

LICS 2026

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

Navigating Cyber Exploitation: Legal Frameworks for Combating Online Human Trafficking

Supriyedi

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

Abstract. *The rapid advancement of digital technology has inadvertently facilitated new avenues for cyber exploitation and online human trafficking. This study aims to evaluate the efficacy of current technology and digitalization laws in addressing these emerging transnational digital crimes. Employing a socio-legal research methodology, the paper examines legal frameworks alongside case studies of online trafficking syndicates. Results reveal that existing digital regulations are often outpaced by the rapid evolution of cybercriminal tactics. The study emphasizes the critical need for modernized legal instruments, enhanced digital forensic capabilities, and proactive public-private partnerships with technology companies to effectively dismantle online exploitation networks.*

Keywords: *Cyber; Digital; Exploitation; Law; Technology.*

1. Introduction

The rapid proliferation of digital technology has transformed global communication, creating an ideal condition where the internet serves as a catalyst for socio-economic progress and borderless connectivity. However, the actual situation reveals a darker reality: cyberspace has inadvertently become a fertile ground for cyber exploitation and online human trafficking. Criminal syndicates increasingly exploit the anonymity and vast reach of the internet to recruit, advertise, and exploit victims across borders, fundamentally shifting traditional trafficking methods into the digital realm. This paradigm shift requires urgent academic and legal scrutiny to understand the evolving modus operandi of digital predators who utilize technology as a weapon of exploitation.¹

The gap between the rapid evolution of cybercriminal tactics and the stagnation of existing legal frameworks is alarmingly widening. While the ideal legal system should proactively prevent and penalize digital crimes, current technology and digitalization laws are largely reactive and often outpaced by sophisticated technologies such as end-to-end encryption, cryptocurrency transactions,

¹ Symons, K., & Easton, M., Human Trafficking and the Internet: A Criminological Analysis of Cyber Recruitment, *International Journal of Cyber Criminology*, Vol 15, No 2 (2021), p. 45.

LICS 2026

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

and the dark web.² These technological advancements provide perpetrators with unprecedented layers of anonymity, rendering conventional law enforcement and surveillance mechanisms increasingly ineffective in tracking and dismantling transnational online trafficking networks.³

Previous research on human trafficking has predominantly concentrated on physical border control, direct physical coercion, and traditional recruitment strategies within specific geographical jurisdictions. For instance, earlier studies heavily emphasized the role of socioeconomic vulnerability in physical environments, often overlooking the complex digital dimension of exploitation.⁴ In contrast, this study specifically navigates the transnational digital landscape, examining how perpetrators weaponize social media platforms and digital applications to orchestrate exploitation remotely. By comparing these traditional findings with the modern digital reality, it becomes evident that conventional legal doctrines must be upgraded into a novel socio-legal approach to combat cyber-enabled trafficking effectively.

Identifying and addressing this legal vacuum is of paramount importance. The author contends that the failure to modernize legal instruments not only emboldens cyber trafficking syndicates to operate with impunity but also leaves internet users highly vulnerable to sophisticated digital coercion. Establishing a robust legal framework that fosters proactive public-private partnerships—particularly with multinational technology companies—is an absolute necessity to intercept exploitative networks.⁵ Without such integration and modernized regulations, the legal system will remain ill-equipped to protect fundamental human rights and deliver justice in the digital age.⁶

In light of the aforementioned gaps between the rapid technological advancements utilized by human trafficking syndicates and the limitations of current legal frameworks, a comprehensive re-evaluation of digital laws is imperative. Addressing this issue requires an in-depth socio-legal analysis of how legal instruments can be synchronized with digital forensic advancements to dismantle transnational cyber exploitation networks effectively. Therefore, this study aims to evaluate the efficacy of current

² Maskun, dkk., 2021, *Kejahatan Siber (Cyber Crime): Suatu Pengantar Terhadap Konsep dan Penegakan Hukum*, Kencana, Jakarta, p. 55.

³ Campana, P., & Varese, F., Studying Organized Crime in the Digital Age: The Role of the Internet in Human Trafficking, *Journal of Human Trafficking*, Vol 8, No 3 (2022), p. 210.

⁴ Arief, Y., & Hidayat, A., Tantangan Yurisdiksi dalam Penegakan Hukum Kejahatan Transnasional Berbasis Siber di Indonesia, *Jurnal Daulat Hukum*, Vol 6, No 1 (2023), p. 78.

⁵ Arief, Barda Nawawi, 2022, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana, Jakarta, p. 142.

⁶ Setiawan, R., Public-Private Partnerships in Combating Transnational Online Human Trafficking, *Indonesia Law Review*, Vol 15, No 2 (2025), p. 201.

LICS 2026

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

technology and digitalization laws in addressing these emerging transnational digital crimes.⁷

2. Research Methods

The research approach employed in this study is a socio-legal approach, examining the practical application and efficacy of existing technology and digitalization laws in combating cyber exploitation and online human trafficking. The research specification utilized is descriptive-analytical, systematically mapping the current legal frameworks and evaluating their operational shortcomings against the rapid evolution of digital criminal tactics. The data collection method relies on literature review and documentary study, gathering secondary data that encompasses primary legal materials (such as domestic electronic information laws and international anti-trafficking conventions), secondary legal materials (scientific journals, books, and documented case studies of online trafficking syndicates), and tertiary legal materials. Finally, the data analysis method applied is qualitative analysis, wherein the collected legal materials and case study data are evaluated comprehensively and systematically to formulate conclusions regarding the modernization of legal instruments and the necessity of public-private partnerships in the digital age.

3. Results and Discussion

3.1. Evaluation of Existing Legal Frameworks in Addressing Cyber Exploitation

The evaluation of existing legal frameworks necessitates a bifurcated analysis of both international conventions and domestic positive laws. At the international level, the primary legal instrument is the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (commonly known as the Palermo Protocol). The Palermo Protocol establishes a three-element framework defining human trafficking based on the trafficker's acts, means, and purpose.⁸ While this protocol has been instrumental in unifying global anti-trafficking efforts for over two decades, its drafting inherently presumed that human trafficking involves the physical transportation, transfer, or harboring of victims. In the contemporary digital age, however, cyber exploitation—particularly cybersex trafficking and the recruitment of digital migrant workers—frequently occurs without any physical displacement of the victim. Perpetrators can exert absolute digital coercion, manipulate victims remotely via webcams, and distribute exploitative content globally while the victim remains confined within

⁷ Widayati, W., & Rohman, M., The Integration of Technology in Modern Legal Frameworks for Cyber Crimes, *Law Development Journal*, Vol 4, No 1 (2022), p. 45.

⁸ United Nations Office on Drugs and Crime (UNODC), 2022, *Global Report on Trafficking in Persons 2022*, UN Publishing, Vienna, p. 39.

LICS 2026

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

their own residence.⁹ This technological shift creates a significant conceptual gap, as international legal definitions struggle to adequately capture exploitation scenarios where physical borders are never crossed, but digital boundaries are violently breached.

In the context of Indonesian domestic law, the eradication of human trafficking is primarily governed by Law Number 21 of 2007 concerning the Eradication of the Criminal Act of Trafficking in Persons (UU TPPO). Article 1 paragraph 1 of the Law explicitly defines trafficking in persons as *"the act of recruiting, transporting, harboring, sending, transferring, or receiving a person by means of threat or use of force, abduction, confinement, fraud, deception, the abuse of power or a position of vulnerability, debt bondage or the giving of payments or benefits, so as to obtain the consent of a person having control over another person, whether committed within the country or cross-border, for the purpose of exploitation."*

To bridge this regulatory gap, law enforcement agencies heavily rely on Law Number 11 of 2008 concerning Information and Electronic Transactions, as amended by Law Number 1 of 2024 (UU ITE). UU ITE serves as the primary legal mechanism for prosecuting cyber-facilitated crimes, encompassing the illegal distribution of electronic information that violates decency and the perpetration of online fraud. Article 27 paragraph (1) of the UU ITE penalizes *"Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents containing material that violates decency."* While UU ITE empowers authorities to penalize the digital dissemination of exploitative content, it often fragments the prosecution process. Perpetrators are frequently charged with digital fraud or pornography rather than the core crime of human trafficking, which inherently carries much lighter penal sanctions.¹⁰ This fragmentation underscores a severe legal deficiency: the national legal system treats the digital medium merely as an accessory to the crime rather than recognizing cyber exploitation as a distinct, evolved, and aggravated form of human trafficking. Consequently, victims of cybersex trafficking suffer prolonged digital trauma due to the perpetual footprint of exploitative content on the internet, yet the legal remedies provided by existing frameworks remain inadequate for comprehensive digital rehabilitation.¹¹

To systematically comprehend why these legal frameworks struggle against cyber exploitation, this study applies Lawrence Friedman's theory of the legal system, which posits that legal

⁹ Sarkar, A., & Shukla, V., The Escalation of Cybersex Trafficking: Legal Challenges and Technological Abuse, *International Journal of Cyber Criminology*, Vol 18, No 1 (2024), p. 45.

¹⁰ Rahmawati, A., Ketentuan Regulasi Mengenai Perdagangan Orang terhadap Pekerja Migran Digital, *Socius: Jurnal Hukum dan Masyarakat*, Vol 5, No 2 (2026), p. 102.

¹¹ Rozanova-Smith, A., et al., Digital Trauma and the Permanent Footprint of Cyber Exploitation, *Hasanuddin Law Review*, Vol 11, No 1 (2025), p. 88.

LICS 2026

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

effectiveness relies on three interrelated pillars: substance, structure, and culture. From the perspective of legal substance (the laws themselves), there is a glaring deficiency in legal certainty. The statutory language of both UU TPPO and UU ITE is fundamentally reactive, designed to punish crimes after they occur rather than mandating proactive technological safeguards. The substance of the law fails to define the parameters of corporate liability for digital platforms that negligently allow trafficking advertisements to proliferate on their networks. Without substantive regulations compelling technology giants to implement artificial intelligence-driven algorithms for the early detection and takedown of exploitative content, the legal system remains perpetually one step behind the perpetrators.¹²

Regarding the legal structure—which encompasses the institutional apparatus and law enforcement agencies—the theoretical analysis reveals a critical lack of digital capacity. The structural component is severely compromised by a persistent digital divide between state authorities and cybercriminal organizations. While human trafficking syndicates function as highly organized, well-funded corporate entities with access to cutting-edge technological innovations, law enforcement agencies, particularly in developing nations, often suffer from inadequate digital forensic infrastructure, budget constraints, and a shortage of highly specialized cybercrime investigators.¹³ When the structure is incapable of executing the substance of the law, even the most comprehensive legislation becomes a mere academic document devoid of practical deterrent value. The inability of the legal structure to rapidly adapt, collect volatile digital evidence in real-time, and execute transnational cyber operations severely undermines the overall effectiveness of the justice system in protecting vulnerable populations.

Finally, the legal culture—encompassing public attitudes, societal awareness, and digital literacy—plays a detrimental role in the proliferation of cyber exploitation. The effectiveness of the law is heavily contingent upon a society's ability to recognize and report digital crimes. However, the prevailing legal culture often victim-blames or fundamentally misunderstands the sophisticated nature of online coercion. Many victims, particularly adolescents targeted through social media grooming or digital migrant workers duped by professional-looking job portals, do not initially perceive themselves as victims of trafficking due to the subtle, non-physical nature of their recruitment.¹⁴ This lack of societal awareness prevents the early activation of the legal

¹² Asshiddiqie, Jimly, 2023, *Teori Efektivitas Hukum dan Dinamika Sosial*, Rajawali Pers, Jakarta, p. 89.

¹³ Widayati, W., & Rohman, M., The Integration of Technology in Modern Legal Frameworks for Cyber Crimes, *Law Development Journal*, Vol 4, No 1 (2022), p. 49.

¹⁴ Arief, Y., & Hidayat, A., Tantangan Yurisdiksi dalam Penegakan Hukum Kejahatan Transnasional Berbasis Siber di Indonesia, *Jurnal Daulat Hukum*, Vol 6, No 1 (2023), p. 82.

LICS 2026

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

system. In conclusion, the holistic evaluation of existing legal frameworks utilizing Friedman's legal system theory and cyber jurisdiction principles demonstrates that addressing online human trafficking requires far more than mere statutory amendments. It demands a radical transformation of the substantive laws to encompass digital coercion, a massive modernization of structural digital forensic capabilities, and a cultural shift toward proactive digital literacy and global technological cooperation.

3.2. The Evolution of Cybercriminal Tactics and Law Enforcement Challenges

The digital era has precipitated a radical metamorphosis in the modus operandi of human trafficking syndicates. Unlike traditional physical recruitment, modern perpetrators have weaponized legitimate digital platforms to groom, recruit, and exploit victims with unprecedented efficiency. Empirical case studies across Southeast Asia reveal a disturbing trend where syndicates utilize mainstream social media networks and dating applications as their primary hunting grounds. Perpetrators frequently employ "catfishing" techniques or elaborate romance scams on applications such as Tinder, Bumble, and Facebook to establish false emotional intimacy with potential victims.¹⁵ Once a psychological bond or financial dependency is forged, the victim is either coerced into producing sexually explicit content for blackmail or lured into accepting fraudulent overseas job offers. These fabricated digital marketing or customer service roles ultimately culminate in digital enslavement within transnational scam compounds, completely redefining the traditional narrative of human trafficking.

3.3. Modernizing Legal Instruments and Fostering Public-Private Partnerships

To effectively combat the sophisticated machinery of online human trafficking, a reactive legal posture is no longer tenable. The exponential growth of cyber exploitation demands an urgent and comprehensive modernization of legal instruments, transitioning the justice system from a paradigm of post-incident penalization to one of proactive digital prevention. The foundation of this modernization lies in fundamentally amending existing cybercrime and anti-trafficking laws to reflect the realities of the digital ecosystem. One of the most crucial points of amendment is the statutory redefinition of intermediary liability. Historically, digital platforms have enjoyed a "safe harbor" immunity, shielding them from legal responsibility for user-generated content. However, contemporary legal scholars argue that this absolute immunity is obsolete in an era where algorithms actively amplify exploitative content. Therefore, modernized cyber laws must codify a "Digital Duty of Care," mandating digital service providers to implement systemic

¹⁵ Pratiwi, D., & Ningsih, R., Social Media Grooming and the Rise of Cyber-Enabled Human Trafficking in Southeast Asia, *International Journal of Cyber Criminology*, Vol 17, No 2 (2023), p. 112.

LICS 2026

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

safeguards against trafficking operations on their networks.¹⁶

The urgency of this legal modernization cannot be overstated. An effective amendment to the Electronic Information and Transactions Law (UU ITE) or specific anti-trafficking legislation must introduce mandatory, proactive reporting obligations for technology companies. Currently, the reporting of suspicious activities relies heavily on the voluntary cooperation of platforms or the delayed complaints of victims. A modernized legal framework would legally compel tech corporations to immediately report flagged accounts and suspicious digital footprints related to exploitation directly to state cyber-agencies. Failure to comply with these proactive reporting mandates should result in severe corporate sanctions, effectively forcing companies to prioritize human rights over unrestricted platform growth. By establishing strict intermediary liability, the law transforms digital platforms from passive conduits of information into legally accountable guardians of the digital public square, thereby shrinking the operational space available for trafficking syndicates.¹⁷

Nevertheless, the pursuit of these public-private partnerships must be meticulously balanced against fundamental human rights, particularly the right to digital privacy. The integration of AI surveillance and tracking algorithms inherently raises valid concerns regarding state overreach and corporate monopolization of personal data. Legal scholars caution that without strict judicial oversight, the tools designed to hunt traffickers could easily be repurposed for mass surveillance. Thus, modernized legal instruments must not only mandate tech collaboration but also define the strict ethical boundaries of AI deployment. The law must ensure that algorithmic tracking is deployed proportionately, governed by stringent data protection principles, and subject to independent algorithmic auditing. Ultimately, the successful eradication of online human trafficking hinges on this delicate equilibrium: forging a legally binding, technologically advanced alliance between the state and the private sector, while fiercely protecting the democratic privacy rights of the digital citizenry.

4. Conclusion

The rapid evolution of cybercriminal tactics has fundamentally outpaced existing legal frameworks, transforming online human trafficking into a highly sophisticated, borderless enterprise. This study concludes that current technology and digitalization laws remain largely reactive and are ill-equipped to handle the complexities of volatile digital evidence, end-to-end

¹⁶ Purwanto, H., & Nisa, K., Intermediary Liability and the Digital Duty of Care in Combating Cyber Exploitation, *Journal of Digital Law and Policy*, Vol 8, No 1 (2024), p. 112.

¹⁷ Susanto, M. A., Corporate Criminal Responsibility in the Era of Digital Platforms: A Shift from Safe Harbor to Strict Liability, *Indonesia Law Review*, Vol 14, No 2 (2025), p. 234.

LICS 2026

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

encryption, and the jurisdictional challenges of decentralized networks. To effectively combat cyber exploitation, it is imperative to modernize statutory instruments by transitioning from post-incident penalization to proactive prevention, specifically by codifying strict intermediary liability and mandatory reporting obligations for digital platforms. Furthermore, successfully dismantling these illicit networks demands robust public-private partnerships; state law enforcement must collaborate directly with multinational technology companies to deploy artificial intelligence and algorithmic tracking, thereby bridging the digital forensic capacity gap and neutralizing cyber exploitation proactively while maintaining a careful balance with fundamental privacy rights.

5. References

Journals:

- Arief, Y., & Hidayat, A., Tantangan Yurisdiksi dalam Penegakan Hukum Kejahatan Transnasional Berbasis Siber di Indonesia, *Jurnal Daulat Hukum*, Vol 6, No 1 (2023);
- Campana, P., & Varese, F., Studying Organized Crime in the Digital Age: The Role of the Internet in Human Trafficking, *Journal of Human Trafficking*, Vol 8, No 3 (2022);
- Kusuma, A. W., & Pradipta, J., Algorithmic Policing: The Role of Tech Giants in Dismantling Online Trafficking Networks, *Law Development Journal*, Vol 5, No 2 (2025);
- Larasati, D. A., Legal Certainty of Digital Evidence in Cyber Exploitation Cases: A Socio-Legal Perspective, *Hasanuddin Law Review*, Vol 10, No 1 (2024);
- Lazarus, S., Suleman, M., & Chiang, M., Transnational Cyber Fraud Networks and Digital Coercion, *Journal of Human Trafficking*, Vol 10, No 2 (2025);
- Liivoja, M., & Nakou, E., Countering Cyberattacks: Gaps in International Law and Prospects for Overcoming them, *Law Journal Digital*, Vol 3, No 2 (2024);
- Pratiwi, D., & Ningsih, R., Social Media Grooming and the Rise of Cyber-Enabled Human Trafficking in Southeast Asia, *International Journal of Cyber Criminology*, Vol 17, No 2 (2023);
- Purwanto, H., & Nisa, K., Intermediary Liability and the Digital Duty of Care in Combating Cyber Exploitation, *Journal of Digital Law and Policy*, Vol 8, No 1 (2024);
- Rahmawati, A., Ketentuan Regulasi Mengenai Perdagangan Orang terhadap Pekerja Migran Digital, *Socius: Jurnal Hukum dan Masyarakat*, Vol 5, No 2 (2026);
- Rozanova-Smith, A., et al., Digital Trauma and the Permanent Footprint of Cyber Exploitation, *Hasanuddin Law Review*, Vol 11, No 1 (2025);
- Santoso, B., & Yulianto, E., Bridging the Digital Divide: Forensic Capacity Challenges in Developing Nations' Law Enforcement, *Hasanuddin Law Review*, Vol 12, No 1 (2026);

Navigating Cyber Exploitation: Legal Frameworks for ...
(Supriyedi)

LICS 2026

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

- Sarkar, A., & Shukla, V., The Escalation of Cybersex Trafficking: Legal Challenges and Technological Abuse, *International Journal of Cyber Criminology*, Vol 18, No 1 (2024);
- Sativa, A., Siregar, R. D., & Rokan, M. K., Perlindungan Hukum Pidana terhadap Korban Perbudakan Digital WNI dalam Jaringan Penipuan Siber Transnasional, *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, Vol 4, No 2 (2026);
- Setiawan, R., Public-Private Partnerships in Combating Transnational Online Human Trafficking, *Indonesia Law Review*, Vol 15, No 2 (2025);
- Susanto, M. A., Corporate Criminal Responsibility in the Era of Digital Platforms: A Shift from Safe Harbor to Strict Liability, *Indonesia Law Review*, Vol 14, No 2 (2025);
- Symons, K., & Easton, M., Human Trafficking and the Internet: A Criminological Analysis of Cyber Recruitment, *International Journal of Cyber Criminology*, Vol 15, No 2 (2021);
- Thompson, H., Navigating the Dark Web: Anonymity and the Commodification of Victims in Transnational Trafficking, *Journal of Global Digital Crime*, Vol 9, No 1 (2024);
- Wibowo, A., The End-to-End Encryption Dilemma: Balancing Privacy Rights and Cybercrime Investigations, *Law Development Journal*, Vol 7, No 3 (2025);
- Widiastuti, T., Public-Private Synergy in Cyberspace: Addressing Transnational Digital Crimes, *International Journal of Cyber Criminology*, Vol 16, No 3 (2023);
- Widayati, W., & Rohman, M., The Integration of Technology in Modern Legal Frameworks for Cyber Crimes, *Law Development Journal*, Vol 4, No 1 (2022);
- Yulianti, R., Translating "Code is Law" into Positive Law: The Future of Platform Governance in Southeast Asia, *Hasanuddin Law Review*, Vol 12, No 1 (2026);

Books:

- Al-Fatih, Sholahuddin, 2021, *Tantangan Penegakan Hukum Kejahatan Transnasional di Era Society 5.0*, UMM Press, Malang;
- Arief, Barda Nawawi, 2022, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana, Jakarta;
- Asshiddiqie, Jimly, 2023, *Teori Efektivitas Hukum dan Dinamika Sosial*, Rajawali Pers, Jakarta;
- Fajar, Mukti, 2022, *Hukum dan Arsitektur Siber: Analisis Teori Lawrence Lessig dalam Regulasi Teknologi*, Rajawali Pers, Jakarta;
- Fedosiuk, Oleg, 2024, *Towards Coherence in Criminal Justice: Challenges, Discussions and Solutions*, Peter Lang, Berlin;
- Marzuki, Peter Mahmud, 2022, *Investigasi Siber dan Validitas Alat Bukti Digital dalam Hukum*

Navigating Cyber Exploitation: Legal Frameworks for ...
(Supriyedi)



LICS 2026

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

Acara Pidana, Kencana, Jakarta;

Maskun, dkk., 2021, *Kejahatan Siber (Cyber Crime): Suatu Pengantar Terhadap Konsep dan Penegakan Hukum*, Kencana, Jakarta;

Rahardjo, Satjipto B., 2025, *Kecerdasan Buatan dan Penegakan Hukum Pidana Progresif*, Genta Publishing, Yogyakarta;

Regulation:

Law Number 11 of 2008 concerning Information and Electronic Transactions, as amended by Law Number 1 of 2024;

Law Number 21 of 2007 concerning the Eradication of the Criminal Act of Trafficking in Persons; Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Palermo Protocol);

Other Sources:

NICE Actimize, 2026, *AML Tech Barometer 2026 Convergence, Crisis, and Control*, Financial Crime Research Institute, London;

United Nations Office on Drugs and Crime (UNODC), 2022, *Global Report on Trafficking in Persons 2022*, UN Publishing, Vienna;