiterate manual laborers but instead focus on Millennials and Generation Z who possess basic digital literacy, can operate computers, have good communication skills, and understand at least basic English. This makes the crime highly organized and targeted, as perpetrators are essentially "recruiting brains" to serve as the frontline operators of their financial crimes. Victims who consider themselves educated often fail to realize they are being ensnared in a human trafficking scheme until they actually arrive in the destination country.

Upon arrival in the transit country, the exploitation shifts to the physical and digital deprivation of human rights. Victims' passports and identification documents are immediately confiscated. Furthermore, their personal communication devices are destroyed or cloned to obtain personal information about their families in Indonesia as leverage for threats. Victims are then taken to heavily guarded compounds surrounded by high barbed-wire walls and armed security personnel (scam compounds). It is there that "digital slavery" begins. Victims are forced to sign fraudulent debt contracts amounting to hundreds of millions of rupiah, allegedly covering their accommodation costs, which can only be repaid by working for the syndicate without compensation.¹²

During the exploitation process, victims are forced to create hundreds of fake accounts across various social media platforms and dating applications. Their task is to locate targets, build fake romantic relationships (grooming), and ultimately deceive victims (located in the United States, Europe, or Asia) into investing in fraudulent cryptocurrency schemes (pig butchering scams). Working hours range from 15 to 18 hours per day. If victims refuse, fail to meet fraud quotas, or attempt to seek assistance from authorities, they face brutal physical punishment, including beatings, electric shocks, solitary confinement in dark isolation rooms, or being sold to other syndicates or scam companies.

Financially, these syndicates have fully exploited decentralized finance (DeFi) and cryptocurrency ecosystems to obscure financial transactions (money laundering). The proceeds generated by the victims (forced laborers) are immediately laundered through thousands of anonymous digital wallets (cold wallets) before being converted back into fiat currency. The use of encryption technology and blockchain makes asset tracing by the Indonesian Financial Transaction Reports and Analysis Center (PPATK) and conventional law enforcement authorities virtually impossible without highly specialized digital forensic experts, allowing the intellectual masterminds behind the syndicates to remain untouched.

¹² Maskun, *Op.Cit.*, hlm. 45-47



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

Anonymity is the primary weapon in cyber-trafficking. The masterminds, syndicate leaders, and principal investors hide behind layers of false identities and Dark Web networks. They operate servers from jurisdictions with weak legal systems or complex extradition laws. Within this criminal hierarchy, Indonesian nationals who become victims are employed as buffers, directly interacting with cyber fraud victims. If a scam center is raided by local law enforcement authorities, the syndicate leaders can easily escape, while the victims are arrested and publicly identified as perpetrators of international cyber fraud.¹³

This creates a unique legal complexity concerning the status of victims. In cyber-trafficking, the boundary between victim and perpetrator (victim-perpetrator nexus) becomes highly blurred. Objectively, these Indonesian nationals commit cybercrimes (defrauding others of thousands of dollars); however, causally and subjectively, they commit these crimes because they lack free will (vitiating consent) due to threats of physical torture. This phenomenon creates an extraordinary dilemma for the criminal justice system and international law regarding how to prosecute cybercrime without punishing victims of human trafficking who were coerced into committing it.

These characteristics of cyber-trafficking clearly demonstrate that crime has evolved faster than criminal law itself. The evolution from physical-space crimes to cyberspace, algorithmic psychological manipulation, cryptocurrency money laundering, and cyber slavery represents the dark residue of the digital era. Indonesian police, immigration authorities, and courts can no longer confront this complex phenomenon using conventional law enforcement perspectives from previous decades. A radical legal disruption is required to counterbalance and combat this disruption in crimes against humanity.

3.2. Gaps and Weaknesses in Indonesia's Current Positive Criminal Law

The primary legal instrument for prosecuting human trafficking perpetrators in Indonesia is Law Number 21 of 2007. Unfortunately, this 17-year-old regulation contains significant legal loopholes in responding to cyber-trafficking. The first and most fundamental weakness lies in the definition of "exploitation" under Article 1 paragraph 7 of the TIP Law. The definition remains limited to prostitution, forced labor, slavery, oppression, extortion, debt bondage, or organ removal.¹⁴ The absence of the terms "forced criminality" or "cyber exploitation" makes it difficult for law enforcement officers to convince judges that forcing someone to sit at a computer and scam others constitutes forced labor or modern slavery. The second

¹³ Barda Nawawi Arief, *Op.Cit.*, hlm. 62

¹⁴ *Undang-Undang Nomor 21 Tahun 2007, Pasal 1 angka 7*



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

weakness originates from the Electronic Information and Transactions Law (ITE Law). Although amended in 2024, the law remains solely oriented toward addressing misuse of electronic systems (such as hacking, interception, and dissemination of illegal content). The ITE Law fails to recognize the intersection between cybercrime and crimes involving human exploitation. Not a single provision regulates the "misuse of electronic systems to facilitate human trafficking." Consequently, police officers who arrest online recruiters (those posting scam advertisements on Facebook) often can only charge them under ordinary fraud provisions, carrying significantly lighter penalties than trafficking offenses and failing to provide meaningful deterrence.

In procedural criminal law, the 1981 Criminal Procedure Code (KUHP) also constitutes a chronic bureaucratic obstacle. Indonesia's procedural regime continues to place excessive emphasis on physical evidence and direct face-to-face testimony. Although the ITE Law and the TIP Law recognize electronic evidence as valid evidence, there are still no detailed procedural standards governing the acquisition (search and seizure), preservation (chain of custody), and forensic examination of digital evidence related to cyber-trafficking. Judges frequently reject screenshots of WhatsApp or Telegram conversations between perpetrators and victims when the original devices have already been destroyed by syndicates, considering them procedurally defective and lacking sufficient evidentiary value.¹⁵

Jurisdictional obstacles (*locus delicti*) constitute one of the greatest frustrations for law enforcement authorities. The territorial principle in Indonesian criminal law limits police authority to conduct investigations and arrests outside Indonesia's sovereign territory. In online scam cases occurring in Cambodia or Myanmar, the criminal server may be located in Russia, the mastermind may be a Chinese national, recruitment may occur in Indonesia, and exploitation may take place in Myanmar. The lack of clear regulations regarding the application of the active nationality principle and the protective principle in cyber-trafficking cases leaves the Indonesian National Police (Polri) with little option but to wait until victims are deported back to Indonesia, while the principal perpetrators remain free abroad.

Furthermore, a structural gap exists in the absence of explicit corporate criminal liability for digital platform providers (Platform Accountability). Currently, trafficking syndicates exploit the infrastructure of major technology companies' social media platforms (Big Tech) free of charge and on a massive scale. However, Indonesian positive law contains no negligence provisions capable of holding platform providers criminally liable for failing to establish filtering mechanisms, automatic reporting systems, and blocking fraudulent international job

¹⁵ Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, Pasal 184



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

advertisements.¹⁶ Allowing technology platforms to enjoy impunity means allowing the digital public sphere to remain dominated by human trafficking predators.

Another weakness concerns protecting victims' digital identities. Indonesian criminal law and victim protection regulations do not comprehensively recognize the Right to be Forgotten for trafficking victims. When victims' faces, passport photos, or torture videos have already been circulated online by perpetrators as intimidation, the state lacks rapid and enforceable legal instruments to remove such humiliating digital traces from search engines. As a result, victims continue to suffer endless psychological trauma even after being physically rescued.

The situation is further aggravated by the weak implementation of the Non-Punishment Principle, which is implicitly embedded in international regulations. Although the TIP Law states that a victim's consent does not eliminate the criminal elements of trafficking, it does not explicitly prohibit law enforcement authorities from prosecuting victims who were "forced" to commit crimes (such as online fraud or online gambling). Institutional conflicts frequently arise between the Cyber Crime Directorate (Ditpid Siber), which seeks to prosecute them as ITE offenders, and the General Crime Directorate (Ditpidum), which recognizes them as trafficking victims.

Based on all the identified gaps, it can be concluded that Indonesia's criminal law civilization is experiencing acute cognitive dissonance in confronting cyber threats. As long as law enforcement officers are forced to wield the blunt sword of outdated legal instruments against cybercriminals shielded by military-grade encryption technology, the state will always remain one step behind in protecting its citizens from the vortex of digital human trafficking.

3.3. Future Criminal Law Formulation and Reconstruction (Ius Constituendum)

To overcome the current paralysis of the legal system, Indonesia urgently requires a comprehensive, progressive, and technology-oriented formulation and reconstruction of its criminal law policy (penal policy). The first urgent formulation is to amend Law Number 21 of 2007 (the TIP Law) by explicitly incorporating cybercrime into the scope of trafficking offenses. The concept of "exploitation" must be broadly reconstructed to include "digital forced criminality" and "cyber slavery." This reform will provide judges and prosecutors with clear legal authority to classify forcing Indonesian citizens to become online scammers as a serious human exploitation offense punishable by the maximum sentence, rather than as ordinary fraud.¹⁷

¹⁶ Romli Atmasasmita, *Op.Cit.*, hlm. 95

¹⁷ Barda Nawawi Arief, *Op.Cit.*, hlm



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

The second formulation focuses on redefining recruitment. New regulations should include technology-based recruitment methods, such as social media algorithm manipulation, fake profiles, fictitious online job advertisements, and victim entrapment through illegal fintech platforms. Moreover, to prosecute upstream perpetrators, criminal law should formulate accomplice liability (complicity in trafficking) for technical actors who provide technological infrastructure, including creators of fake websites, providers of mule accounts, and IT specialists who build encryption systems to conceal the identities of trafficking syndicates.

The third formulation extends into procedural criminal law. The future Criminal Procedure Code (KUHP) must radically accommodate digital forensic governance. Law enforcement authorities should be granted exceptional authority (lawful interception) to intercept communications, regain access through hacking, and freeze cryptocurrency wallets suspected of being affiliated with trafficking networks without cumbersome court authorization procedures during exigent circumstances. Furthermore, the legal validity of electronic evidence such as disappearing messages, GPS records, and biometric data retrieved from cloud servers should be recognized as primary evidence standing independently, equal to physical witness testimony.¹⁸

The fourth formulation requires the state to courageously implement corporate criminal liability and strict liability for major technology companies operating social media platforms (such as Meta, X, Google, and Telegram). If a corporation fails to establish AI-based filtering systems capable of blocking trafficking recruitment content, it should be subject to massive criminal fines and obligated to compensate victims. This Platform Accountability principle would compel technology companies to invest substantially more in digital security governance instead of merely profiting from Indonesian users' data.

The fifth formulation aims to resolve jurisdictional deadlocks by strengthening international legal cooperation. Indonesian criminal law should formulate a more aggressive extended extraterritorial jurisdiction clause, allowing the Indonesian National Police to pursue and prosecute intellectual masterminds wherever they may be located, provided their actions harm Indonesia's national interests or exploit Indonesian citizens. This formulation should be accompanied by initiatives establishing ASEAN-specific Mutual Legal Assistance (MLA) agreements and extradition treaties specifically addressing cyber-trafficking, thereby eliminating safe havens for regional trafficking syndicates.¹⁹

¹⁸ Eddy O.S. Hiarij, *Op.Cit.*, hlm. 122

¹⁹ Diana Yusyanti, *Op.Cit.*, hlm. 401



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

The sixth formulation focuses on legal and digital victim protection. Indonesia's positive law should immediately incorporate a Non-Punishment Provision explicitly stating: "Any victim of trafficking in persons who is compelled to commit a criminal offense, including cybercrime and electronic information offenses, shall not be subject to criminal or civil liability for such acts." This legal immunity clause is essential so that Indonesian citizens trapped in Cambodia or Myanmar will not fear imprisonment upon rescue, thereby encouraging them to cooperate as whistleblowers in dismantling trafficking networks.

The seventh formulation concerns comprehensive victim recovery, particularly regarding asset recovery and restitution. Future legal frameworks should enable the state to confiscate cryptocurrency assets belonging to syndicates, auction them through official exchanges, and use the proceeds directly to pay restitution to victims. Since syndicate members are often difficult to apprehend physically, "digital impoverishment" through virtual asset confiscation represents the most logical and deterrent financial punishment. Furthermore, victims should be granted a legally enforceable Right to be Erased, fully supported by the relevant ministries, to ensure long-term psychological rehabilitation.

Through these seven pillars of criminal law reform, Indonesia would no longer remain reactive while waiting for its citizens to become victims. The integration of robust substantive criminal law, legitimate digital forensic procedures, corporate accountability for major technology companies, and comprehensive victim protection will establish a resilient legal architecture. The transformation from conventional criminal law to cyber-savvy criminal law represents a constitutional obligation that the state must urgently fulfill to uphold human dignity and justice in the digital era.

4. Conclusion

The dynamics of the digital era have transformed conventional trafficking in persons (TIP) into the far more organized, systematic, and borderless threat of cyber-trafficking. International syndicates now exploit Indonesian citizens by recruiting them through fake job advertisements on social media and forcing them into cyber slavery, including cryptocurrency fraud and online gambling operations, from heavily guarded compounds in third countries. Unfortunately, Indonesia's current criminal law regime, based on Law No. 21 of 2007 (the TIP Law), the ITE Law, and the Criminal Procedure Code (KUHAP), has proven technologically inadequate. The absence of a definition of cyber exploitation, difficulties in recognizing digital forensic evidence, overlapping cross-border jurisdiction, and the lack of criminal liability for digital platform providers render existing legal instruments fragile and incapable of dismantling criminal networks up to their intellectual masterminds.

Criminal Law Formulation in Indonesia...
(Wagiyo)



LICS 2026

Topic: *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

5. References

Journals:

Hiariej, Eddy O.S. "Evolusi Kejahatan Transnasional dan Kesiapan Hukum Pidana Indonesia." *Jurnal Hukum Pidana dan Kriminologi* 1, no. 2 (2020): 110-125.

Yusyanti, Diana. "Pelindungan Hukum Terhadap WNI Korban Tindak Pidana Perdagangan Orang di Era Digital." *Jurnal Penelitian Hukum De Jure* 21, no. 3 (2021): 389-402.

Books:

Arief, Barda Nawawi. *Kebijakan Hukum Pidana (Penal Policy)*. Jakarta: Kencana, 2011.

Atmasasmita, Romli. *Sistem Peradilan Pidana Kontemporer*. Jakarta: Kencana Prenada Media Group, 2010.

Maskun. *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana, 2013.

Regulation:

Law Number 1 of 2023 concerning the Criminal Code.

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons.

Law Number 8 of 1981 concerning Criminal Procedure Law (KUHP).

The 1945 Constitution of the Republic of Indonesia.