

LICS 2026

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

## **Understanding the Various Modes of Human Trafficking That Frequently Ensnare Women and Children in the Digital Era**

**Ari Widodo**

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia,  
E-mail: [arwid76@gmail.com](mailto:arwid76@gmail.com)

**Abstract.** *The advancement of technology and the digital era has facilitated unprecedented access to information. At the same time, however, it has created new centers of vulnerability in the form of cybercrime, one of which is Human Trafficking. Criminal syndicates now exploit the internet and social media as primary tools to identify, recruit, deceive, and exploit victims. Women and children constitute the groups that are disproportionately affected by this crime. This article aims to identify and analyze the various modes of operation of human trafficking that have evolved within the digital environment and to formulate appropriate countermeasures. This study employs a normative juridical research method with a library research approach and is analyzed using descriptive-qualitative techniques. The findings indicate that contemporary trafficking methods in the digital era primarily revolve around cyber grooming, online job scams, sexual exploitation through live-streaming platforms, and romance scams (love scamming). The anonymity of perpetrators and cross-border jurisdictional complexities constitute the most significant challenges to law enforcement. Therefore, strengthening family-based digital literacy, implementing proactive cyber patrols, and harmonizing national and international legal instruments are essential measures to protect women and children from trafficking and exploitation.*

**Keywords:** *Cyber Grooming; Digital Era; Exploitation; Human Trafficking; Protection of Women and Children.*

## 1. Introduction

The rapid development of information and communication technology in the digital era can be likened to a double-edged sword. On one hand, technology accelerates globalization and provides unlimited access to education and economic opportunities. On the other hand, cyberspace has created a highly favorable environment for transnational criminal organizations, particularly those involved in Human Trafficking.

Human trafficking is fundamentally a form of modern slavery that severely violates human dignity and basic human rights.

In the evolution of this crime, perpetrators no longer need to physically monitor or abduct their victims. Instead, they operate behind digital screens under anonymous identities, spreading networks of manipulation through various online platforms. Women and children remain the primary targets and the most vulnerable groups. Economic hardship, inadequate family supervision, and low levels of digital literacy make these groups particularly susceptible to online deception and exploitation.

From a legal perspective, Indonesia has prohibited all forms of human exploitation and trafficking through Law No. 21 of 2007 concerning the Eradication of the Criminal Act of Human Trafficking. Nevertheless, legal regulations often lag behind the rapid evolution of criminal methods. Law enforcement agencies, government institutions, and society can no longer rely solely on conventional approaches. A comprehensive understanding of the evolving modus operandi of human trafficking in the digital era is therefore indispensable for developing effective protection strategies for women and children.

## 2. Research Methods

This study adopts a normative juridical research method using a library research approach. Data collection focuses on the examination of primary legal materials, including legislation related to criminal law, human rights, information technology, and the eradication of human trafficking.

Secondary legal materials were obtained through an extensive review of academic books, scientific journals, and research reports analyzing cybercrime and human trafficking phenomena. The collected data were subsequently analyzed using a descriptive-qualitative approach to explain theoretical findings, examine

**LICS 2026**

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

trafficking modus operandi, and formulate prescriptive conclusions regarding victim protection strategies in the digital era.

### **3. Results and Discussion**

#### **3.1. The Transformation of Human Trafficking Modus Operandi in the Digital Era**

The rapid advancement of digitalization today resembles a double-edged sword. While it facilitates the exchange of information, it has also transformed the modus operandi of human trafficking into a far more sophisticated and alarming phenomenon. Technological advancement has enabled criminal syndicates to design recruitment schemes that are more efficient, cost-effective, and transnational, without requiring physical contact during the initial stages. Unfortunately, women and children continue to occupy the most vulnerable position within this evolving landscape of cybercrime.

Cyberspace provides perpetrators with anonymity, enabling them to exploit the economic and psychological vulnerabilities of potential victims on a massive scale.

One of the most prevalent and dangerous methods is the use of **Online Job Scams**. This scheme specifically targets women of productive age who are experiencing financial hardship or seeking better employment opportunities. Criminal syndicates widely advertise fraudulent job vacancies through social media platforms such as Facebook, Telegram, and Instagram. To attract victims, they promise unrealistic benefits, including exceptionally high salaries, luxurious accommodations, and minimal qualification requirements.

Tragically, once victims arrive at their destination countries, their passports and identity documents are confiscated. Isolated and powerless, they are forced to work as online gambling operators, members of international scam networks, or become victims of sexual exploitation.

In addition to adult women, children and adolescents are increasingly targeted through psychological manipulation tactics known as **Cyber Grooming**. Perpetrators create anonymous social media accounts or infiltrate online gaming chat platforms to approach potential victims. This process is gradual and involves establishing trust through excessive attention, emotional support, and digital gifts.

Once emotional dependency has been established, perpetrators begin requesting intimate photographs or videos. These materials subsequently become tools of blackmail through a practice known as **sextortion**, whereby victims are threatened

#### LICS 2026

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

with public exposure unless they comply with the perpetrators' demands. In many cases, this manipulation ultimately leads to physical exploitation offline.

Another highly manipulative form of trafficking is **Romance Scamming (Love Scamming)**. This method commonly targets adult women, widows, or young women experiencing loneliness or seeking companionship. Perpetrators exploit dating applications to establish seemingly genuine long-distance romantic relationships. Through intensive communication and emotional manipulation, victims gradually lose their critical judgment and become emotionally dependent.

Once the emotional bond has been sufficiently established, perpetrators arrange a meeting, often requiring victims to travel to another region or country. However, what appears to be the culmination of a romantic relationship frequently turns into a nightmare. Upon arrival, victims may be detained, robbed, and subsequently trafficked by organized criminal networks.

Human trafficking has also evolved into a particularly degrading form of exploitation through **Live-Streaming-Based Sexual Exploitation**. Under the guise of talent agencies or opportunities to become "application celebrities," perpetrators recruit women and minors to participate in live-streaming activities. Initially, the content appears harmless; however, victims are gradually pressured through manipulation, debt bondage, or threats to perform sexually explicit acts before a live audience in exchange for virtual gifts or digital currency.

Through these digital platforms, victims are transformed into commodities for international audiences, generating substantial profits for criminal syndicates while inflicting severe psychological and physical trauma upon the victims.

### 3.2. Vulnerability Factors and Challenges of Law Enforcement in Cyberspace

The vulnerability experienced by individuals in the digital environment stems largely from a significant disparity in digital literacy. Although many people possess the technical ability to operate smartphones and social media applications, they often lack an adequate understanding of personal data protection and digital privacy.

Many individuals openly share sensitive information, including home addresses, financial difficulties, and daily routines online, without realizing that such information constitutes valuable intelligence for criminals. This lack of awareness creates substantial vulnerabilities and makes them easy targets for cybercriminal organizations.

## LICS 2026

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

For human trafficking syndicates, personal information scattered across social media serves as a valuable resource for profiling potential victims. By analyzing digital footprints, perpetrators can identify women desperately seeking employment or children experiencing emotional neglect. Once a target has been identified, perpetrators tailor their manipulation strategies accordingly.

Ironically, when victims eventually realize they have been deceived, their digital records such as photographs and private conversations—are often used as instruments of intimidation and extortion to prevent them from reporting the crime.

From a law enforcement perspective, investigators face significant technical challenges in cyberspace. Modern traffickers employ sophisticated methods to conceal their identities, including the use of fake accounts, encrypted communication channels, and Virtual Private Networks (VPNs) that disguise their actual locations.

More sophisticated criminal networks frequently operate within the **Dark Web**, a hidden segment of the internet inaccessible through conventional search engines and protected by advanced encryption technologies. These factors significantly complicate investigative efforts and make the identification and apprehension of perpetrators exceedingly difficult.

These challenges are further exacerbated by the increasing use of **cryptocurrencies**. Traditionally, investigators have relied on the principle of follow the money by tracing financial transactions through banking systems. However, digital trafficking networks increasingly utilize cryptocurrencies, whose decentralized and pseudonymous nature makes financial tracking considerably more difficult.

Another major obstacle concerns **jurisdictional limitations**. Human trafficking cases in the digital era often involve multiple countries. For example, the server hosting an application may be located in Europe, the perpetrator may operate from Southeast Asia, and the victim may reside in Indonesia.

Addressing such crimes requires international cooperation through mechanisms such as **Mutual Legal Assistance (MLA)**. However, MLA procedures are often bureaucratic, time-consuming, and dependent on diplomatic processes. Consequently, victims may continue to suffer exploitation before international legal assistance can be effectively mobilized.

**LICS 2026**

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

### **3.3. Prevention and Protection Strategies**

To combat the continuously evolving forms of human trafficking facilitated by technological advancement, both governments and society must adopt proactive rather than reactive approaches. Waiting until victims have already been harmed before initiating legal action is no longer sufficient.

A preventive-progressive approach is therefore essential. This approach requires the development of preventive mechanisms that are more sophisticated than the tactics employed by criminal organizations, combined with legal measures capable of anticipating emerging threats.

The first and most fundamental strategy is the Strengthening of Family-Based Digital Literacy. The fight against cyber-enabled trafficking must begin within the family. Parents should be equipped with sufficient technological knowledge to supervise and guide their children's online activities effectively.

Education regarding cyber grooming, online manipulation, and methods for verifying online job opportunities should become an integral component of family discussions. Such awareness can significantly reduce vulnerability to fraudulent recruitment schemes.

Digital literacy should also be institutionalized within educational systems. Curricula on **Digital Competence and Online Safety** should be incorporated into primary and secondary education. Through formal education, children can develop critical thinking skills, recognize online threats, and confidently reject inappropriate requests for personal images or information.

At the community level, digital literacy campaigns should be promoted through local organizations, youth groups, and village forums to strengthen collective resilience against trafficking networks.

From a law enforcement perspective, proactive **Cyber Patrols** are essential. The Indonesian National Police, particularly its Cyber Crime Directorate, should not rely solely on victim reports. Instead, authorities must actively monitor cyberspace using big data analytics and artificial intelligence technologies to identify suspicious activities at an early stage.

When indicators of illegal recruitment or child predation are detected, authorities should immediately implement account takedown measures. Rapid intervention can prevent thousands of potential victims from falling into trafficking networks.



## LICS 2026

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

Finally, **Electronic System Operators and Digital Platforms** must be held accountable. Social media companies, messaging service providers, and internet platforms should not evade responsibility by claiming to be merely neutral intermediaries.

Governments should require these companies to integrate advanced Artificial Intelligence (AI) systems capable of automatically detecting grooming behaviors, identifying trafficking-related content, and removing fraudulent job advertisements linked to transnational criminal networks. Failure to implement adequate safety measures should result in substantial sanctions, including significant fines and potential restrictions on operational licenses.

## 4. Conclusion

The digital era has transformed human trafficking into a crime that often begins without physical contact, concealed behind computer and smartphone screens. Methods such as online job scams, cyber grooming, romance scams, and live-streaming-based sexual exploitation have become serious threats to the safety and future of women and children. Indonesia's legal system faces significant challenges due to the anonymity of cybercriminals and the complexity of international jurisdiction. Consequently, cybercrime regulations and data protection laws must continuously evolve to keep pace with criminal innovation. The state must move beyond a reactive approach and implement preventive cyber patrols and proactive interventions. At the same time, society particularly parents must serve as the first line of defense by enhancing supervision of children's online activities. Through collaborative efforts among families, educational institutions, law enforcement agencies, governments, and technology companies, a safer, smarter, and more dignified digital ecosystem can be established for women and children.

## 5. References

### Journals:

- Lestari, M. "Pencegahan Tindak Pidana Perdagangan Orang Berkedok Lowongan Kerja di Era Digital." *Jurnal Kriminologi Indonesia*, Vol. 9, No. 1, 2022, p. 33-48.
- Putri, A. "Perkembangan Modus Operandi Tindak Pidana Perdagangan Orang Melalui Media Sosial." *Jurnal Hukum Pidana dan Kriminologi*, Vol. 4, No. 2, 2021, p. 110-125.



## LICS 2026

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

Rahayu, S. "Literasi Digital sebagai Upaya Preventif Perempuan dari Ancaman Human Trafficking." *Jurnal Studi Gender dan Anak*, Vol. 7, No. 3, 2023, p. 210-225.

Setyawati, D. "Jerat Eksploitasi Seksual Berbasis Online: Analisis Korban Perempuan." *Jurnal HAM*, Vol. 12, No. 2, 2023, p. 78-92.

Wibowo, A. "Tantangan Penegakan Hukum terhadap Cyber Grooming sebagai Pintu Masuk Perdagangan Anak." *Jurnal Perlindungan Anak Indonesia*, Vol. 6, No. 1, 2022, p. 45-60.

## Books:

Arif Gosita. *Masalah Korban Kejahatan*. Jakarta: Bhuana Ilmu Populer, 2004.

Barda Nawawi Arief. *Kapita Selekta Hukum Pidana*. Bandung: Citra Aditya Bakti, 2010.

Farhana. *Aspek Hukum Perdagangan Orang di Indonesia*. Jakarta: Sinar Grafika, 2010.

Harkristuti Harkrisnowo. *Perdagangan Manusia: Kebijakan dan Strategi Penanggulangan*. Jakarta: Pusat Kajian Perlindungan Anak, 2003.

Widodo. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime)*. Yogyakarta: Aswaja Pressindo, 2013.

## Regulation:

Law No. 11 of 2008 in conjunction with 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 the Crime of Sexual Violence.

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

Law No. 39 of 1999 concerning Human Rights.

The 1945 Constitution of the Republic of Indonesia.