



LICS 2026

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

Cyber Trafficking and Online Exploitation of Women and Children: Legal Analysis, Victim Protection, and Digital Prevention Strategies in Indonesia

Liena

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,
E-mail: lienamardy55@gmail.com

Abstract. *This study aims to analyze cyber trafficking and online exploitation against women and children in Indonesia by examining legal protection, victim recovery, and digital prevention strategies. A normative juridical approach was employed through statutory, conceptual, and analytical approaches. The study uses primary legal materials consisting of Indonesian laws and regulations concerning human trafficking, child protection, sexual violence, electronic information, personal data protection, migrant worker protection, and ASEAN anti-trafficking instruments. Secondary legal materials include reputable journal articles with DOI, books, and institutional reports. The findings show that cyber trafficking has transformed conventional human trafficking through online recruitment, grooming, sextortion, fraudulent job advertisements, misuse of personal data, encrypted communication, and digital financial transactions. Indonesia already has a broad legal framework through the Anti-Trafficking Law, Child Protection Law, Sexual Violence Crime Law, Electronic Information and Transactions Law, Personal Data Protection Law, Migrant Worker Protection Law, and regional cooperation under ACTIP. However, implementation remains challenged by fragmented regulation, limited digital investigation capacity, cross-border jurisdiction, weak platform accountability, and insufficient trauma-informed recovery services. This article proposes a 5P model consisting of prevention, protection, prosecution, partnership, and platform governance.*

Keywords: *Cyber Trafficking; Digital Law; Human Trafficking; Victim Protection; 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 serious crime that attacks human dignity by subjecting a person to economic exploitation, sexual exploitation, forced labor, modern slavery, or other forms of control that violate human rights. In the context of Indonesian law, the crime of human trafficking is not only understood as the transfer of a person from one place to another, but also as a series of acts of recruiting, transporting, harboring, sending, transferring, or receiving a person in an unlawful manner for the purpose of exploitation. The development of digital technology has shifted the pattern of human trafficking from physical space to a virtual space that is more hidden, fast, cross-regional, and difficult to control. The internet, social media, instant messaging applications, job platforms, advertising sites, digital wallets, and electronic payment systems can now be used by perpetrators to recruit, control, threaten, advertise, and exploit victims without always having to deal directly with the victim (Gezinski & Gonzalez-Pons, 2024; L'Hoiry et al., 2024).

This phenomenon is often referred to as cyber trafficking, which involves the use of information and communication technology to facilitate one or more stages of human trafficking. Digital technology does not change the substance of human trafficking, but it does change the means, space, speed, reach, and patterns of relationships between perpetrators and victims. Perpetrators can create fake accounts, pose as employers, peers, romantic partners, entertainment agents, model recruiters, scholarship providers, or overseas employment brokers. Once the victim trusts them, perpetrators can engage in emotional manipulation, solicit personal data, collect intimate photos or videos, offer fake jobs, arrange meetings, or move the victim into exploitative situations. In some cases, exploitation can even occur without physical movement, for example through live streaming of sexual exploitation, sextortion, the production of forced sexual content, digital job fraud, or controlling the victim through threats of disclosing personal data (O'Brien & Li, 2020; Reeves et al., 2024).

LICS 2026

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

Women and children are highly vulnerable to cyber trafficking. This vulnerability is linked to social, economic, cultural, age-related factors, power relations, economic dependency, low digital literacy, gender-based violence, and limited access to legal services and redress. Children can be groomed through online games, chat rooms, social media, or content-sharing apps. Young women can be lured through offers of high-paying jobs, entertainment work, product endorsements, labor migration, or fake romantic relationships. Once victims are vulnerable, perpetrators often use threats, shame, manipulation, debt, violence, extortion of intimate images, and misuse of personal data to maintain control (Hemmings et al., 2016; Ottisova et al., 2016).

In the Indonesian context, the legal framework for eradicating human trafficking is regulated by Law No. 21 of 2007 concerning the Eradication of the Crime of Human Trafficking. Child protection is strengthened through Law No. 35 of 2014 and Law No. 17 of 2016. Sexual violence is regulated more specifically through Law No. 12 of 2022 concerning the Crime of Sexual Violence. Meanwhile, the digital aspect of cyber trafficking is closely related to 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. Regarding cross-border migration and work, Law No. 18 of 2017 concerning the Protection of Indonesian Migrant Workers and the ratification of the ASEAN Convention Against Trafficking in Persons, Especially Women and Children through Law No. 12 of 2017 are important instruments in strengthening regional cooperation.

Despite Indonesia's relatively broad legal framework, cyber trafficking still presents significant challenges. First, regulations are often applied separately, even though cyber trafficking cases typically involve a combination of human trafficking, sexual violence, misuse of personal data, electronic fraud, extortion, and child exploitation. Second, digital evidence requires forensic capacity, electronic transaction tracking, digital evidence security, and collaboration with platforms, which are not evenly distributed across all regions. Third, victims often experience re-victimization because digital content once created or coerced can continue to be stored, copied, sold, or redistributed. Fourth, victim recovery mechanisms are not always trauma-based and do not guarantee long-term psychological, social, educational, and economic recovery (Chambers et al., 2022; Mak et al., 2023).

LICS 2026

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

The study of cyber trafficking is crucial because conventional criminal law approaches are no longer sufficient to address the crime of human trafficking, which has been transformed through digital technology. Addressing cyber trafficking requires an integrated approach involving law, technology, victim protection, digital literacy, platform governance, cross-border cooperation, and social recovery. States are required not only to punish perpetrators but also to prevent online recruitment, strengthen reporting systems, protect victim data, remove exploitative content, provide reparations for victims, and ensure that digital platforms share responsibility for preventing the digital space from becoming a marketplace for human exploitation (Moore, 2024; Van Der Watt, 2023).

Based on this description, this article aims to analyze cyber trafficking and online exploitation of women and children in Indonesia and formulate a prevention and handling strategy model that is victim-oriented, law-based, and adaptive to developments in digital technology.

2. Research Methods

This research uses a juridical-normative method with a statutory approach, conceptual approach and analytical approach. Normative legal research was chosen because the main focus of this article is to examine legal norms, legal principles, doctrine, and legal concepts related to cyber trafficking, protection of women and children, digital evidence, and victim recovery. In normative legal research, legal materials are the main basis for building legal arguments through systematic, conceptual and teleological interpretations of applicable laws and regulations (Marzuki, P. M., 2017; Soekanto, S., 2015).

A legislative approach is used to examine legal norms related to the crime of human trafficking, child protection, sexual violence, electronic information, personal data protection, migrant workers, victim services, and regional cooperation in eradicating human trafficking. A conceptual approach is used to understand the concepts of cyber trafficking, online sexual exploitation and abuse, digital grooming, sextortion, victim-centered approaches, trauma-informed care, digital evidence, and platform governance. An analytical approach is used to connect legal norms with the methods of cyber trafficking and the protection needs of women and children as victims.

The primary legal materials in this study include the 1945 Constitution of the Republic of Indonesia, Law No. 21 of 2007 concerning the Eradication of the Crime of Human Trafficking, Law No. 35 of 2014 concerning Child Protection, Law No. 17

LICS 2026

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

of 2016 concerning the Second Amendment to the Child Protection Law, Law No. 18 of 2017 concerning the Protection of Indonesian Migrant Workers, Law No. 12 of 2017 concerning the Ratification of the ASEAN Convention Against Trafficking in Persons, Especially Women and Children, Law No. 12 of 2022 concerning the Crime of Sexual Violence, Law No. 27 of 2022 concerning the Protection of Personal Data, Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, Government Regulation No. 9 of 2008 concerning Procedures and Mechanisms for Integrated Services for Witnesses and/or Victims of Human Trafficking, Presidential Regulation No. 19 ... 2023 concerning the National Action Plan for the Prevention and Handling of Human Trafficking in 2020–2024, as well as Presidential Regulation No. 49 of 2023 concerning the Task Force for the Prevention and Handling of Human Trafficking in 2023.

The secondary legal materials used included reputable scientific journal articles with DOIs, law textbooks, international organization reports, and academic studies on human trafficking, online sexual exploitation, child protection, gender-based violence, digital evidence, victim recovery, and digital platform liability. The analysis was conducted qualitatively through interpretation of legal norms, conceptual grouping, assessment of the suitability between regulations and crime modes, and formulation of policy recommendations based on victim protection.

3. Results and Discussion

3.1. Characteristics of Cyber Trafficking of Women and Children

Cyber trafficking has distinct characteristics from conventional human trafficking. In conventional human trafficking, perpetrators typically physically recruit, transfer, harbor, or transport victims. In cyber trafficking, digital elements can be present from the initial stages through to the exploitation stage. Perpetrators can use social media, social networking apps, job boards, entertainment platforms, online games, instant messaging groups, digital advertising, and electronic payment systems to find, select, influence, control, and exploit victims. Thus, digital technology functions as a means of recruitment, communication, control, transaction, and disguise the perpetrator's identity (Gezinski & Gonzalez-Pons, 2024; L'Hoiry et al., 2024).

The first characteristic of cyber trafficking is online recruitment. Perpetrators no longer need to approach victims in person, but simply contact them through digital accounts. Offers often seem legitimate, such as high-paying jobs, modeling opportunities, overseas work offers, influencer opportunities, scholarships, travel,

LICS 2026

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

gifts, or romantic relationships. In the case of children, approaches can be made through online games, chat rooms, or fake accounts pretending to be the same age. In the case of young women, perpetrators may pose as employment agents, entertainment agents, content recruiters, or partners promising a better life. This modus operandi demonstrates that human trafficking crimes have exploited the logic of social trust in the digital space, namely the speed of communication, the ease of establishing false identities, and the lack of identity verification.

The second characteristic is emotional manipulation and grooming. Grooming is a gradual process carried out by the perpetrator to build trust, closeness, dependence and a false sense of security in the victim. The perpetrator usually does not immediately make threats, but starts with attention, praise, gifts, economic assistance, or intensive communication. Once the victim feels close, the perpetrator starts asking for photos, videos, personal data, location, family contacts, or other sensitive information. When the victim has provided certain information or content, the perpetrator can use it as a tool of blackmail to force the victim to follow his will (O'Brien & Li, 2020).

The third characteristic is that exploitation does not always require physical movement. In the digital age, exploitation can take place from the victim's own home. Child or female victims may be forced to live stream sexual acts, create sexual content, fulfill online customer requests, work in digital fraud schemes, or engage in exploitative economic activities through electronic devices. This broadens the understanding of human trafficking because victims can remain in their original location, but their bodies, data, labor, sexuality, and identities are exploited by perpetrators through digital networks. L'Hoiry et al. (2024) emphasizes that digital technology allows perpetrators to maintain distance from the location of exploitation, disguise their identity, and maintain control over victims through online communication means.

The fourth characteristic is the use of anonymity and obfuscation technology. Perpetrators can use fake accounts, disposable phone No.s, virtual private networks, encrypted apps, digital wallets, escrow accounts, crypto assets, or intermediaries to conceal their identities. Conversations can be deleted, accounts can be changed, data can be transferred to offshore servers, and transactions can be disguised. This makes cyber trafficking investigations more complex than human trafficking cases based solely on physical evidence. Lazarus et al. (2025) explains that the intersection between human trafficking and cybercrime shows the need to read human trafficking not only as a crime of exploitation, but also as a digital crime involving technological infrastructure.

LICS 2026

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

The fifth characteristic is digital revictimization. In cases of online sexual exploitation, content created, recorded, or forced upon the victim can continue to circulate after the victim is rescued. This content can be copied, sold, redistributed, or used to blackmail the victim again. Digital revictimization leaves victims feeling like the exploitation never truly ends. Therefore, protection for victims of cyber trafficking must include content removal, blocking distribution, personal data protection, psychological recovery, and guarantees of identity confidentiality (Hemmings et al., 2016; Ottisova et al., 2016).

3.2. Vulnerability of Women and Children in the Digital Ecosystem

Women and children are particularly vulnerable because cyber trafficking exploits structural weaknesses. Poverty, unemployment, educational needs, family conflict, domestic violence, unsafe migration, economic dependency, and gender inequality can all push victims to accept seemingly promising offers without adequate verification. Digital job offers often appear legitimate, using professional language, company logos, fake contracts, or fabricated testimonials. Victims seeking employment can struggle to distinguish between legitimate job offers and exploitation schemes. (Farrell & Reichert, 2017).

Children are particularly vulnerable because they lack the psychological maturity, risk-assessment skills, and legal capacity of adults. They may perceive online communication with strangers as ordinary friendships. They may also be easily convinced when perpetrators offer compliments, digital gifts, game items, or emotional attention. When perpetrators begin to request personal information, children often don't realize they are being groomed for exploitation. Even after exploitation occurs, children are often afraid to report it due to feelings of guilt, shame, or fear of punishment by parents and schools. (Reeves et al., 2024) emphasizes that preventing online child sexual exploitation needs to be done through digital education that is close to children's experiences, including through interactive media and safe learning environments.

Women also face vulnerability due to power relations and social stigma. In many cases, women who are victims of sexual exploitation are blamed by their environment. This stigma discourages victims from reporting the abuse and allows perpetrators to continue controlling them. Perpetrators often exploit victims' fears of family, partners, school, workplace, or community. The threat of sharing intimate photos, private conversations, or identifying information can be a powerful tool of control, as victims fear losing their honor, job, education, or family support (Matos et al., 2025).

LICS 2026

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

Low digital literacy exacerbates the risks. Many internet users don't understand the importance of safeguarding personal data, limiting account access, verifying employer identities, recognizing malicious links, reporting suspicious accounts, or safely storing digital evidence. For children, this problem is even more serious because internet use often lacks parental supervision and digital safety education. For female prospective migrant workers, low digital literacy can make them easily trust unregistered online employment agencies. This situation demonstrates that digital literacy must be understood as part of legal protection policies, not simply as technical skills in using the internet.

Family, school, and community environments play a crucial role in preventing cyber trafficking. Parents need to understand the platforms their children use, recognize behavioral changes, and build communication that doesn't blame the victim. Schools need to integrate education on digital safety, the dangers of grooming, personal data protection, and reporting mechanisms for online violence. Community and village officials also need to be involved, as victim recruitment often begins locally, even though exploitation occurs across regions or even countries Savoia et al. (2024) shows that schools and education personnel can be important actors in raising awareness of sex trafficking and early identification of the risk of exploitation.

3.3. Indonesia's Legal Framework for the Protection of Cyber Trafficking Victims

Law No. 21 of 2007 concerning the Eradication of the Crime of Human Trafficking is the primary basis for addressing cyber trafficking. This law regulates the actions, methods, and purposes of exploitation. Because its focus is exploitation, the use of digital technology as a means does not eliminate the possibility of applying the Human Trafficking Law. If the perpetrator uses social media or a digital platform to recruit, control, send, harbor, or exploit a victim, the act can still be classified as Human Trafficking as long as the criminal elements are met. Thus, cyber trafficking is essentially a new form of human trafficking that uses digital means.

The advantage of the Human Trafficking Law is its relatively broad scope of exploitation. This law views human trafficking not only as physical movement but also as the process of controlling victims for the purpose of exploitation. This is crucial in cyber trafficking, as perpetrators can control victims through digital threats, blackmail, control of personal data, debt bondage, or emotional manipulation. However, its application is weak due to the need for more complex evidence. Authorities must be able to prove the link between digital communication, the perpetrator's intent, the act of control, and the purpose of exploitation. From a criminal law policy perspective, an updated law enforcement

LICS 2026

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

approach is necessary when social and technological developments give rise to new crime patterns that were not fully envisioned at the time the law was drafted (Arief, B. N., 2011; Muladi & Arief, B. N., 2010).

The Child Protection Law provides a basis for special protection for child victims of cyber trafficking. Children must be viewed as subjects of rights who must be protected from economic exploitation, sexual exploitation, violence, discrimination, abuse, and child trafficking. In the case of children, a child's consent cannot be used to justify exploitation. Therefore, when children are involved in the production of sexual content, live streaming, or sexual communication with adults, the legal approach must position the child as a victim, not a perpetrator of a moral violation. The principle of the best interests of the child must be the basis for investigations, prosecutions, court hearings, media coverage, and redress.

Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence strengthens protections for women and children who are victims of cyber trafficking, particularly when trafficking intersects with electronic-based sexual violence. Many cyber trafficking cases involve coercion into the creation of intimate content, threats to disseminate it, sexual exploitation, forced sexual intercourse, or abuse of power. The TPKS Law is important because it emphasizes victims' rights to treatment, protection, and recovery. This strengthens the legal system's orientation from simply punishing perpetrators to rehabilitating victims.

The Electronic Information and Transactions Law is a crucial instrument for establishing and prosecuting digital crimes. Electronic information and electronic documents can serve as relevant evidence in cyber trafficking cases. Instant messaging conversations, call histories, social media posts, metadata, transaction evidence, online advertisements, links, IP addresses, and digital recordings can help demonstrate patterns of recruitment, threats, control, and exploitation. However, the use of digital evidence must consider the legality of data collection, the chain of custody of evidence, data integrity, and the protection of victim privacy. Giommoni (2024) reminded that the identification of human trafficking through online indicators cannot be done mechanically because there is a risk of misidentification, both false positive and false negative.

The Personal Data Protection Law is also relevant because perpetrators often use victims' data as a means of control. Data such as photos, home addresses, family contacts, ID No.s, social media accounts, location history, bank accounts, and private conversations can be used to blackmail or threaten victims. In cyber trafficking, protecting personal data concerns not only privacy but also the safety

LICS 2026

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

of victims. Therefore, data protection must be an integral part of protecting human trafficking victims. Without strong data protection, victims can continue to be controlled by perpetrators even after escaping their exploitative situation.

In the context of migrant workers, Law No. 18 of 2017 is crucial because many victims are recruited through overseas job offers. Digital methods can include fake job postings, offers to work as domestic workers, entertainment workers, digital operators, customer service workers, or other jobs that ultimately result in forced labor, sexual exploitation, online fraud, or modern slavery. Migrant worker regulations need to be linked to the prevention of cyber trafficking through verification of employment agencies, education of prospective workers, supervision of online recruiters, and collaboration with Indonesian representatives abroad.

Ratification of the ASEAN Convention Against Trafficking in Persons, Especially Women and Children strengthens regional cooperation. Cyber trafficking often involves transnational networks, including recruitment, transfer of victims, locations of exploitation, financial flows, digital servers, and platforms. Therefore, addressing cyber trafficking cannot rely solely on national laws. Cooperation between countries is required in the exchange of information, mutual legal assistance, victim protection, repatriation, rehabilitation, and prosecution of transnational networks (ASEAN, 2015).

3.4. Challenges of Digital Evidence and Investigation

Proving cyber trafficking faces both technical and legal challenges. The first challenge is the perpetrator's identity, which is often disguised. Perpetrators may use fake names, anonymous accounts, stolen photos, temporary phone No.s, encrypted apps, or communication intermediaries. This makes it difficult for authorities to link digital accounts to the perpetrator's legal identity. In some cases, the main perpetrator never interacts directly with the victim but instead uses recruiters, account administrators, or local intermediaries. This situation suggests that proving cyber trafficking requires tracing the network, not just the individuals who communicate directly with the victim.

The second challenge is that digital evidence is easily lost or altered. Conversations can be deleted, accounts can be closed, data can be moved, devices can be destroyed, and platforms can remove content for violating internal policies before authorities can obtain a copy of the evidence. Therefore, victims, their families, advocates, and authorities need to understand how to securely store digital evidence without sharing it. Screenshots alone are often insufficient if they are not

LICS 2026

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

supported by metadata, links, devices, or expert testimony. In cases of child exploitation, digital evidence must be handled with extreme care to prevent the spread of exploitative content.

The third challenge is cross-border jurisdiction. Digital platforms, servers, service providers, or perpetrators can be located outside Indonesia. Data requests from international platforms require specific legal procedures and often take time. In cases involving children, a delayed response can increase the risk of spreading exploitative content and prolong the trauma of victims. Therefore, a rapid response mechanism is needed between law enforcement officials, relevant ministries, and platform providers. International cooperation must also be strengthened, as human trafficking is often a transnational crime (UNODC, 2022).

The fourth challenge is limited digital forensic capacity. Not all regions have adequate human resources, equipment, laboratories, and procedures to handle electronic evidence. Yet, cyber trafficking can occur in villages, small towns, border regions, migration areas, and even urban centers. This capacity gap can lead to cases not being identified as human trafficking (TPPO), but instead being considered fraud, ITE (Information and Transactions) violations, or moral issues. As a result, victims lack the protection they deserve, while perpetrators can escape prosecution.

The fifth challenge is the risk of criminalization or misunderstanding of victims. In cases of online sexual exploitation, victims may be seen as "sending" photos, "communicating" with the perpetrator, or "receiving" money. Without understanding the victim as the center of policy, authorities may mistakenly view the victim as the perpetrator. However, victims' actions often occur under conditions of threat, manipulation, blackmail, dependency, or the child's inability to provide valid consent. Therefore, proving cyber trafficking must examine the context of power relations and patterns of exploitation, not just fragments of digital communication.

3.5. Victim Protection and Trauma-Based Recovery

Protection for victims of cyber trafficking must begin at the identification stage. Victims don't always immediately identify themselves as victims. Some feel afraid, ashamed, threatened, or don't understand that they are being exploited. Child victims of grooming may perceive the perpetrator as a friend or partner. Female victims of digital blackmail may feel responsible for the content they send. Therefore, service officers, officials, teachers, health workers, and advocates must have the ability to identify signs of exploitation without judging the victim. This

LICS 2026

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

approach aligns with the concept of a victim-centered approach, which prioritizes the safety, dignity, and needs of victims. (Hemmings et al., 2016).

A victim-centered policy approach requires the state to treat victims as subjects of rights. Victims have the right to safety, anonymity, legal assistance, medical services, psychological support, safe housing, restitution, social rehabilitation, repatriation, and reintegration. In cases of cyber trafficking, victims also have the right to protection of their personal data and the removal of exploitative content. This protection is crucial because digital footprints can perpetuate the victim's suffering. (Ottisova et al., 2016) shows that victims of human trafficking are at high risk of experiencing violence, mental health disorders, physical health disorders, and sexual health problems.

Trauma-informed recovery is a key need. Cyber trafficking victims can experience complex trauma due to physical exploitation, sexual violence, threats, manipulation, shame, social isolation, and fear of the spread of content. Recovery should not be conducted in a way that corners victims or forces them to repeat their stories repeatedly without clear legal justification. Victim assessments should be conducted by trained personnel, in a safe environment, and should take into account the victim's age, gender, psychological condition, and specific needs. Chambers et al. (2022) emphasized the importance of trauma-informed care services that are consistent, ongoing, and sensitive to the experiences of human trafficking survivors.

Child victims need stronger protection. Their identities must be kept confidential in legal proceedings, news reports, and school settings. Children must receive psychological services, educational assistance, family support, and protection from stigma. Schools must be spaces of healing, not social punishment. Teachers and education personnel need to understand that child victims of online exploitation are not perpetrators of deviance, but victims of crime in need of support. UNICEF (2021) emphasized that preventing and addressing online child sexual exploitation requires the involvement of families, schools, communities, authorities, service providers, and digital platforms.

Female victims also need economic recovery. Many victims enter exploitative situations due to economic pressure or dependence on their perpetrators. If recovery consists solely of physical rescue without support for employment, training, education, and social protection, victims risk returning to vulnerable situations. Therefore, cyber trafficking recovery must include economic empowerment programs, job training, social assistance, access to education, and community support. Mak et al. (2023) showed that psychosocial interventions for

LICS 2026

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

survivors of human trafficking need to consider the social context, the victim's relationships, and realistic needs in the recovery process.

Restitution is also a crucial aspect of victim protection. Human trafficking victims experience material and immaterial losses, including lost income, medical expenses, psychological trauma, reputational damage, lost educational opportunities, and social suffering. Restitution mechanisms need to be made more effective so that victims not only receive a criminal verdict against the perpetrator but also receive concrete restitution. In practice, restitution must be accompanied by legal assistance so that victims understand their rights and can pursue appropriate restitution.

3.6. Digital Platform Responsibility

Digital platforms play a crucial role in cyber trafficking. On the one hand, platforms can provide a platform for communication, education, reporting, and victim rescue. On the other hand, platforms can be used by perpetrators to recruit, advertise, exploit, and control victims. Therefore, platforms cannot be viewed as completely neutral. Platforms have a responsibility to prevent their systems from being used as a means of human trafficking and child exploitation. Moore (2024) showed that social media algorithms can increase the risk of exploitation when recommendation systems, advertising, and content distribution are not managed with vulnerable user safety principles in mind.

Platform responsibilities should include mechanisms for detection, reporting, content removal, data protection, and cooperation with authorities. Platforms should have systems in place to identify grooming, sextortion, child sexual exploitation, fake job ads, suspicious recruitment, and risky transaction patterns. However, automated detection systems should not be the sole basis for action, as they can lead to errors. A combination of technology, human moderation, user reports, expert collaboration, and clear legal procedures is needed. Giommoni (2024) reminded that online data cannot automatically prove human trafficking without careful contextual analysis.

Platforms also need to provide easily accessible reporting channels for victims. Child and female victims often don't know where to report. Reporting features should be simple, secure, responsive, and non-shaming. If reports relate to child sexual exploitation or the threat of sharing intimate content, platforms should have a rapid escalation mechanism to prevent further dissemination. Content removal must be carried out while preserving evidence for legal purposes. Victim

LICS 2026

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

protection will be weakened if platforms simply remove content without helping to preserve valid evidence.

Algorithmic accountability is a critical issue. Platform algorithms can connect users with risky content, accounts, groups, or ads. If platform design encourages virality without adequate oversight, vulnerable groups can be more easily identified by perpetrators. Therefore, platform regulations need to address risk audits, moderation transparency, child-safety design, restrictions on risky ads, and mandatory responses to reports of exploitation. However, platform regulations must also be careful not to violate freedom of expression, privacy, or victims' rights. Digital surveillance policies should not degenerate into excessive surveillance of vulnerable groups.

In the Indonesian context, platform responsibilities need to be linked to the ITE Law, the PDP Law, the TPKS Law, the Child Protection Law, and the Human Trafficking Law. Regulations should encourage platforms to conduct risk assessments, provide reporting channels, remove exploitative content, protect victim data, and cooperate with law enforcement officials based on legal procedures. The state needs to ensure that platform governance is carried out proportionally, based on human rights, and oriented toward victim protection.

3.7. 5P Strategy Model in Preventing and Handling Cyber Trafficking

This article proposes a 5P model as an integrated strategy for preventing and addressing cyber trafficking of women and children in Indonesia: prevention, protection, prosecution, partnership, and platform governance. This model was developed because cyber trafficking is not only a criminal issue, but also encompasses social, technological, migration, education, personal data, mental health, and platform governance issues. Therefore, policy responses should not focus solely on punishing perpetrators but should also close recruitment opportunities, strengthen the resilience of potential victims, provide victim recovery, and build a safer digital ecosystem.

First, prevention. Prevention must be implemented through digital literacy, legal education, anti-trafficking campaigns, family strengthening, school supervision, job vacancy verification, and migrant worker education. Children need to be taught to recognize grooming, protect their personal data, refuse requests for intimate content, and report to a trusted adult. Young women and prospective migrant workers need to be informed about legal employment agencies, employment contracts, departure documents, the risks of online offers, and signs of exploitative recruitment. Prevention must also target those who create demand

LICS 2026

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

for sexual exploitation and forced labor, as trafficking persists when demand for exploitation exists (Van Der Watt, 2023).

Second, protection. Protection must ensure easy, safe, and victim-friendly reporting. Victims must have access to safe housing, legal assistance, medical services, psychological services, social recovery, identity protection, personal data protection, and the removal of exploitative content. Protection must also ensure victims are not punished for acts committed under threat, manipulation, or exploitation. The principle of non-punishment of victims needs to be strengthened in law enforcement practices, particularly in cases of online sexual exploitation when victims appear to be involved in digital communication or content production under pressure from the perpetrator.

Third, prosecution. Law enforcement needs to be strengthened through digital forensic capabilities, electronic transaction tracking, evidence preservation, the use of multiple provisions, cross-border cooperation, and officer training. Investigators, prosecutors, and judges need to understand the links between human trafficking, digital sexual violence, personal data misuse, and child exploitation. Prosecutors must prove the full pattern of exploitation, not just examine digital conversations in isolation. Prosecution in cyber trafficking must also encompass actors who assist, facilitate, advertise, receive benefits from, or allow exploitation to occur.

Fourth, partnership. Cyber trafficking cannot be handled by one agency alone. Collaboration is needed between the central government, regional governments, the police, the prosecutor's office, the courts, the Ministry of Women's Empowerment and Child Protection, the Ministry of Communication and Informatics, the Ministry of Manpower, the BP2MI (Indonesian Migrant Workers Protection Agency), the LPSK (Lembaga Penida Indonesia), social services agencies, service institutions, schools, universities, civil society organizations, the media, families, communities, and digital platforms. ASEAN and international cooperation are also crucial because many cases involve cross-border interventions. This collaborative model must be supported by a clear division of roles, a victim referral system, secure data exchange, and regular evaluations.

Fifth, platform governance. Platform governance must be a special pillar because cyber trafficking occurs through digital ecosystems. Platforms need to have mandatory risk assessments, rapid reporting systems, moderation of exploitative content, protection of victim data, removal of illegal content, preservation of evidence for legal proceedings, and cooperation with authorities. States need to develop regulations that encourage platform accountability without neglecting



LICS 2026

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

privacy and human rights. Platform governance must be directed at preventing technological designs that facilitate exploitation, rather than simply responding after a victim has been victimized.

3.8. Recommendations for Strengthening Policy in Indonesia

First, harmonization is needed between the Anti-Trafficking Law, the Child Protection Law, the TPKS Law, the ITE Law, the PDP Law, the Indonesian Migrant Worker Protection Law, and ASEAN instruments. This harmonization is crucial to prevent authorities from viewing cyber trafficking cases in a fragmented manner. A single incident can contain elements of human trafficking, sexual violence, child exploitation, personal data breaches, extortion, and electronic crime. Without harmonization, there is a risk that perpetrators will only be charged with less severe charges, while the exploitative structure of human trafficking remains undisclosed.

Second, operational guidelines for handling cyber trafficking are needed. These guidelines should include cyber trafficking indicators, victim identification procedures, rescue procedures, digital evidence handling, data requests to platforms, protection of child exploitation content, victim support, and inter-agency coordination. These guidelines need to be implemented from the national to regional levels. They should also include standards for communication with victims to prevent authorities from repeating practices that marginalize victims.

Third, digital investigative capacity must be strengthened. TIP units need to be equipped with capabilities in open-source intelligence, device forensics, social media analysis, electronic transaction tracking, data recovery, and platform collaboration. Training should be provided not only to central investigators but also to regional officials, as victim recruitment often begins locally. Furthermore, officials need to understand trauma-informed approaches to prevent the legal process from worsening victims' psychological well-being.

Fourth, an integrated, victim-friendly reporting system is needed. The reporting system must be accessible through digital channels, schools, villages/sub-districts, women's and children's service institutions, the police, hospitals, and Indonesian missions abroad. Reporting must ensure confidentiality, data security, a rapid response, and referral to recovery services. This system needs to be supported by trained staff to prevent victims from experiencing rejection, misunderstanding, or stigma when reporting.

LICS 2026

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

Fifth, digital literacy must be part of child protection and women's empowerment education. Digital literacy materials should not only cover social media ethics but also address grooming, sextortion, personal data privacy, fake job postings, human trafficking, online sexual exploitation, and reporting. This education should be provided to children, parents, teachers, social workers, village officials, prospective migrant workers, and vulnerable communities. Digital literacy should also be tailored to age, local language, and the social context of the community.

Sixth, the state needs to strengthen trauma-based recovery for victims. Recovery services must be long-term, encompassing psychological, medical, legal, social, educational, and economic assistance, as well as community reintegration. Child victims must be protected from stigma at school and identity disclosure. Female victims must receive economic support to prevent them from returning to vulnerable situations. Effective recovery must not stop at rescuing victims but must restore their dignity, self-confidence, independence, and future.

Seventh, digital platform regulations need to be directed at preventing exploitation. Platforms should be required to have rapid response mechanisms for child exploitation content, grooming, fake job advertisements, human trafficking, and digital extortion. Platforms should also conduct risk audits, implement moderation transparency, protect victim data, and cooperate with authorities within legal boundaries. Platform governance should make the safety of women and children part of the system design, not just an added feature.

4. Conclusion

Cyber trafficking and online exploitation of women and children represent a transformation of the crime of human trafficking that utilizes digital technology to recruit, manipulate, control, exploit, advertise, and threaten victims. Women and children are vulnerable groups due to economic factors, age, gender inequality, power relations, low digital literacy, social stigma, and limited access to protection and recovery services. Indonesia already has a fairly broad legal framework through the Anti-Trafficking Law, the Child Protection Law, the TPKS Law, the ITE Law, the PDP Law, the Indonesian Migrant Worker Protection Law, and the ratification of ACTIP, but its implementation still faces challenges in regulatory harmonization, digital evidence, the capacity of authorities, cross-border cooperation, platform responsibility, and trauma-based victim recovery. Therefore, the 5P model consisting of prevention, protection, prosecution, partnership, and platform governance can be used as a strategic framework to strengthen the prevention and handling of cyber trafficking in Indonesia by placing



LICS 2026

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

victims at the center of policy and making the protection of women and children an integrated legal, social, technological, and human rights agenda.

5. References

Journals:

- Chambers, R., Greenbaum, J., Cox, J., & Galvan, T. (2022). Trauma Informed Care: Trafficking Out-Comes (TIC TOC Study). *Journal of Primary Care & Community Health*, 13, 21501319221093119. <https://doi.org/10.1177/21501319221093119>
- Farrell, A., & Reichert, J. (2017). Using U.S. Law-Enforcement Data: Promise and Limits in Measuring Human Trafficking. *Journal of Human Trafficking*, 3(1), 39–60. <https://doi.org/10.1080/23322705.2017.1280324>
- Gezinski, L. B., & Gonzalez-Pons, K. M. (2024). Sex Trafficking and Technology: A Systematic Review of Recruitment and Exploitation. *Journal of Human Trafficking*, 10(3), 497–511. <https://doi.org/10.1080/23322705.2022.2034378>
- Giommoni, L. (2024). Why We Cannot Identify Human Trafficking from Online Advertisements. *Journal of Human Trafficking*, 1–15. <https://doi.org/10.1080/23322705.2024.2435198>
- Hemmings, S., Jakobowitz, S., Abas, M., Bick, D., Howard, L. M., Stanley, N., Zimmerman, C., & Oram, S. (2016). Responding to the health needs of survivors of human trafficking: A systematic review. *BMC Health Services Research*, 16(1), 320. <https://doi.org/10.1186/s12913-016-1538-8>
- Lazarus, S., Chiang, M., & Button, M. (2025). Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. *Deviant Behavior*, 1–18. <https://doi.org/10.1080/01639625.2025.2470402>
- L’Hoiry, X., Moretti, A., & Antonopoulos, G. A. (2024). Human trafficking, sexual exploitation and digital technologies. *Trends in Organized Crime*, 27(1), 1–9. <https://doi.org/10.1007/s12117-024-09526-4>
- Mak, J., Bentley, A., Paphitis, S., Huq, M., Zimmerman, C., Osrin, D., Devakumar, D., Abas, M., & Kiss, L. (2023). Psychosocial interventions to improve the mental health of survivors of human trafficking: A realist review. *The Lancet Psychiatry*, 10(7), 557–574. [https://doi.org/10.1016/S2215-0366\(23\)00105-0](https://doi.org/10.1016/S2215-0366(23)00105-0)
- Matos, M., Sousa, J., Caridade, S., & Dias, I. (2025). Sexual Exploitation: Professionals’ and Stakeholders’ Perceptions of Prevention, Assistance, and Protection for Victims in Portugal. *Social Sciences*, 14(3), 167. <https://doi.org/10.3390/socsci14030167>



LICS 2026

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

Moore, D. M. (2024). Algorithmic Exploitation in Social Media Human Trafficking and Strategies for Regulation. *Laws*, 13(3), 31.
<https://doi.org/10.3390/laws13030031>

O'Brien, J. E., & Li, W. (2020). The role of the internet in the grooming, exploitation, and exit of United States domestic minor sex trafficking victims. *Journal of Children and Media*, 14(2), 187–203.
<https://doi.org/10.1080/17482798.2019.1688668>

Ottisova, L., Hemmings, S., Howard, L. M., Zimmerman, C., & Oram, S. (2016). Prevalence and risk of violence and the mental, physical and sexual health problems associated with human trafficking: An updated systematic review. *Epidemiology and Psychiatric Sciences*, 25(4), 317–341.
<https://doi.org/10.1017/S2045796016000135>

Reeves, E. J., Jones, S. E., Kosaraju, A., Shemmings, D., Rigby, P., Scharf, K., & Soutar, E. (2024). May and Bay: Online Child Sexual Exploitation and Abuse in Southeast Asia — Using Digital Games in Preventative Education. *Journal of Human Rights and Social Work*, 9(4), 615–629.
<https://doi.org/10.1007/s41134-024-00314-2>

Savoia, E., Liu, A., Leffler, A., Nadril Churchill, L. K., & Su, M. (2024). Raising Awareness about Sex Trafficking among School Personnel. *International Journal of Environmental Research and Public Health*, 21(8), 978.
<https://doi.org/10.3390/ijerph21080978>

Van Der Watt, M. (2023). Discouraging the Demand That Fosters Sex Trafficking: Collaboration through Augmented Intelligence. *Societies*, 13(4), 94.
<https://doi.org/10.3390/soc13040094>

Books:

Arief, B. N. (2011). *Bunga rampai kebijakan hukum pidana*. Kencana.

ASEAN. (2015). *ASEAN Convention Against Trafficking in Persons, Especially Women and Children*.

International Labour Organization. (2017). *Global estimates of modern slavery: Forced labour and forced marriage*.

Marzuki, P. M. (2017). *Penelitian hukum*. Kencana.

Muladi, & Arief, B. N. (2010). *Teori-teori dan kebijakan pidana*. Alumni.

Soekanto, S., & Mamudji, S. (2015). *Penelitian hukum normatif: Suatu tinjauan singkat*. Rajawali Pers.

United Nations Office on Drugs and Crime. (2022). *Global report on trafficking in persons*.

UNICEF. (2021). *Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries*.



LICS 2026

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

Regulation:

Government Regulation No. 27 of 2024 concerning Coordination and Monitoring of the Implementation of Prevention and Handling of Victims of the Crime of Sexual Violence.

Government Regulation No. 30 of 2025 concerning the Prevention of the Crime of Sexual Violence and the Handling, Protection, and Recovery of Victims of the Crime of Sexual Violence. Presidential Regulation No. 19 of 2023 concerning the National Action Plan for the Prevention and Handling of the Crime of Human Trafficking for the Years 2020–2024.

Government Regulation No. 9 of 2008 concerning Procedures and Mechanisms for Integrated Services for Witnesses and/or Victims of the Crime of Trafficking in Persons.

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

Law No. 12 of 2017 concerning the Ratification of the ASEAN Convention Against Trafficking in Persons, Especially Women and Children.

Law No. 12 of 2022 concerning the Crime of Sexual Violence.

Law No. 17 of 2016 concerning the Enactment of Government Regulation in Lieu of Law No. 1 of 2016 concerning the Second Amendment to Law No. 23 of 2002 concerning Child Protection into Law.

Law No. 18 of 2017 concerning the Protection of Indonesian Migrant Workers.

Law No. 21 of 2007 concerning the Eradication of the Crime of Trafficking in Persons.

Law No. 27 of 2022 concerning Personal Data Protection.

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

Presidential Regulation No. 49 of 2023 concerning the Second Amendment to Presidential Regulation No. 69 of 2008 concerning the Task Force for the Prevention and Handling of the Crime of Human Trafficking.

Presidential Regulation No. 9 of 2024 concerning the Implementation of Education and Training on the Prevention and Handling of the Crime of Sexual Violence.

The 1945 Constitution of the Republic of Indonesia.