



LICS 2026

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

Reconstructing Indonesian Cyber Law to Combat AI-Facilitated Trafficking of Women and Children

Ganesh Deo Gangga

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,

E-mail: ganeshgangga35@gmail.com

Abstract. *This study examines the inadequacy of Indonesia's cyber-law framework in confronting human trafficking and the online exploitation of women and children that is increasingly facilitated by artificial intelligence (AI). Traffickers now exploit social media, deepfake, voice synthesis, and large language models for victim profiling, cyber-recruitment, online scam operations, and coercive control, while Law No. 1 of 2024 on Electronic Information and Transactions, the Personal Data Protection Law, the Anti-Trafficking Law, and the Child Protection Law have not specifically governed algorithmic accountability and platform due diligence. A juridical-normative approach was employed, using statutory, conceptual, and comparative analyses of secondary legal materials, examined prescriptively and qualitatively. The findings show that the protection gap originates from normative disharmony, the absence of AI-specific rules, weak cross-border digital-evidence mechanisms, and victim-protection schemes that are not yet trauma-sensitive. This study proposes a legal reconstruction integrating ethical AI governance, mandatory platform accountability, and a permissioned-blockchain mechanism for digital-evidence integrity and victim digital identity, grounded in human-rights principles and the value of Pancasila justice, in order to strengthen prevention and the recovery of women and child victims.*

Keywords: *Artificial Intelligence; Cyber Law; Human Trafficking; Legal Reconstruction; Protection of Women and Children.*

LICS 2026

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

1. Introduction

Human trafficking is a transnational organized crime that not only violates positive law but also undermines individual dignity and autonomy, with women and children being the most vulnerable groups. Indonesia has adopted many elements of the Palermo Protocol through Law No. 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, but its implementation continues to be hampered by weak law enforcement, minimal inter-agency coordination, and limited budgets for victim protection.¹ This gap between normative idealism and the reality of implementation is what has kept eradication efforts from being optimal amidst the ever-evolving nature of crime. This discrepancy is evident at the level of legal substance, enforcement structures, and the legal culture of society, which is not yet fully aware of new forms of exploitation.²

The Indonesian context places additional pressure on this issue. As an archipelagic nation with a large population, high internet penetration, and inter-regional economic disparities, Indonesia presents a vulnerable environment for trafficking networks to exploit to recruit victims from groups facing economic hardship. The promise of lucrative jobs serves as an effective lure amidst limited employment opportunities, while a lack of digital literacy makes it difficult for potential victims to distinguish legitimate offers from traps. In such a landscape, the law is required to serve not only as a punitive instrument but also as a protective framework capable of addressing society's structural vulnerabilities to increasingly sophisticated modes of exploitation.

Digital transformation has transformed human trafficking into a crime based on online platforms. Recruitment of victims is now often conducted through social media, offering fictitious, high-paying jobs that ultimately lead to forced labor in online scams, as illustrated by the wave of cases of Indonesian citizens trapped in Myanmar and surrounding countries.³ This digital method complicates authorities' investigations because exploitation isn't always accompanied by visible physical violence, so it's often misclassified as a regular immigration or employment issue

¹Ni Kadek Puspawati, Implementation of the Anti-Trafficking Policy from an International and National Legal Perspective, Indonesian Journal of Law and Justice, Vol. 2 No. 3 (2025), p. 9, <https://doi.org/10.47134/ijlj.v2i3.3661>.

²*Ibid.*, p. 10.

³Satriya Aldi Putrazta, Legal Protection for Victims of Cross-Border Human Trafficking Under the Guise of Digital Job Vacancies in Myanmar, Majelis: Jurnal Hukum Indonesia, Vol. 2 No. 4 (2025), p. 93, <https://doi.org/10.62383/majelis.v2i4.1204>.

LICS 2026

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

rather than a human trafficking crime. As a result, victims who are actually being exploited may be treated as immigration administrative violators.⁴

The challenge intensifies when artificial intelligence is integrated into human trafficking operations. Large language models, voice synthesis, and deepfakes allow perpetrators to profile potential victims, conduct personalized social engineering for recruitment, and disguise their tracks and establish control over them.⁵ This automation increases the scale of the crime because one perpetrator can reach thousands of targets in a short time, so that the character of human trafficking shifts from a labor-intensive crime to a technology-intensive crime.⁶

The use of AI to combat human trafficking is not without ethical consequences. Implementing surveillance technology without human rights principles risks disproportionate burdens on already vulnerable groups, ranging from over-surveillance to misidentification.⁷ This tension between the goal of protection and the potential for privacy violations demands a careful balance so that technological solutions do not create new human rights issues.⁸

The specific impact on women is evident in the surge in online gender-based sexual violence that exploits advances in information technology as a means of threats, blackmail, and distribution of content without consent.⁹ Female victims not only suffer material losses, but also prolonged psychological trauma and social stigma that complicate the recovery process.¹⁰

Children, especially those whose figures are exposed on digital channels, face the risk of sexualization and image abuse through deepfakes, thereby losing control of their identity and digital footprint.¹¹ Without adequate digital trace removal

⁴*Ibid.*, p. 95.

⁵Joel Levesque, The AI-Enhanced Trafficking Threat: Examining the Technological Evolution of Trafficking in Persons Operations with AI Tools, *Journal of Human Trafficking*, advanced online publication (2025), p. 3, <https://doi.org/10.1080/23322705.2025.2572911>.

⁶*Ibid.*, p. 5.

⁷Julia Deeb-Swihart, Alex Endert, and Amy Bruckman, Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective, *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6 CSCW2 (2022), p. 8, <https://doi.org/10.1145/3555186>.

⁸*Ibid.*, p. 12.

⁹Ni Putu Lina Sudiyawati and I Ketut Mertha, Cybercrime in the Context of Online Gender-Based Sexual Violence in Indonesia, *Kertha Semaya*, Vol. 10 No. 4 (2022), p. 852, <https://doi.org/10.24843/ks.2022.v10.i04.p11>.

¹⁰*Ibid.*, p. 855.

¹¹Muhammad Deckri Algamar and Aliya Ilysia Irfana Ampri, The Right to Be Forgotten: Erasing Digital Traces as Protection for Child Celebrities from the Dangers of Deepfakes, *Jurnal Yustika*:

LICS 2026

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

mechanisms, manipulated images of children can be disseminated and reproduced indefinitely, extending victimization far beyond the initial event.¹²

Indonesia's existing legal framework Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, Law No. 27 of 2022 concerning Personal Data Protection, and Law No. 35 of 2014 concerning Child Protection does provide a basic foundation for protecting digital spaces. However, these regulations do not specifically address the issues of automated decision-making and algorithmic accountability, leaving loopholes for AI to be exploited.¹³ This regulatory gap is a structural weakness in combating AI-based crimes targeting women and children.¹⁴

On the victim side, protection mechanisms are still ineffective. Cybercrime victims often experience secondary victimization because existing legal frameworks have not been translated into truly victim-friendly procedures.¹⁵ A similar situation is seen in migrant workers who are vulnerable to trafficking, where the state's protection system from the departure process to the destination country still needs to be strengthened to prevent it becoming a loophole for forced recruitment.¹⁶

At the same time, technology shouldn't be viewed solely as a threat. Deep learning and AI-based analytics have proven potential for identifying patterns and anomalies indicative of human trafficking, from suspicious online advertisements to unusual financial transactions, thus becoming tools for prevention and early detection.¹⁷ Based on this paradox, this study aims to analyze the weaknesses of Indonesia's cyber legal framework in addressing AI-facilitated trafficking of women and children, while simultaneously formulating a legal reconstruction that

Media Hukum dan Keadilan, Vol. 25 No. 1 (2022), p. 30, <https://doi.org/10.24123/yustika.v25i01.5091>.

¹²*Ibid.*, p. 33.

¹³Loso Judijanto and Rabith Madah Khulaili Harsya, Ethics and Law in the Use of Artificial Intelligence on Digital Privacy in Indonesia, *Sanskara Hukum dan HAM*, Vol. 3 No. 3 (2025), p. 143, <https://doi.org/10.58812/shh.v3i03.543>.

¹⁴*Ibid.*, p. 145.

¹⁵An Nisya Nursabilah, et al., Legal Protection for Victims of Cyber Scam Crimes and Their Impact on Victims as a Form of Secondary Victimization, *Innovative Law: Journal of Social Law and Humanities*, Vol. 2 No. 3 (2025), p. 175, <https://doi.org/10.62383/humif.v2i3.1912>.

¹⁶M. Nizar, A. Inayah, and AT Dwijono, Strengthening the Role of Government through Legal Protection for Indonesian Migrant Workers, *SOCIOLOGY: Scientific Journal of Social and Cultural Studies*, Vol. 20 No. 2 (2018), p. 98, <https://doi.org/10.23960/sosiologi.v20i2.10>.

¹⁷Amina Catherine Ijiga, et al., Advanced Surveillance and Detection Systems Using Deep Learning to Combat Human Trafficking, *Magna Scientia Advanced Research and Reviews*, Vol. 11 No. 1 (2024), p. 270, <https://doi.org/10.30574/msarr.2024.11.1.0091>.

LICS 2026

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

integrates ethical AI governance and blockchain mechanisms to strengthen prevention and victim protection.

The urgency of this study stems from the fact that the pace of technological innovation far outpaces the pace of lawmaking. While human traffickers have leveraged recruitment automation, generative AI-based identity forgery, and cross-jurisdictional encryption to disguise their tracks, available legal tools still rely on conventional crime paradigms. As a result, a structural gap has emerged between the reality of digital *modus operandi* and the state's normative capacity to respond. This gap cannot be closed simply by stricter law enforcement; it also demands a renewed conceptual framework for how the law views non-human actors, autonomous systems, and evidence generated by algorithmic processes.

The approach offered in this paper is integrative and goes beyond criticizing the lack of norms. The author argues that the reconstruction of cyber law must simultaneously link three layers of protection: prevention through accountable technology governance, proof through ensuring the integrity of electronic evidence, and redress through victim-centered mechanisms. These three layers must be woven into a coherent framework rooted in the Pancasila values of justice, so that technology is positioned not as an end in itself but as a means to uphold the dignity of women and children, who are the primary targets of exploitation. This framework of thought is the common thread throughout the discussion in the following sections.

This study is relevant to collective efforts to combat human trafficking and strengthen the protection of women and children, as it positions these groups as those most impacted by the shift in crime modes to the digital realm. Women and children face multiple vulnerabilities: socially, they are often in a weak bargaining position, economically, they are the targets of false job promises, and digitally, they are vulnerable to manipulation utilizing advanced technology. Therefore, reforming cyber law cannot be separated from the perspective of gender and child protection. Each recommendation proposed in this paper is tested for its relevance to the actual needs of these vulnerable groups, so that technology and law truly work to protect, rather than add to the burden on those already marginalized.

2. Research Methods

This research uses a normative legal research method (juridical-normative), namely research that examines law as norms, principles, and doctrines contained

LICS 2026

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

in legal materials, not as empirical social phenomena.¹⁸ Normative research places legal materials as the main object of study, so that analysis is focused on the coherence, synchronization, and completeness of applicable norms.¹⁹

The approaches used are the statute approach, the conceptual approach, and the comparative approach to compare the effectiveness of legal frameworks between jurisdictions in the context of cross-border enforcement.²⁰ The conceptual approach is used to explore legal doctrines and concepts regarding algorithmic liability, victim protection, and the integrity of electronic evidence, while the legislative approach examines the consistency between relevant regulations.²¹

The data sources are secondary data consisting of primary legal materials (relevant laws and regulations, including Law No. 21 of 2007, Law No. 1 of 2024, Law No. 27 of 2022, Law No. 35 of 2014, and Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence), secondary legal materials in the form of scientific journals and legal literature, and tertiary legal materials as supporting materials. Legal materials were collected through literature and documentation studies, then inventoried and classified according to the legal issues being studied. The research specifications are prescriptive, and all materials are analyzed qualitatively to obtain arguments and conclusions that systematically answer the problems.

The analysis is conducted by sequentially linking three layers of study. First, the weaknesses of the applicable legal framework are identified by examining gaps and disharmonies in norms. Second, the relevant concepts and doctrines are explored in the legal literature and regulatory practices in comparative jurisdictions. Third, the formulation of a prescriptive normative reconstruction in response to the identified weaknesses. This process ensures that the recommendations proposed are not speculative but rather emerge from a careful diagnosis of the actual legal issues. Thus, the research conclusions demonstrate a logical connection between the problem formulation, findings, and recommendations that can be methodologically justified. The comparative approach serves as a mirror for assessing the feasibility of adaptation, rather than as a basis for the raw transplantation of foreign norms, ensuring that the study results remain rooted in the context and values of Indonesian national law.

¹⁸Soerjono Soekanto and Sri Mamudji, *Normative Legal Research: A Brief Review*, Rajawali Pers, Jakarta, 2015, p. 13.

¹⁹*Ibid.*, p. 15.

²⁰Peter Mahmud Marzuki, *Legal Research*, Revised Edition, Kencana, Jakarta, 2021, p. 133.

²¹*Ibid.*, p. 137.

LICS 2026

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

3. Results and Discussion

3.1. Weaknesses in Indonesia's Cyber Legal Framework in Addressing Artificial Intelligence-Facilitated Trafficking of Women and Children

The first root of the problem is disharmony and a lack of norms. Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law and Law No. 27 of 2022 concerning Personal Data Protection provide the foundation for protecting digital activities and data, but neither explicitly addresses the dimensions of artificial intelligence, such as automated decision-making and algorithmic accountability.²² The absence of norms that specifically impose transparency and accountability obligations on developers and administrators of AI systems creates a gray area that can be exploited by criminals.²³

This gap directly impacts the handling of deepfakes. When manipulative content is used as a means of cybercrime targeting women and children, law enforcement can only rely on general provisions not designed for generative technology, making attribution of responsibility unclear and proving malicious intent difficult.²⁴ The easily reproducible and disseminated nature of deepfakes across platforms complicates the identification of the original perpetrator, while victims already suffer reputational and psychological damage.²⁵

This ambiguity is exacerbated by the evolving *modus operandi*. Perpetrators are leveraging AI for three stages simultaneously: identifying potential victims, recruiting through personalized social engineering, and controlling and exploiting victims with the help of deepfakes and voice synthesis.²⁶ The automation of each stage makes crimes faster, cheaper, and harder to trace, so that legal frameworks that still rely on conventional methods are left behind.²⁷

In the practice of cross-border human trafficking under the guise of digital job vacancies, elements of recruitment, deception, harboring, and forced labor exploitation are fulfilled, but supervision of digital recruitment remains

²²LoSo Judijanto and Rabith Madah Khulaili Harsya, *Op.Cit.*, p. 145.

²³*Ibid.*, p. 146.

²⁴Fabrizio Richardo Marvil Wanggai, Made Sugi Hartono, and Ni Putu Ega Parwati, Normative Analysis of the Spread of Deepfakes as a Form of Cybercrime in Indonesia, *Majelis: Jurnal Hukum Indonesia*, Vol. 3 No. 1 (2026), p. 124, <https://doi.org/10.62383/majelis.v3i1.1509>.

²⁵*Ibid.*, p. 126.

²⁶Joel Levesque, *Op.Cit.*, p. 6.

²⁷*Ibid.*, p. 7.

LICS 2026

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

weak.²⁸ Jurisdictional limitations and suboptimal cross-border cooperation have hampered the handling of cases like this at the stage of providing evidence and repatriating victims, especially when the perpetrator and server are located outside of Indonesia.²⁹

The third weakness lies in victim protection and digital evidence. Cybercrime victims are vulnerable to secondary victimization because protection mechanisms are not recovery-oriented, while law enforcement often lacks empathy and digital literacy in handling cases.³⁰ The heavy burden of proof is placed on the victims, even though they are the ones who have the most difficulty accessing and securing electronic traces.³¹

In cases of online gender-based sexual violence, female victims face double barriers: social stigma and the difficulty of providing valid and complete electronic evidence.³² The absence of specific technical standards for handling electronic evidence is a vulnerable point that perpetrators exploit to delete or manipulate digital traces.³³

Fourth, the structural vulnerability of women and children exacerbates the impact. Gender inequality, poverty, and lack of digital literacy make them easy targets for criminal networks, including those involved in the trafficking of migrant workers who travel through unofficial channels.³⁴ Weak protection at the point of departure extends the chain of vulnerability all the way to the destination country, where victims often lose documents and access to communications.³⁵

Without harmonization of legal definitions and strengthening of law enforcement capacity as required by international standards, protection remains reactive and partial.³⁶ The exploitation of children's images through generative technologies can even continue indefinitely if there is no adequate mechanism for erasing digital traces, thereby failing the state to fulfill its long-term protection obligations towards children.³⁷

²⁸Satriya Aldi Putrazta, Op.Cit., p. 97.

²⁹*Ibid.*, p. 99.

³⁰An Nisya Nursabilah, et al., Op.Cit., p. 178.

³¹*Ibid.*, p. 180.

³²Ni Putu Lina Sudiyawati and I Ketut Mertha, Op.Cit., p. 856.

³³*Loc.Cit.*

³⁴M. Nizar, A. Inayah, and AT Dwijono, Op.Cit., p. 101.

³⁵*Ibid.*, p. 103.

³⁶Ni Kadek Puspawati, Op.Cit., p. 11.

³⁷Muhammad Deckri Algamar and Aliya Ilysia Irfana Ampri, Op.Cit., p. 35.

LICS 2026

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

Doctrinally, this weakness can be explained through the principle of *lex specialis derogat legi generali*, which cannot function optimally when specific norms regarding artificial intelligence do not yet exist. Law enforcement is forced to relegate AI-based acts to general articles that are not designed to address the nature of generative technology, making it difficult to prove the element of fault and the causal relationship between the algorithm's output and the victim's losses. The problem is further complicated by the distributed nature of responsibility in the AI ecosystem: model developers, training data providers, platform operators, and end users each contribute to the final outcome, while Indonesian criminal law remains grounded in the concept of a clearly identifiable single actor. Without an adaptive framework of accountability, the gap for impunity will continue to open.

From a comparative perspective, several jurisdictions have moved toward risk-based regulation, imposing transparency and due diligence obligations on high-risk AI systems, and establishing strict data protection obligations as a prerequisite for processing personal information. Such an approach is relevant for adaptation to Indonesia's civil law legal tradition, provided it is tailored to the domestic institutional context and enforcement capacity. Adaptation does not mean a crude transplant, but rather a harmonization that maintains coherence with national legal principles and constitutional values. In the context of trafficking in women and children, this risk-based regulation is crucial so that the heaviest compliance burden is allocated to systems that have the greatest potential to facilitate exploitation, rather than being imposed on all operators.

The evidentiary dimension presents its own challenges. Procedural law recognizes electronic evidence, but does not yet provide standard technical guidelines for obtaining, storing, and testing the integrity of digital data originating from AI-based systems. As a result, the admissibility and evidentiary weight of electronic evidence depend heavily on the judge's discretionary interpretation, which can vary from case to case. This uncertainty harms female and child victims, who generally lack the resources to hire digital forensic experts, and also allows perpetrators to challenge the integrity of evidence. Standard standards for handling electronic evidence are thus an urgent need, linking substantive issues with enforcement structures.

Weaknesses in the structural dimension are exacerbated by the transboundary nature of these crimes. Trafficking networks often operate servers, payment channels, and recruitment accounts in jurisdictions different from those of the victims, thus conflicting with the limitations of national law enforcement regarding territorial sovereignty. Existing mutual legal assistance mechanisms between countries are slow and formalistic, while digital evidence is easily lost and altered.



LICS 2026

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

Without a more agile cooperation framework and standardized evidence-sharing channels, perpetrators can exploit jurisdictional loopholes to escape accountability. This issue underscores the point that domestic legal reform will not be optimal unless it is accompanied by a strengthening of concrete and operational international cooperation.

Budget and human resource constraints further exacerbate structural weaknesses. Addressing cybercrime facilitated by artificial intelligence requires scarce and expensive digital forensic expertise, while the distribution of such capacity is uneven between the central and regional levels. Many local law enforcement units lack the equipment or personnel capable of reliably extracting and analyzing electronic evidence. This capacity imbalance makes case handling highly dependent on geographic location, placing victims in areas with limited infrastructure at greater risk of injustice. Without serious investment in strengthening equitable technical capacity, even the best legal instruments will lose their effectiveness in the field.

Furthermore, the position of digital platform operators within the existing legal framework remains unclear. Platform obligations to conduct proactive detection, respond quickly to reports, and adequately store digital footprints remain general and lack deterrent sanctions. Yet, platforms control the data, infrastructure, and technical capabilities necessary to mitigate upstream risks. This lack of clarity creates an asymmetry of responsibility, where the burden of prevention rests with victims and authorities, who have limited access to the system. Restructuring the responsibilities of electronic system operators is key to closing the loopholes exploited by trafficking networks.

Furthermore, weaknesses in legal culture are evident in the way some officials and the public view cybercrime as a technical issue separate from human rights protection. This perspective leads to an overemphasis on procedural-technical aspects of case handling and a neglect of the victim recovery dimension. Yet, women and children who become victims of online exploitation often experience multiple traumas that require a sensitive and sustainable approach. Reorienting legal culture toward a victim-centered paradigm is a prerequisite for substantive and structural reforms to truly impact the lives of vulnerable groups, not simply improve case handling statistics.

Thus, the weaknesses in Indonesia's cyber legal framework are systemic and mutually reinforcing. Substantively, there is a lack of norms governing artificial intelligence; structurally, there are limitations in capacity, jurisdiction, and inter-institutional coordination; and in terms of legal culture, there is low digital literacy

LICS 2026

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

among both officials and the public. These three components explain why existing regulations have not been able to protect women and children from exploitation facilitated by artificial intelligence, and therefore, partial reforms are insufficient. What is needed is a reconstruction that addresses all three layers simultaneously and in an integrated manner, not a reactive patchwork of solutions to each new case.

3.2. Legal Reconstruction: Artificial Intelligence Governance and Blockchain Mechanisms for Victim Prevention and Protection

The first reconstruction concerns legal substance. Indonesia needs an adaptive and progressive AI regulatory framework, either through specific legislation or targeted amendments to the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law, that guarantees transparency, algorithmic accountability, and accountability of providers.³⁸ The framework should include mandatory impact assessments of high-risk systems and clear risk categorization, so that oversight can be proportionate to potential hazards.³⁹

These regulations must be framed by human rights principles so that anti-trafficking technology does not become a surveillance instrument that oppresses vulnerable groups.⁴⁰ It is this rights-based approach that distinguishes ethical AI governance from mere technocratic solutions, by placing victim dignity as the normative boundary for any technological intervention.⁴¹

It is important to emphasize that updating the legal substance must not stop at formulating abstract norms. Any obligations for algorithmic transparency and accountability need to be translated into measurable technical standards, auditable compliance indicators, and proportionate and deterrent sanctions. Without concrete operationalization, legal obligations risk becoming mere rhetoric that does not change the behavior of system administrators. Therefore, the formulation of norms must be designed in collaboration with technologists, academics, and practitioners to avoid creating an impossible compliance burden while still providing real protection. This balance between legal certainty, technical feasibility, and rights protection will determine whether the new framework can be truly implemented.

³⁸ Loso Judijanto and Rabith Madah Khulaili Harsya, Op.Cit., p. 146.

³⁹ *Ibid.*, p. 147.

⁴⁰ Julia Deeb-Swihart, Alex Endert, and Amy Bruckman, Op.Cit., p. 12.

⁴¹ *Ibid.*, p. 15.

LICS 2026

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

Algorithmic accountability also requires acknowledging that decisions made by automated systems remain the responsibility of the humans and legal entities operating them. The principle that no legally binding decision should be entirely left to machines without human oversight needs to be affirmed, particularly when it comes to assessing the risks to vulnerable individuals. The right of victims to receive an explanation of the mechanisms that influence their fate, as well as the right to challenge erroneous decisions, must be guaranteed as part of legal protection. By placing responsibility on the human actors behind the system, the law prevents the emergence of loopholes of impunity that arise from technological anonymity. This approach also ensures that the use of artificial intelligence in law enforcement does not compromise the presumption of innocence and the right to a fair trial.

The second reconstruction positions AI as a legitimate protective instrument. Deep learning-based surveillance and detection systems can map patterns and anomalies in human trafficking from online advertisements and communication trails to suspicious financial flows thus accelerating the identification of victims in historically overlooked communities.⁴² The use of natural language processing and predictive analytics enables network mapping and early detection, as long as it is accompanied by safeguards against data bias and maintaining data integrity.⁴³

For such detection to be effective, countries need to require digital platforms to conduct due diligence, proactively detect exploitative content and accounts, and report findings to law enforcement as a form of platform accountability.⁴⁴ This obligation shifts some of the burden of prevention to the party best able to mitigate upstream risks, namely the electronic system provider.⁴⁵

The third reconstruction involves strengthening the integrity of digital evidence and victim identities through blockchain technology. A permissioned blockchain model involving law enforcement authorities and relevant institutions as validator nodes can implement an off-chain storage scheme for encrypted documents, while on-chain recording consists only of hashes, timestamps, and essential metadata to ensure immutable and auditable records. This scheme addresses the weaknesses of digital evidence that have hampered the handling of deepfake and

⁴²Amina Catherine Ijiga, et al., Op.Cit., p. 274.

⁴³*Ibid.*, p. 277.

⁴⁴Joel Levesque, Op.Cit., p. 9.

⁴⁵*Ibid.*, p. 10.

LICS 2026

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

cross-border cyber exploitation cases.⁴⁶ With an irreversible trail, manipulation or deletion of evidence by the perpetrator can be detected early.⁴⁷

As a progressive legal approach, reconstruction does not stop at the text, but rather positions the law as a means of realizing substantive justice for victims.⁴⁸ Progressive law demands the courage to interpret and create new norms when the existing order fails to respond to the needs of society, including in dealing with technology-based crimes.⁴⁹

This evidence integrity mechanism also overcomes cross-jurisdictional barriers. Permanently recorded hash integrity facilitates the exchange of evidence within the framework of mutual legal assistance, reducing reliance on lengthy procedures when conversation data is stored on overseas servers.⁵⁰ A victim's verified digital identity also makes vulnerable individuals more "visible" to protection systems, facilitating assistance and preventing perpetrators from obliterating traces of the victim's identity.⁵¹

The application of blockchain to evidence assurance requires caution to avoid creating new issues. The choice of a permissioned model, rather than a public one, ensures that access control remains with legitimate authorities and that sensitive victim data is not publicly exposed. The principle of data minimization must be upheld by recording only digital signatures and essential metadata on-chain, while the complete document remains encrypted off-chain. Cryptographic key governance, validator authority settings, and recovery protocols in the event of a security compromise are crucial aspects. Without a well-thought-out governance design, technology intended to protect can actually become a source of privacy risks. Therefore, the adoption of this technology must go hand in hand with the development of a legal framework and operational standards that prioritize the protection of victim data, rather than an afterthought after the system has been built.

The fourth reconstruction places victims at the center. Protection must be trauma-sensitive, gender-sensitive, and sensitive to children's needs, ensuring access to real restitution and recovery, not just procedural formalities.⁵² Law enforcement

⁴⁶Fabrizio Richardo Marvil Wanggai, et al., Op.Cit., p. 127.

⁴⁷*Ibid.*, p. 128.

⁴⁸Satjipto Rahardjo, *Dissecting Progressive Law*, Kompas Book Publisher, Jakarta, 2006, p. 20.

⁴⁹*Ibid.*, p. 23.

⁵⁰Satriya Aldi Putrazta, Op.Cit., p. 100.

⁵¹*Ibid.*, p. 101.

⁵²An Nisya Nursabilah, et al., Op.Cit., p. 181.

LICS 2026

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

officers need to be equipped with digital literacy and handling protocols that prevent the repetition of victim trauma during the judicial process.⁵³

A victim-centric approach also requires the provision of integrated support services that combine legal aid, psychosocial support, and access to economic recovery under one roof. Victims of technology-facilitated trafficking often suffer digital reputation damage, debt burdens resulting from recruitment traps, and prolonged trauma that hinders social reintegration. Without integrated services, victims are forced to navigate fragmented bureaucracies and risk secondary victimization at every stage. States need to ensure that recovery does not stop with a court decision, but continues until victims are truly able to rebuild their lives. Within this framework, secure digital identity technology can help victims access services without having to repeatedly prove their status, thereby enhancing the recovery process and minimizing psychological burdens.

For child victims of image exploitation, the right to be forgotten needs to be operationalized as an obligation for platform organizers to delete digital traces, so that manipulated images do not continue to circulate.⁵⁴ All these steps must be synchronized with the standards of the Palermo Protocol and strengthened international cooperation so that domestic approaches are not isolated from the global anti-trafficking regime.⁵⁵

To ensure reconstruction remains a normative idea, a supportive institutional design is required. The state needs to clarify the authority of electronic system supervisory bodies to assess platform compliance with AI governance and data protection obligations, while establishing a coordination mechanism between institutionsthe police, the prosecutor's office, the data protection authority, relevant ministries, and witness and victim protection agencieswhich has so far been fragmented. Without a clear coordination hub, even new legal obligations will lose their validity because no single actor is responsible for ensuring their implementation. Strong institutions are also a prerequisite for blockchain mechanisms for evidence integrity to operate across agencies with accountable governance.

Reconstruction should be implemented in stages. In the short term, priority should be given to developing technical guidelines for handling electronic evidence and increasing the capacity of authorities through digital forensics training and trauma-sensitive victim care. In the medium term, targeted amendments to the

⁵³*Ibid.*, p. 182.

⁵⁴Muhammad Deckri Algamar and Aliya Ilysia Irfana Ampri, *Op.Cit.*, p. 35.

⁵⁵Ni Kadek Puspawati, *Op.Cit.*, p. 12.



LICS 2026

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

ITE Law and the Personal Data Protection Law could include algorithmic transparency requirements, high-risk system impact testing, and platform due diligence requirements. In the long term, Indonesia could consider a comprehensive, dedicated law on artificial intelligence governance, complete with a monitoring and sanctions framework. This phasing is crucial to ensure the reforms are politically and budgetarily realistic, while also allowing time for strengthening institutional capacity.

This reconstruction certainly faces challenges. First, limited budget and technically qualified human resources can slow the implementation of AI-based detection systems and blockchain infrastructure. Second, there is a risk of tension between the need for oversight and privacy protection, requiring the proportionality of each instrument to prevent it from degenerating into mass surveillance that erodes civil liberties. Third, interoperability of systems between institutions and countries requires mutually agreed-upon technical standards. Mitigating these challenges includes partnerships with universities and the private sector for knowledge transfer, the application of data minimization principles, and strengthening international cooperation in evidence exchange and standards harmonization. With careful risk management, the benefits of technology can be maximized without compromising the human rights of the groups it seeks to protect.

Equally important, legal reconstruction must be accompanied by strengthening legal culture and digital literacy in society. Women and children, the primary targets of cyber exploitation, need to be equipped with the skills to recognize online recruitment methods, protect their personal data, and identify safe reporting channels. The role of civil society, educational institutions, and digital communities is crucial in building a community-based prevention ecosystem that complements repressive approaches. Good law not only prosecutes perpetrators after a crime occurs, but also builds social resilience that closes the scope for criminal networks to operate from the start.

The proposed reconstruction also requires clear institutional arrangements. A coordinating hub is needed that unites the authority of law enforcement, data protection authorities, electronic system administrators, and women's and children's protection agencies into a single, integrated workflow. Without clear mandates and role allocations, even sophisticated technological interventions will lose their effectiveness due to sectoral egos and overlapping authority. This institutional arrangement should be accompanied by data-sharing protocols that uphold the principles of minimization and limited objectives, so that information exchange between institutions does not become a source of new data leaks that

LICS 2026

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

endanger victims. With well-organized institutions, the state's response can shift from a reactive, case-by-case approach to a systemic, preventative strategy.

The victim recovery dimension requires equal attention to the enforcement dimension. Restitution and rehabilitation mechanisms need to be designed to be easily accessible, not increase the burden of trauma, and ensure the confidentiality of victims' identities. The use of blockchain-based digital identity technology can help victims prove their history and rights without having to repeatedly disclose traumatic experiences to multiple parties. At the same time, protection must address groups with multiple vulnerabilities, such as minors, people with disabilities, and victims from areas with limited access to justice. A victim-centered approach positions recovery not as the final stage after the criminal process, but as a guiding principle that accompanies all stages of case management from the beginning.

Ultimately, the success of reconstruction depends heavily on ongoing evaluation. Artificial intelligence governance and blockchain utilization are not one-size-fits-all solutions, but rather systems that must be continually audited, tested, and adapted as crime modes evolve and technology advances. Regular review mechanisms, the involvement of academics and civil society in oversight, and openness to criticism are safeguards to ensure the legal framework does not fall behind. Adaptive law demands institutions that are willing to learn, and this willingness to learn is what ultimately distinguishes a living protection framework from a static normative document.

Harmonization with international standards needs to be translated into concrete steps, not just statements of commitment. Indonesia has ratified international anti-trafficking instruments, but their operationalization requires alignment of definitions, evidence-sharing procedures, and cross-border victim-witness protection mechanisms. In Southeast Asia, the cross-border nature of online fraud and forced labor cases demands a stronger regional cooperation framework, including rapid communication channels between authorities and joint protocols for handling victim repatriation. Without operational harmonization, national legal reconstruction will remain hampered when faced with networks that deliberately spread their operations across multiple jurisdictions to complicate enforcement.

Capacity building through legal education is also an integral part of this reconstruction. Legal curricula need to integrate an understanding of technology, the ethics of artificial intelligence, and digital forensics to ensure that future generations of law enforcement officers and practitioners have adequate literacy.

LICS 2026

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

Certification programs for investigators, prosecutors, and judges in handling electronic evidence will improve the consistency of case handling and reduce reliance on case interpretation. Investment in this knowledge is long-term, but it is precisely where the sustainability of reform lies: a sound legal framework will only be effective if implemented by officials who understand the logic of the technology they are dealing with while adhering to the principles of human rights protection.

Philosophically, this reconstruction is grounded in the Pancasila value of justice, particularly the fifth principle, which demands social justice for all people. Substantive justice is achieved by limiting AI to accountable and bias-free functions; procedural justice is guaranteed through blockchain-based evidence integrity; and individual justice is realized through data governance that implements the principle of privacy by design. With this framework, the law not only pursues perpetrators but also builds a barrier of prevention and recovery that supports women and children as the primary victims of human trafficking in the digital era. This reconstruction demands synergy between legislators, law enforcement, platform operators, and civil society so that technology governance is truly oriented toward protection, not merely surveillance.

4. Conclusion

Indonesia's cyber legal framework is unable to protect women and children from human trafficking facilitated by artificial intelligence due to the lack of AI norms in the 2024 Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law, weak cross-border digital evidence mechanisms, and victim protection that is not yet recovery-oriented. Therefore, legal reconstruction is needed that integrates ethical and accountable AI governance, mandatory due diligence and algorithmic accountability for platforms, the use of AI as a detection tool that adheres to human rights principles, and a permissioned blockchain mechanism to ensure the integrity of evidence and victims' digital identities. All of this reconstruction is based on the Pancasila value of justice to strengthen prevention and victim recovery, and demands synchronization of national regulations with international anti-trafficking standards to ensure real, adaptive, and sustainable protection for women and children. As a follow-up, three main steps are recommended. First, lawmakers need to develop risk-based artificial intelligence governance arrangements through specific legislation or targeted amendments that include transparency obligations, algorithmic accountability, and impact testing for high-risk systems. Second, law enforcement needs to be supported by technical guidelines for handling blockchain-based electronic evidence, as well as increasing digital forensics capacity and trauma-sensitive

LICS 2026

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

victim care. Third, international cooperation and interagency coordination need to be strengthened to ensure that cross-border cases are not stalled at the evidence and repatriation stages. These three steps are expected to close legal loopholes exploited by perpetrators and prioritize the protection of women and children in national technology governance. Ultimately, the ideas put forward in this paper emphasize that the law must boldly engage in dialogue with technology without losing its value orientation. Artificial intelligence and blockchain are not threats to be rejected, but rather resources that can be directed to protect the most vulnerable, as long as they are managed within an accountable and victim-centered framework. The greatest challenge lies not in technological limitations, but in the political will and institutional capacity to build just governance. With a commitment to the Pancasila values of justice and a willingness to continuously learn and adapt, Indonesia has the opportunity to make cyber law an instrument for upholding human dignity, not merely a cold surveillance tool. Herein lies the relevance of the proposed reconstruction: linking technological progress with humanitarian commitments within a unified and sustainable framework of protection.

5. References

Journals:

- Algamar, Muhammad Deckri, dan Aliya Ilysia Irfana Ampri, Hak untuk Dilupakan: Penghapusan Jejak Digital sebagai Perlindungan Selebriti Anak dari Bahaya *Deepfake*, *Jurnal Yustika: Media Hukum dan Keadilan*, Vol. 25 No. 1 (2022), <https://doi.org/10.24123/yustika.v25i01.5091>;
- Deeb-Swihart, Julia, Alex Endert, dan Amy Bruckman, Ethical Tensions in Applications of AI for Addressing Human Trafficking: A Human Rights Perspective, *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6 CSCW2 (2022), <https://doi.org/10.1145/3555186>;
- Ijiga, Amina Catherine, et al., Advanced Surveillance and Detection Systems Using Deep Learning to Combat Human Trafficking, *Magna Scientia Advanced Research and Reviews*, Vol. 11 No. 1 (2024), <https://doi.org/10.30574/msarr.2024.11.1.0091>;
- Judijanto, Loso, dan Rabith Madah Khulaili Harsya, Etika dan Hukum dalam Penggunaan *Artificial Intelligence* terhadap Privasi Digital di Indonesia, *Sanskara Hukum dan HAM*, Vol. 3 No. 3 (2025), <https://doi.org/10.58812/shh.v3i03.543>;
- Levesque, Joel, The AI-Enhanced Trafficking Threat: Examining the Technological Evolution of Trafficking in Persons Operations with AI Tools, *Journal of Human Trafficking*, advance online publication (2025), <https://doi.org/10.1080/23322705.2025.2572911>;



LICS 2026

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

Nizar, M., A. Inayah, dan A. T. Dwijono, Penguatan Peran Pemerintah melalui Perlindungan Hukum terhadap Pekerja Migran Indonesia, *SOSIOLOGI: Jurnal Ilmiah Kajian Ilmu Sosial dan Budaya*, Vol. 20 No. 2 (2018), <https://doi.org/10.23960/sosiologi.v20i2.10>;

Nursabilah, An Nisya, dkk., Perlindungan Hukum bagi Korban Tindak Pidana *Cyber Scam* serta Dampaknya bagi Korban sebagai Bentuk Viktimisasi Sekunder, *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, Vol. 2 No. 3 (2025), <https://doi.org/10.62383/humif.v2i3.1912>;

Puspawati, Ni Kadek, Implementasi Kebijakan Pemberantasan Perdagangan Orang dalam Perspektif Hukum Internasional dan Nasional, *Indonesian Journal of Law and Justice*, Vol. 2 No. 3 (2025), <https://doi.org/10.47134/ijlj.v2i3.3661>;

Putrazta, Satriya Aldi, Perlindungan Hukum Korban Tindak Pidana Perdagangan Orang Lintas Negara Berkedok Lowongan Kerja Digital di Myanmar, *Majelis: Jurnal Hukum Indonesia*, Vol. 2 No. 4 (2025), <https://doi.org/10.62383/majelis.v2i4.1204>;

Sudiyawati, Ni Putu Lina, dan I Ketut Mertha, Kejahatan Siber (*Cybercrime*) dalam Konteks Kekerasan Seksual Berbasis Gender Online di Indonesia, *Kertha Semaya*, Vol. 10 No. 4 (2022), <https://doi.org/10.24843/ks.2022.v10.i04.p11>;

Wanggai, Fabrizio Richardo Marvil, Made Sugi Hartono, dan Ni Putu Ega Parwati, Analisis Normatif terhadap Penyebaran *Deepfake* sebagai Bentuk Kejahatan Siber di Indonesia, *Majelis: Jurnal Hukum Indonesia*, Vol. 3 No. 1 (2026), <https://doi.org/10.62383/majelis.v3i1.1509>.

Books:

Marzuki, Peter Mahmud, *Penelitian Hukum*, Edisi Revisi, Jakarta : Kencana, 2021;

Rahardjo, Satjipto, *Membedah Hukum Progresif*, Jakarta : Penerbit Buku Kompas, 2006;

Soekanto, Soerjono, dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta : Rajawali Pers, 2015.

Regulation:

Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions.

Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence;

Law No. 21 of 2007 concerning the Eradication of the Crime of Human Trafficking;

Law No. 27 of 2022 concerning Personal Data Protection;



LICS 2026

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

Law No. 35 of 2014 concerning Amendments to Law No. 23 of 2002 concerning Child Protection;