LICS PROCEEDINGS OF LEGAL INTERNATIONAL AND STUDIES
No. ISSN : 2986-4089
Published by Universitas Islam Sultan Agung, Semarang, INDONESIA

**LICS 2026**
**Topic:** *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

# Invisible Footprints in Cyberspace: Legal Reconstruction for the Protection of Vulnerable Groups from Digital Exploitation Threats

**Aris Cahyo Wibowo**

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: ariscahyowibowo.std@unissula.ac.id

***Abstract.***

*The rapid digitalization of crime has created "invisible" footprints, leaving vulnerable groups exposed to cyber exploitation and online human trafficking, which traditional legal frameworks struggle to effectively address. This study aims to examine the legal reconstruction required to protect vulnerable groups from digital exploitation threats under the newly implemented National Criminal Code (KUHP Nasional). A normative legal approach was employed in conducting the research, utilizing statutory and conceptual analyses to evaluate current cyber-victimology frameworks. Based on the findings, it can be concluded that while the new code provides a stronger substantive basis, effective protection demands the integration of digital forensic guidelines, proactive transnational cooperation, and a specialized cyber-victim protection infrastructure to dismantle anonymous online syndicates.*

***Keywords:*** *Cyber Trafficking; Digital Exploitation; Legal Reconstruction; National Criminal Code; Vulnerable Groups.*

## 1. Introduction

The rapid advancement of digital technology has idealized cyberspace as a safe, accessible, and progressive domain for global communication and development. However, the actual situation starkly contrasts with this ideal condition, as cyberspace has increasingly transformed into a borderless arena for digital exploitation, particularly targeting vulnerable groups such as women and children. These "invisible footprints" of exploitation ranging from online grooming and cyber-harassment to digital human trafficking often circumvent traditional law enforcement boundaries, creating a severe legal gap between the protection that ought to be provided by the

state and the harsh reality of modern cyber-victimization.[1]

When compared to previous research findings, early legal studies have predominantly focused on the physical dimensions of human trafficking and conventional cybercrimes, such as financial fraud or data breaches. Previous scholars have extensively highlighted the limitations of domestic regulations in addressing the physical movement of trafficking victims, yet there remains a significant academic void concerning the specific legal reconstruction required to tackle the anonymity and digital modalities of modern exploitation.[2] Consequently, the existing legal paradigms must be fundamentally re-evaluated and reconstructed to address these non-physical, cyber-enabled threats effectively.

Addressing this complex legal gap requires a critical analysis of the newly implemented National Criminal Code (Law Number 1 of 2023), which officially took effect on January 2, 2026. This modernized penal instrument introduces essential provisions regarding cyber-related offenses and expands the scope of corporate criminal liability, offering a new foundation to combat sophisticated digital crimes. However, the mere codification of these offenses is insufficient; the application of these new norms to explicitly protect vulnerable groups from digital exploitation still requires comprehensive substantive and structural harmonization to ensure that the law is fully operational against invisible cyber-syndicates.[3]

In the author's opinion, identifying and resolving this specific research problem is of paramount importance. The failure to reconstruct and adapt the legal protection frameworks to the realities of cyberspace will render the new National Criminal Code underutilized and ineffective in preventing digital exploitation. Law enforcement agencies currently face unprecedented challenges in gathering electronic evidence, tracking encrypted communications, and overcoming transnational jurisdictional hurdles. Without a targeted legal reconstruction, perpetrators will continue to hide behind digital anonymity while vulnerable groups suffer irreversible psychological and societal harm.[4]

Furthermore, the required legal reconstruction must inherently prioritize a victim-

[1] Barda Nawawi Arief. Kebijakan Hukum Pidana dalam Penanggulangan Cybercrime. *Semarang: Pustaka Magister*, 2022.hlm. 4-6

[2] Wan Rahmat Kurniawan; Alwan Hadiyanto; Ciptono. Tindak pidana perdagangan orang dalam perspektif tindak pidana pencucian uang di Indonesia. *Jurnal USM Law Review*, 2024, 7.2: p.688-698.

[3] Reno Apri Dwijayanto. Tinjauan yuridis perbandingan KUHP lama dan KUHP baru dalam sistem peradilan pidana Indonesia. *Jurnal Sosial Teknologi*, 2026, 6.2: p.746-754.

[4] Eka Fitri Lestari; Rahmayanti; Donly Calner Aruan. Problematika Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia. *Dewantara: Jurnal Pendidikan Sosial Humaniora*, 2026, 5.2: p.178-191.

centered approach. Digital exploitation leaves permanent, replicable digital footprints that continuously revictimize the targets even long after the initial abuse has ceased. Therefore, the justice system must not only focus on the retributive punishment of cyber-traffickers but also establish robust, legally binding mechanisms for digital restitution, data erasure, and psychological recovery, which are currently underdeveloped in standard criminal procedures.[5]

Therefore, a proactive and technology-responsive legal strategy is urgently needed to synchronize the new criminal provisions with international cyber-law standards, ensuring absolute protection for vulnerable populations. By dissecting how the recent legislative reforms can be practically maximized to dismantle online exploitation networks, this research will contribute to formulating a more adaptive legal framework.[6] This study aims to examine the legal reconstruction for the protection of vulnerable groups from digital exploitation threats within the framework of the new National Criminal Code.

## 2. Research Method

This study employed a normative legal research approach, specifically utilizing statutory and conceptual approaches to examine the current legal frameworks and formulate the necessary legal reconstruction for protecting vulnerable groups from digital exploitation. The research specification applied in this study was descriptive-analytical, aimed at systematically mapping the "invisible footprints" of cyber-exploitation and critically analyzing the efficacy of the new National Criminal Code (which officially took effect on January 2, 2026) in addressing these technological threats.

The data collection method was conducted through a documentary study (library research) focusing entirely on secondary data. This data comprised primary legal materials, including the newly enforced National Criminal Code (Law Number 1 of 2023), the Law on Electronic Information and Transactions, and the Law on the Eradication of the Criminal Act of Trafficking in Persons. Secondary legal materials encompassed scholarly books, scientific journal articles, and relevant previous studies concerning cyber-victimology, digital privacy, and human rights. Tertiary legal materials, such as legal dictionaries and encyclopedias, were utilized to support and clarify the primary and secondary materials.

The collected legal materials were systematically processed and analyzed using a qualitative normative data analysis method. Through this method, the statutory

[5] SUNARSO, H. Siswanto;. *Viktimologi dalam sistem peradilan pidana*. Sinar Grafika, 2022. p. 50.
[6] SUSENO, Sigid, et al. Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences*, 2025, 11.1: p. 2439543.

provisions, legal texts, and academic literature were interpreted and logically correlated to draw deductive conclusions and propose a comprehensive legal reconstruction strategy to combat online human trafficking and digital exploitation.

## 3. Research and Discussion

### 3.1. Mapping the "Invisible Footprints": The Modus Operandi of Digital Exploitation Targeting Vulnerable Groups

The advent of the digital era has fundamentally revolutionized the *modus operandi* of transnational organized crime. Human trafficking and the exploitation of vulnerable groups—historically characterized by physical coercion, geographical displacement, and visible confinement—have rapidly migrated into the obscure and borderless realm of cyberspace. This migration has birthed a new paradigm of victimization, leaving behind "invisible footprints"—digital traces that are highly elusive to conventional law enforcement but permanently devastating to the victims. Analyzing how trafficking syndicates weaponize technology to target women and children is critical to understanding the necessity for a modernized legal reconstruction. This section maps the evolutionary trajectory of cyber-grooming, online solicitation, and the theoretical underpinnings of digital anonymity that facilitate these invisible crimes.

#### 3.1.1. The Evolution of Cyber-Grooming and Online Solicitation

Historically, the recruitment phase of human trafficking relied heavily on physical proximity. Syndicates deployed local brokers (*calo*) into rural or economically marginalized communities to deceive victims through false promises of employment, marriage, or financial assistance.[7] This physical modality left tangible trails: witness testimonies, physical transportation records, and geographical patterns. However, the proliferation of digital technology has drastically transformed this landscape. The recruitment phase has evolved into sophisticated online solicitation and *cyber-grooming*, allowing perpetrators to reach hundreds of potential victims simultaneously across different jurisdictions without ever leaving their operational bases.[8]

The transition from physical to digital recruitment primarily utilizes three

[7] Rian Rusmana Putra, et al. Analisis Penegakan Hukum Terhadap Tindak Pidana Perdagangan Orang di Kamboja dalam Perspektif Hukum Pidana Nasional. *JURNAL USM LAW REVIEW*, 2026, 9.2: p. 771-790.
[8] Dikdik M. Arief Mansur and Elisatris Gultom, *Cyber Law: Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, 2005, p. 112.

interconnected digital ecosystems: social media platforms, dating applications, and encrypted communication channels. Social media platforms (such as Facebook, Instagram, and TikTok) serve as expansive hunting grounds. Traffickers employ data-mining techniques and social engineering to identify the vulnerabilities of women and children.[9] By monitoring a target's digital footprint—such as posts expressing emotional distress, financial instability, or familial alienation—perpetrators can tailor their manipulative approaches. For instance, syndicates frequently deploy fraudulent job advertisements targeting economically vulnerable women, promising lucrative overseas employment. Once the victim engages, the recruitment transitions into a digital trap.[10]

Simultaneously, dating applications have become a prevalent vector for exploitation. Perpetrators create fabricated personas (a practice known as *catfishing*) to initiate romance scams. Through feigned romantic interest, the trafficker builds profound emotional reliance and trust with the victim. This phase, known as *cyber-grooming*, is highly systematic. It involves targeting, gaining trust, fulfilling an emotional or financial need, isolating the victim from their real-world support system, and ultimately transitioning to abuse or exploitation.[11] In the context of child exploitation, cyber-grooming often culminates in the production of child sexual abuse material (CSAM) or the coercion of the child into physical encounters. For women, the romance scam often pivots into debt bondage or forced prostitution, where the victim is psychologically coerced into traveling to a location controlled by the syndicate.[12]

To obscure these illicit operations, syndicates heavily rely on encrypted communication channels (such as WhatsApp, Telegram, or the Dark Web). Once initial contact is established on open platforms, the communication is swiftly moved to these end-to-end encrypted applications. This transition is a deliberate operational security measure designed to severe the digital evidence chain.[13] Encrypted channels provide a secure environment for traffickers to coordinate logistics, distribute explicit materials, and issue threats (such as *sextortion*—

[9] Budi Suharyanto. Tindak Pidana Teknologi Informasi (Cybercrime). *Raja Grafindo Persada: Jakarta*, 2014. p.40.
[10] Nurul Mutiara Aisyah; Erna Ewi; Fristia Berdian Tamza. Pemanfaatan Teknologi sebagai Sarana Viktimisasi dalam Cyber Grooming. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 2026, 4.3: 2880-2886.
[11] K Jaishankar. Cyber victimology: A new sub-discipline of the twenty-first century victimology. In: *An international perspective on contemporary developments in victimology: A festschrift in honor of Marc Groenhuijsen*. Cham: Springer International Publishing, 2020. p. 3-19.
[12] Rena Yulia, *Viktimologi: Perlindungan Hukum Terhadap Korban Kejahatan*, Graha Ilmu, Yogyakarta, 2010, p. 145.
[13] Wenggedes Frensh. Kelemahan Pelaksanaan Kebijakan Kriminal Terhadap Cyberbullying Anak Di Indonesia. *Indonesia Criminal Law Review*, 2022, 1.2: p.3.

threatening to release intimate images if the victim does not comply) without the immediate risk of surveillance by internet service providers or law enforcement agencies. Consequently, the digital footprints of the exploitation become functionally invisible, heavily complicating the evidentiary process required for conventional prosecution.[14]

### 3.1.2. The Anonymity and Accessibility Factors: A Theoretical Analysis

To fully comprehend why cyberspace has become the preferred domain for human trafficking syndicates, it is imperative to analyze the structural vulnerabilities of the digital landscape. The *Routine Activity Theory* (RAT), originally formulated by Lawrence E. Cohen and Marcus Felson, provides a robust theoretical framework for this analysis. According to RAT, a crime occurs when three elements converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian. When transposed into the digital realm—often referred to as *Routine Activity Theory in Cyberspace*—these elements elucidate how anonymity and accessibility create an environment ripe for digital exploitation.[15]

Firstly, the *motivated offender* in cyberspace is emboldened by unprecedented structural advantages. Trafficking syndicates are highly motivated by the low-risk, high-reward nature of digital crimes. The internet affords perpetrators absolute anonymity. Through the use of Virtual Private Networks (VPNs), proxy servers, and cryptocurrency transactions, syndicates can mask their identities, locations, and financial trails.[11] This anonymity dissolves the geographical boundaries that once restricted criminal enterprises, allowing a trafficker based in one continent to seamlessly exploit a victim in another. The digital shield drastically lowers the perceived risk of apprehension, thereby increasing the motivation to offend.

Secondly, the *suitable target* has become infinitely more accessible. The rapid digitalization of daily life means that vulnerable groups—specifically women and children—spend a significant portion of their routine activities online. The hyper-connectivity of modern society results in targets volunteering vast amounts of personal information into the public domain. In cyberspace, suitability is defined by digital vulnerability: a lack of digital literacy, a high degree of online social interaction, and emotional or economic susceptibility. Children playing online games or women seeking employment on unregulated forums inadvertently present themselves as highly visible and suitable targets to anonymous predators

[14] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Rajawali Pers, Jakarta, 2006, p. 95.
[15] Lawrence E Cohen.; Marcus Felson. Routine activity theory: A routine activity approach. In: *Criminology theory*. Routledge, 2015. p. 313-321.

prowling these digital spaces.[16]

Thirdly, and most critically, is the *absence of capable guardians*. In the physical world, capable guardians include parents, police officers, community members, and physical security systems. In cyberspace, the concept of a guardian is far more complex and often severely deficient. Capable guardians in the digital realm should theoretically include digital literacy education, robust platform moderation, algorithmic threat detection, and proactive cyber-patrols by law enforcement. However, the reality reveals a profound guardianship void. Social media platforms often prioritize user engagement over stringent security protocols, resulting in inadequate moderation of grooming behaviors. Parents are frequently ill-equipped to monitor or understand the encrypted digital lives of their children.[17] Furthermore, law enforcement agencies are consistently hindered by transnational jurisdictional complexities, a lack of advanced digital forensic capabilities, and the sheer volume of cyber-traffic.

When a motivated, anonymous syndicate (the offender) easily accesses a vulnerable, hyper-connected child or woman (the target) within an encrypted platform lacking adequate moderation or legal oversight (the absence of a capable guardian), digital exploitation is not merely possible; it is inevitable.

The intersection of these factors demonstrates that the "invisible footprints" of digital exploitation are the result of systemic technological vulnerabilities that syndicates actively exploit. The anonymity provides the shield, while the unparalleled accessibility provides the ammunition. Therefore, combating this modern manifestation of human trafficking requires a profound legal reconstruction. Law enforcement can no longer rely solely on physical interceptions; the legal system must be structurally upgraded to penetrate digital anonymity, enforce accountability upon digital platforms as capable guardians, and establish proactive cyber-victimology frameworks that recognize and mitigate the unique harms of digital exploitation.

### 3.2. The Normative Gap in Victim Protection within Pre-Existing Cyber Laws

[16] Rizwan Ullah; Tariq Zaman. Contextualizing Space Transition Theory: A Socio-technical Exploratory Study of Cybercrimes in Khyber Pakhtunkhwa. In: *Computational Intelligent Systems: Applications of AI and Machine Learning*. Singapore: Springer Nature Singapore, 2026. p. 261-297.

[17] Ridha Fahmi Ananda, et al. Perlindungan Hukum Terhadap Anak Sebagai Korban Kejahatan Pelecehan Seksual Dalam Perspektif Viktimologi. *Locus Journal of Academic Literature Review*, 2023, p.52-65.

Before the integration of the new National Criminal Code, the Indonesian legal system relied on a patchwork of specific regulations to address digital offenses and human trafficking. The primary instruments were Law Number 21 of 2007 on the Eradication of the Criminal Act of Trafficking in Persons (UU TPPO) and Law Number 11 of 2008 as amended by Law Number 19 of 2016 on Electronic Information and Transactions (UU ITE). However, a critical evaluation of these pre-existing laws reveals a severe normative gap, particularly regarding evidentiary standards and the protection of digital victim rights. These limitations severely hindered the state's capacity to intercept modern syndicates and mitigate the permanent harms caused by cyber-exploitation.

The core limitation of the pre-existing anti-trafficking framework lies in its conceptual dependency on physical, geographical modalities. Article 1 paragraph (1) of the UU TPPO defines human trafficking through acts such as "recruiting, transporting, harboring, sending, transferring, or receiving a person."[18] This definition is intrinsically tied to the requirement of physical movement (physical movement). In the context of conventional human trafficking, proving that a victim was transported from a village to an overseas destination was the primary evidentiary standard to establish the crime.

However, in the era of digital exploitation, this physical movement requirement becomes a major normative obstacle. Syndicates no longer need to physically transport victims to exploit them. Through the use of webcams, live streaming, and social media, victims—particularly children—can be sexually or economically exploited in situ, within the confines of their own homes.[19] Because the victim is never physically moved or transported across borders, prosecutors faced immense difficulties in applying the severe penalties of the UU TPPO. The evidentiary standards of the conventional framework were simply incompatible with the mechanics of digital exploitation.

Consequently, law enforcement agencies were often forced to rely on the UU ITE, specifically Article 27 paragraph (1) regarding the distribution of materials violating decency (muatan yang melanggar kesusilaan).[20] While the UU ITE successfully criminalized the transmission of the exploitation material, it failed to

[18] Karina Maulidia Kusuma, et al. Analisis Tindak Pidana Perdagangan Orang (TPPO) WNI Di Kamboja: Kronologi Dan Penanganan Hukum. *Causa: Jurnal Hukum dan Kewarganegaraan*, 2025, 14.3: p.71-80.

[19] Barda Nawai Arief. Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia. *PT Raja Grafindo Persada. Jakarta*, 2005. p. 20.

[20] Agus Santoso; Dyah Pratiwi. Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan Dalam Kegiatan Transaksi Elektronik Pasca Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Legislasi Indonesia*, 2018, 5.4: p.74-88.

conceptualize the act as human trafficking. The UU ITE is fundamentally a regulation on electronic transactions and content moderation, not a comprehensive human rights instrument designed to dismantle organized exploitation syndicates.[21] As a result, the intellectual masterminds who orchestrated and profited from the online exploitation often evaded the devastating corporate and financial sanctions inherent in anti-trafficking laws. They were merely treated as distributors of prohibited content, facing significantly lighter penalties, which failed to reflect the gravity of the organized exploitation they perpetrated.

The normative gap extends beyond the prosecution of perpetrators; it acutely affects the post-crime recovery of the victims. To understand this gap, one must apply the theoretical lens of Cyber-Victimology. In physical crimes, the victimization generally concludes once the victim is rescued from the exploitative environment. In cyberspace, however, victimization is perpetual. Digital footprints, such as exploitation videos, explicit photographs, or coercive communications, are infinitely replicable, globally distributable, and virtually indestructible.[22]

According to Cyber-Victimology, the nature of digital data creates a phenomenon of perpetual harm and revictimization. Every instance an exploitation video is downloaded, shared on a hidden forum, or re-uploaded to the internet, the victim is essentially re-trafficked and revictimized.[23] The trauma is not an isolated event but a continuous psychological assault, severely impending the victim's social reintegration and future livelihood.

The pre-existing procedural laws, including the conventional Criminal Procedure Code (KUHAP), lacked the structural capacity to address this perpetual digital harm. A critical omission in the conventional procedural framework was the absence of a swift, integrated mechanism for the "Right to be Forgotten" (Hak untuk Dilupakan) within the criminal justice process. While Article 26 of the UU ITE (as amended) introduced a rudimentary concept of deleting irrelevant electronic information, it was structured primarily as a civil or administrative remedy requiring a separate court order.[24] It was not seamlessly integrated as a

[21] Dikdik M. Arief Mansur and Elisatris Gultom, 2005, *Cyber Law: Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung, p. 88.
[22] Maskun, 2013, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, Kencana, Jakarta, p. 112.
[23] Ajeng Yuni Astari. Perdagangan Manusia di Balik Layar Aplikasi: Pelajaran Hukum dari Kasus MiChat. *Jurnal Hukum Lex Generalis*, 2025, 6.7. p.10.
[24] Yusuf Daeng, et al. Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of Social Science Research*, 2023, 3.6: p.2898-2905.

mandatory, immediate restorative sanction within criminal verdicts.

This resulted in a tragic reality: a cyber-trafficker could be arrested and imprisoned, but the digital evidence of the exploitation would remain accessible on servers worldwide, completely outside the control of the victim or local law enforcement.[25] The conventional procedural law focused exclusively on the physical confiscation of devices (such as laptops or servers) as evidence but provided no comprehensive, transnational legal avenue to compel digital platforms to permanently erase the victim's digital footprint. Without an operationalized Right to be Forgotten within the criminal restitution framework, the pre-existing laws offered no finality or true protection to the victims, condemning them to a lifetime of digital revictimization.

This normative gap underscores the absolute necessity for a legal reconstruction that transcends physical boundaries, integrating cyber-victimology principles directly into the substantive and procedural mechanisms of the new National Criminal Code.

### 3.3. Legal Reconstruction under the New National Criminal Code

The enactment of the new National Criminal Code (Law Number 1 of 2023), which officially took effect on January 2, 2026, serves as a watershed moment in Indonesian criminal jurisprudence. It systematically reconstructs the legal protection architecture, specifically addressing the normative gaps that previously left vulnerable groups exposed to digital exploitation. By recognizing the complexities of modern cyberspace, the new code provides prosecutors and judges with progressive legal instruments designed to penetrate digital anonymity and mandate comprehensive victim recovery.

A paramount breakthrough in the new National Criminal Code is the explicit codification of corporate criminal liability, which decisively expands the scope of criminalization to include digital facilitators and technology companies. Under the previous framework, prosecuting digital platforms or Internet Service Providers (ISPs) that facilitated or turned a blind eye to cyber-grooming and online trafficking was exceptionally difficult due to scattered regulations. The new code, however, definitively establishes that a corporation is an active subject of criminal law. This encompasses a wide array of legal entities, including limited liability companies, foundations, and unincorporated associations.

Articles 46 and 47 stipulate that a criminal act by a corporation is committed by

[25] Mahsun Ismail. Kebijakan Hukum Pidana cyberpornography terhadap perlindungan korban. *Jurnal Hukum Ekonomi Syariah*, 2018, 1.2: p.117-134.

management personnel holding functional positions, order givers, controllers, or beneficial owners who act for the benefit of the corporation. More importantly, Article 48 expands this liability significantly by establishing that a corporation can be held accountable if it fails to take the necessary steps to prevent the crime, mitigate its broader impacts, ensure legal compliance, and essentially allows the criminal act to occur within its ecosystem.

In the context of digital exploitation, this means that social media platforms, hosting providers, or dating applications can be indicted as corporate facilitators if they demonstrate gross negligence or willful blindness toward human trafficking activities on their networks.[26] If a platform lacks adequate moderation, ignores reports of child sexual abuse material (CSAM), or fails to implement basic safety protocols for vulnerable users, it fulfills the criteria of "allowing the crime to occur" under Article 48. Consequently, law enforcement can now impose severe corporate sanctions, ranging from massive fines to the suspension of business activities and permanent corporate dissolution, compelling tech entities to act as capable digital guardians.

Beyond corporate accountability, the legal reconstruction introduces a profound paradigm shift toward restorative justice, particularly addressing the perpetual harm inherent in cyber-victimization. The new National Criminal Code actively departs from purely retributive punishments by integrating corrective measures directly into the sentencing framework.

Article 103 of the new code outlines specific "actions" (tindakan) that can be imposed alongside principal penalties, which explicitly include "repairing the consequences of the criminal act" (perbaikan akibat Tindak Pidana). Article 108 further defines this action as a concrete effort to restore or repair the damages caused by the crime to their original state. This provision is revolutionary for cyber-victimology. Previously, victims of digital exploitation had to pursue separate, arduous civil lawsuits to demand the removal of explicit content or digital footprints.

Now, judges possess the statutory authority to order the forced deletion of digital footprints as a direct criminal sanction ("tindakan perbaikan") against the convicted trafficker or the facilitating corporation. This legally operationalizes the "Right to be Forgotten" within the criminal procedure, allowing the state to forcefully erase the victim's data from servers and search indices as part of the penal execution. By embedding digital restitution into the judicial verdict, the new code ensures that the cessation of digital revictimization is an automatic and

[26] Nataliya Mentukh; Oksana Shevchuck. Protection of information in electronic registers: Comparative and legal aspect. *Law, Policy and Security*, 2023, 1.1: p. 4-17.

mandatory outcome of the justice process, thereby providing absolute and proactive protection for vulnerable groups.

To illustrate this systemic transformation, the following table summarizes the comparative shift in the legal protection framework against digital exploitation:

Table 1. Paradigm Shift in Victim Protection against Digital Exploitation

| Framework | Evidence Focus | Protection Scope | Corporate Liability |
|---|---|---|---|
| Previous System | Physical Movement | Reactive / Physical Safety | Limited / Scattered |
| New National Code | Digital Footprints | Proactive / Digital Restitution | Explicitly Codified |

Sumber: Processed secondary data, 2026.

### 3.4. Formulating a Cyber-Victimology Framework and Transnational Enforcement

While the substantive legal reconstruction provided by the new National Criminal Code (KUHP Nasional) establishes a formidable foundation for combating digital exploitation, theoretical laws alone are insufficient without adaptive operational frameworks. The transition from physical to digital crimes necessitates a corresponding evolution in procedural execution and international collaboration. Formulating a practical "Cyber-Victimology" framework and enhancing transnational enforcement are imperative operational solutions to complement the new substantive laws. This section delineates the practical strategies required to integrate digital victim protection into criminal procedures and addresses the complex jurisdictional challenges of borderless cyber-syndicates.

Cyber-Victimology is an emerging criminological sub-discipline that specifically studies the victimization process within the digital environment, acknowledging that digital harms are often perpetual, borderless, and infinitely replicable.[27] To effectively operationalize the new National Criminal Code, law enforcement agencies must integrate cyber-victimology principles directly into their standard operating procedures (SOPs) during the investigation, prosecution, and recovery phases.

The foremost operational solution is the establishment of "Victim-Centric Digital Forensic Guidelines." In conventional digital forensics, the primary objective is the extraction and preservation of electronic evidence to secure a conviction. However, when dealing with cases of online exploitation, child sexual abuse material (CSAM), or cyber-grooming, the raw extraction process can inadvertently lead to secondary victimization. Victims are often forced to recount

[27] Maskun, 2013, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, Kencana, Jakarta, p. 115.

their trauma or have their deeply intimate and exploitative digital records excessively reviewed by numerous officers.[28] A cyber-victimology framework requires that forensic extractions are conducted using highly specialized, privacy-preserving algorithms that limit human exposure to the sensitive materials. The procedural law must mandate that only certified, specialized cyber-investigators with trauma-informed training are permitted to handle such digital evidence.

Furthermore, the operationalization of the "Right to be Forgotten" (Hak untuk Dilupakan) must be streamlined within the criminal procedure. Under the new KUHP Nasional, judges have the authority to impose "actions" (tindakan) to repair the consequences of a crime (Pasal 103). Procedurally, this must translate into immediate, court-ordered injunctions issued directly to Internet Service Providers (ISPs), search engines, and social media platforms to permanently erase the victim's digital footprint globally.[3] Currently, the process of taking down exploitative content is often treated as a separate administrative or civil hurdle. A practical cyber-victimology framework would empower criminal court judges to embed absolute data-erasure mandates directly into the final criminal verdict, compelling corporate entities to deploy algorithmic hashing (such as PhotoDNA) to prevent the future re-uploading of the specific exploitative materials.[29]

Additionally, the role of the Witness and Victim Protection Agency (LPSK) must be structurally expanded to include "Digital Psychological Recovery." The trauma inflicted by digital exploitation is distinct; victims live in constant fear of their digital footprints resurfacing. The procedural framework must facilitate immediate psychological interventions tailored for cyber-trauma, ensuring that the victim's digital identity and privacy are fully insulated throughout and after the trial process.[30]

The second operational imperative is addressing the transnational nature of digital exploitation. Human trafficking syndicates operating in the digital sphere deliberately exploit jurisdictional boundaries. A typical modus operandi may involve perpetrators based in Indonesia targeting victims domestically, but

[28] Rahma Mentari. Mewujudkan Keadilan: Perlindungan Hukum bagi Perempuan Korban KDRT dalam Sistem Peradilan Pidana Indonesia. *SPECTRUM: Journal of Gender and Children Studies*, 2024, 4.1: p.32-45.
[29] Karunia Fitria Ramaadani; M. Darin Arif. Analisis Yuridis Pengaturan Hak Untuk Dilupakan (Right To Be Forgotten) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Legacy: Jurnal Hukum dan Perundang-Undangan*, 2023, 3.1: p.18-41.
[30] Cheryl Michaelia Ongkowiguno; Irsyaf Marsal. Politik hukum perlindungan data pribadi dalam layanan publik digital di Indonesia. *Judge: Jurnal Hukum*, 2025, 6.04: 1321-1326.

utilizing encrypted communication servers hosted in Eastern Europe, and laundering the proceeds through cryptocurrency exchanges in the Caribbean. Conventional law enforcement mechanisms, which are strictly bound by territorial sovereignty, are severely handicapped in this environment.

To complement the substantive sharpness of the new KUHP Nasional, Indonesia must aggressively optimize its transnational enforcement strategies. The traditional mechanism for cross-border evidence gathering is the Mutual Legal Assistance (MLA) treaty. However, conventional MLA processes are notoriously bureaucratic, reliant on diplomatic channels, and excessively time-consuming—often taking months or years to execute. In the realm of cybercrime, where digital evidence can be deleted, encrypted, or migrated to a different server with a single keystroke, the traditional MLA process is fundamentally obsolete.

A practical operational solution is the modernization of bilateral and multilateral digital treaties, moving towards "Direct Digital Evidence Sharing." Indonesia must actively engage in and ratify progressive international frameworks, such as the Budapest Convention on Cybercrime, which facilitates rapid, 24/7 cross-border police-to-police cooperation for the preservation of volatile electronic evidence. By adopting a modernized transnational framework, Indonesian law enforcement can bypass sluggish diplomatic channels when requesting urgent data preservation orders from foreign jurisdictions.

Moreover, transnational enforcement must heavily integrate Public-Private Partnerships (PPP). The majority of digital exploitation occurs on infrastructure owned by multinational technology giants (e.g., Meta, Google, Telegram). Establishing direct, legally binding compliance channels between Indonesian law enforcement and the legal departments of these global tech entities is vital. Instead of relying solely on state-to-state treaties, operational frameworks should include specialized portals that allow Indonesian authorities to directly compel foreign-based tech platforms to freeze accounts, preserve IP logs, and takedown exploitative networks in real-time, backed by the expansive corporate liability provisions of the new KUHP Nasional.

To systematically capture these operational shifts, the following formulation table compares the pre-existing enforcement rules with the proposed cyber-victimology and transnational enforcement ideas based on the newly enacted legal framework:

**Table 2.** Formulation of Procedural and Operational Enforcement Frameworks

| Aspect | Pre-Existing Framework (Conventional Rules) | Proposed Framework (Cyber-Victimology & KUHP Nasional) |
|---|---|---|
| **Evidence Handling** | Focused solely on data extraction for conviction; high risk of secondary victimization during forensic analysis. | Trauma-informed digital forensics; limited human exposure to sensitive data; strict privacy preservation. |
| **Digital Restitution** | "Right to be Forgotten" treated as a separate administrative/civil process (UU ITE); slow and detached from criminal verdicts. | "Right to be Forgotten" operationalized as an automatic criminal sanction (Tindakan Perbaikan); mandatory algorithmic hashing by ISPs. |
| **Victim Recovery** | Physical and physical-psychological protection (LPSK); limited understanding of perpetual digital trauma. | Specialized Digital Psychological Recovery; proactive insulation of digital identity; continuous monitoring of digital footprint resurfacing. |
| **Cross-Border Evidence** | Heavy reliance on traditional, bureaucratic Mutual Legal Assistance (MLA) treaties via diplomatic channels. | 24/7 Direct Digital Evidence Sharing; adoption of progressive international cybercrime protocols (e.g., Budapest Convention). |
| **Platform Engagement** | Reactive takedown requests; weak enforcement against foreign-based multinational tech companies. | Direct Public-Private Partnerships (PPP); legally binding, real-time compliance portals backed by corporate criminal liability. |

Sumber: Processed secondary data, 2026.

In conclusion, the efficacy of dismantling digital human trafficking syndicates does not rest solely on the existence of the new National Criminal Code. It requires a holistic reconstruction of the operational machinery. By formulating a strict cyber-victimology framework within procedural law and modernizing transnational digital cooperation, the Indonesian justice system can effectively bridge the gap between substantive legal theories and the practical realities of enforcing absolute protection for vulnerable groups in cyberspace.

## 4. Conclusion

The rapid migration of human trafficking and exploitation into the digital realm necessitates a profound legal reconstruction to safeguard vulnerable groups from invisible cyber-threats. The enactment of the new National Criminal Code (Law Number 1 of 2023) fundamentally addresses the normative gaps of pre-existing frameworks by explicitly expanding criminal liability to corporate entities and digital facilitators, while shifting the penal paradigm toward restorative justice through corrective judicial actions. However, to effectively dismantle transnational cyber-syndicates and mitigate perpetual digital revictimization, this substantive legal foundation must be systematically operationalized through a specialized cyber-victimology framework within procedural law. Therefore, it can be concluded that absolute protection in cyberspace demands the integration of trauma-informed digital forensics, the automatic execution of the "Right to be

Forgotten" as a mandatory criminal sanction, and the modernization of direct transnational digital evidence sharing, ensuring that the Indonesian justice system is structurally equipped to proactively intercept and eradicate borderless technological threats.

## 5. References

**Journal:**

Agus Santoso and Dyah Pratiwi, Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan Dalam Kegiatan Transaksi Elektronik Pasca Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Jurnal Legislasi Indonesia, Vol 5, No 4 (2018);

Ajeng Yuni Astari, Perdagangan Manusia di Balik Layar Aplikasi: Pelajaran Hukum dari Kasus MiChat, Jurnal Hukum Lex Generalis, Vol 6, No 7 (2025);

Cheryl Michaelia Ongkowiguno and Irsyaf Marsal, Politik hukum perlindungan data pribadi dalam layanan publik digital di Indonesia, Judge: Jurnal Hukum, Vol 6, No 4 (2025);

Eka Fitri Lestari, Rahmayanti, and Donly Calner Aruan, Problematika Pembuktian Digital dalam Penegakan Hukum Tindak Pidana Siber di Indonesia, Dewantara: Jurnal Pendidikan Sosial Humaniora, Vol 5, No 2 (2026);

Karina Maulidia Kusuma, et al., Analisis Tindak Pidana Perdagangan Orang (TPPO) WNI Di Kamboja: Kronologi Dan Penanganan Hukum, Causa: Jurnal Hukum dan Kewarganegaraan, Vol 14, No 3 (2025);

Karunia Fitria Ramaadani and M. Darin Arif, Analisis Yuridis Pengaturan Hak Untuk Dilupakan (Right To Be Forgotten) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Legacy: Jurnal Hukum dan Perundang-Undangan, Vol 3, No 1 (2023);

Mahsun Ismail, Kebijakan Hukum Pidana cyberpornography terhadap perlindungan korban, Jurnal Hukum Ekonomi Syariah, Vol 1, No 2 (2018);

**LICS 2026**
**Topic:** *Strengthening Legal Frameworks for Combating Human Trafficking and Enhancing Protection of Women and Children*

Nataliya Mentukh and Oksana Shevchuck, Protection of information in electronic registers: Comparative and legal aspect, Law, Policy and Security, Vol 1, No 1 (2023);

Nurul Mutiara Aisyah, Erna Ewi, and Fristia Berdian Tamza, Pemanfaatan Teknologi sebagai Sarana Viktimisasi dalam Cyber Grooming, Al-Zayn: Jurnal Ilmu Sosial & Hukum, Vol 4, No 3 (2026);

Rahma Mentari, Mewujudkan Keadilan: Perlindungan Hukum bagi Perempuan Korban KDRT dalam Sistem Peradilan Pidana Indonesia, SPECTRUM: Journal of Gender and Children Studies, Vol 4, No 1 (2024);

Reno Apri Dwijayanto, Tinjauan yuridis perbandingan KUHP lama dan KUHP baru dalam sistem peradilan pidana Indonesia, Jurnal Sosial Teknologi, Vol 6, No 2 (2026);

Rian Rusmana Putra, et al., Analisis Penegakan Hukum Terhadap Tindak Pidana Perdagangan Orang di Kamboja dalam Perspektif Hukum Pidana Nasional, Jurnal USM Law Review, Vol 9, No 2 (2026);

Ridha Fahmi Ananda, et al., Perlindungan Hukum Terhadap Anak Sebagai Korban Kejahatan Pelecehan Seksual Dalam Perspektif Viktimologi, Locus Journal of Academic Literature Review, Vol 2, No 2 (2023);

Sigid Suseno, et al., Cybercrime in the new criminal code in Indonesia, Cogent Social Sciences, Vol 11, No 1 (2025);

Wan Rahmat Kurniawan, Alwan Hadiyanto, and Ciptono, Tindak pidana perdagangan orang dalam perspektif tindak pidana pencucian uang di Indonesia, Jurnal USM Law Review, Vol 7, No 2 (2024);

Wenggedes Frensh, Kelemahan Pelaksanaan Kebijakan Kriminal Terhadap Cyberbullying Anak Di Indonesia, Indonesia Criminal Law Review, Vol 1, No 2 (2022);

Yusuf Daeng, et al., Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi, Innovative: Journal of Social Science Research, Vol 3, No 6 (2023);

Barda Nawawi Arief, 2006, Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia, Rajawali Pers, Jakarta;

Barda Nawawi Arief, 2022, Kebijakan Hukum Pidana dalam Penanggulangan Cybercrime, Pustaka Magister, Semarang;

Budi Suharyanto, 2014, Tindak Pidana Teknologi Informasi (Cybercrime), Raja Grafindo Persada, Jakarta;

Dikdik M. Arief Mansur and Elisatris Gultom, 2005, Cyber Law: Aspek Hukum Teknologi Informasi, Refika Aditama, Bandung;

H. Siswanto Sunarso, 2022, Viktimologi dalam sistem peradilan pidana, Sinar Grafika, Jakarta;

K. Jaishankar, 2020, Cyber victimology: A new sub-discipline of the twenty-first century victimology, Springer International Publishing, Cham;

Lawrence E. Cohen and Marcus Felson, 2015, Routine activity theory: A routine activity approach, Routledge, London;

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

Rena Yulia, 2010, Viktimologi: Perlindungan Hukum Terhadap Korban Kejahatan, Graha Ilmu, Yogyakarta;

Rizwan Ullah and Tariq Zaman, 2026, Contextualizing Space Transition Theory: A Socio-technical Exploratory Study of Cybercrimes in Khyber Pakhtunkhwa, Springer Nature Singapore, Singapore;

**Regulations:**

Law Number 1 of 2023 concerning the Criminal Code (National Criminal Code);

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

Law Number 11 of 2008, as amended by Law Number 19 of 2016, concerning Electronic Information and Transactions;