

Article

Illegal Online Gambling as Cyber Economic Crime in Indonesia and Southeast Asia

Siti Nurul Indah Cahyani

¹Master of Law, Faculty of Law, Universitas Pancasila, Jakarta, Indonesia

Article information	Abstract
DOI : xxx Correspondence :	Illegal online gambling has developed into a cyber-enabled form of economic crime with substantial consequences for financial systems, money laundering, and transnational organized crime throughout Southeast Asia. This study examines the regulatory framework, effectiveness of law enforcement, and patterns of illicit financial flows associated with online gambling in Indonesia and the wider Southeast Asian region. It employs a systematic review methodology integrated with a normative legal approach and comparative analysis of relevant legislation, academic literature, reports issued by the Indonesian Financial Transaction Reports and Analysis Center, and publications of the United Nations Office on Drugs and Crime. The findings indicate that, although Indonesia has established a legal basis through the Indonesian Criminal Code, the Electronic Information and Transactions Law, and the formation of the Task Force for the Eradication of Online Gambling, law-enforcement efforts remain limited by regulatory inconsistencies, inadequate digital-forensic capabilities, and the cross-border structure of online gambling networks. Moreover, illicit proceeds generated through online gambling are increasingly connected to money-laundering activities and transnational cybercrime. These developments highlight the need for a more integrated and coordinated strategy to address illegal online gambling and its related financial and cyber threats. The study recommends harmonizing regulatory frameworks, enhancing digital-forensics-based law-enforcement capacity, strengthening financial-intelligence mechanisms, and expanding cooperation among ASEAN member states to improve the detection, investigation, disruption, and prosecution of illegal online gambling networks and associated financial crimes.
Submission Track	
Submission : April 12, 2026 Final Review : May 15, 2026 Accepted : May 18, 2026	
Keywords	
illegal online gambling, cyber-enabled economic crime, law enforcement, money laundering, illicit financial flows	
 This is an open access article under the CC BY https://creativecommons.org/licenses/by/4.0/	

INTRODUCTION

The rapid advancement of information and communication technologies has transformed economic and social activities while also creating conditions that enable increasingly sophisticated forms of technologically mediated crime (Loughlin, 2026; Samphy et al., 2025). Among these emerging threats, illegal online gambling has become a particularly significant transnational form of cyber-enabled economic crime (Budairti & Patodongi, 2025; Huang et al., 2022; Mawardi et al., 2026). Unlike traditional gambling, online gambling operates through digital platforms that can be established, modified, and relocated across jurisdictions with considerable speed. Virtual private networks, offshore servers, encrypted communications, digital payment systems, and continuously changing domain names allow operators to evade national regulatory controls, obscure financial transactions, and conceal the identities of the individuals and entities directing these operations. These characteristics demonstrate that illegal online gambling is not merely a violation of gambling regulations; it is a multidimensional criminal enterprise

that can facilitate financial crime, money laundering, cyber fraud, and, in certain cases, transnational organized crime (Haribowo et al., 2025; Widijowati et al., 2025). Accordingly, treating the phenomenon solely as a conventional gambling offense risks understating its technological sophistication, economic scale, and broader implications for cybersecurity, financial integrity, and public security. Current legal instruments, such as the Electronic Information and Transactions Law and the prevailing Criminal Code, often prove inadequate due to their reactive nature and reliance on outdated definitions that fail to address the complexity of modern cyber-based delinquency (Anggoro & Santoso, 2025).

Indonesia provides a particularly important case for examining this phenomenon because it demonstrates the substantial gap between formal prohibition and effective control. Although online gambling is explicitly prohibited under Indonesian law and widely rejected within prevailing social norms, its scale has expanded dramatically over the past decade. The Indonesian Financial Transaction Reports and Analysis Center recorded an increase in the value of transactions associated with online gambling from approximately IDR 155.4 trillion in 2022 to IDR 327 trillion in 2023, followed by a further increase to approximately IDR 359 trillion in 2024. This escalation indicates that conventional legal prohibitions and institutional controls have been insufficient to contain digitally mediated criminal activities. More significantly, the volume and rapid growth of these transactions suggest that illegal online gambling has moved beyond isolated individual conduct and developed into an organized economic ecosystem capable of generating, transferring, and disguising substantial illicit financial flows (Loughlin, 2026; Mawardi et al., 2026). Accordingly, the Indonesian case supports the argument that online gambling should be addressed not merely as a moral or regulatory violation, but as a cyber-enabled economic crime requiring coordinated financial, technological, and transnational law-enforcement responses.

The implications extend far beyond gambling-related offenses. Illegal online gambling platforms increasingly function as enabling infrastructure for broader forms of cyber-enabled and organized crime, including money laundering, cyber fraud, human trafficking, and illicit financial transfers (Frăsilă, 2025; Loughlin, 2026). The United Nations Office on Drugs and Crime reported in 2024 that online gambling platforms in Southeast Asia were increasingly exploited by transnational criminal organizations to move, integrate, and conceal illicit proceeds. The estimated losses from cyber-enabled fraud in Southeast Asia reached between USD 18 billion and USD 37 billion in 2023 alone, illustrating the scale of the financial threat associated with these interconnected criminal ecosystems. In Indonesia, PPATK has likewise identified suspicious financial flows linked to online gambling that extend beyond national borders to Thailand, Cambodia, and the Philippines, as well as to offshore financial jurisdictions. These cross-border flows demonstrate that illegal online gambling is not an isolated violation of gambling law; it constitutes a broader threat to the integrity, transparency, and security of national and regional financial systems. Accordingly, an effective response must address not only the operation of gambling platforms but also the financial channels, digital infrastructures, and criminal networks that enable them to operate. Furthermore, addressing the systemic nature of these operations requires integrating banking fraud countermeasures, as perpetrators frequently utilize sophisticated financial layering techniques to facilitate illicit capital flight (Pasha & Mulyana, 2025).

Indonesia has nevertheless established a relatively extensive legal and institutional framework to address illegal gambling. Gambling is prohibited under Articles 303 and 303 bis of the Indonesian Criminal Code (KUHP), while its digital dimension has been addressed through Article 27(2) of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), as subsequently amended, most recently through Law No. 1 of 2024. The 2024 amendment reinforced the criminal sanctions applicable to online gambling, including imprisonment of up to six years and/or a maximum fine of IDR 1 billion. At the institutional level, the Indonesian government established the Task Force for the Eradication of Online Gambling through Presidential Decree No. 21 of 2024, signed on June 14, 2024, with a mandate to strengthen integrated prevention and law enforcement across ministries and government institutions. These developments indicate that Indonesia has progressively recognized online gambling as a complex

digital governance and law-enforcement challenge rather than merely a conventional criminal offense.

Despite these regulatory developments, the persistence and expansion of illegal online gambling indicate a significant gap between regulatory design and enforcement effectiveness. Existing studies have identified potential disharmony between the new Criminal Code and the ITE Law, particularly concerning the attribution of criminal responsibility to online gambling operators and other dominant actors within gambling networks (Adlina, 2025; Bentara et al., 2025; Okta & Vera, 2026). This regulatory fragmentation can create uncertainty regarding the applicable legal provisions, investigative procedures, and prosecution strategies. At the operational level, online gambling networks continuously adapt their technological and financial strategies to evade detection. The use of VPNs, overseas servers, encrypted communication channels, frequently changing domains, multiple bank accounts, and alternative digital payment mechanisms creates substantial challenges for investigators (Gulyamov, 2025; Mawardi et al., 2026; Uzougbo et al., 2024). The effectiveness of law enforcement is further constrained by limited digital-forensic capabilities, difficulties in tracing cross-border financial transactions, jurisdictional barriers, and fragmented coordination among relevant government institutions.

The challenges become even more pronounced when the Indonesian case is situated within the broader Southeast Asian context. The region has developed a complex transnational ecosystem in which illegal online gambling, cyber fraud, money laundering, human trafficking, and organized crime operate through interconnected networks rather than as isolated offenses. The Mekong subregion, particularly Myanmar, Laos, and Cambodia, has emerged as a major center for transnational criminal activities associated with online gambling and cyber-enabled fraud. These activities have been facilitated by corruption, weak institutional governance, limited regulatory oversight, and the exploitation of Special Economic Zones as locations for criminal enterprises (Loughlin, 2026; Uhm & Zhang, 2022). Special Economic Zones can provide criminal networks with concentrated infrastructure, access to casinos and digital-payment systems, weak or fragmented oversight, and proximity to multiple jurisdictions, thereby enabling them to conceal operations, move illicit funds, and rapidly adapt to enforcement pressure. The regional experience therefore demonstrates that illegal online gambling cannot be effectively addressed through isolated national enforcement measures: criminal networks can relocate their infrastructure, personnel, financial channels, and digital operations across borders whenever domestic controls become more effective. Consequently, the persistence of online gambling networks reflects not only weaknesses in individual national laws but also the absence of coordinated regional mechanisms for information sharing, financial monitoring, digital investigation, and cross-border prosecution. Such transnational criminal syndicates intentionally exploit these jurisdictional gaps and regulatory inconsistencies to construct fluid, decentralized operational models that prioritize resilience against state intervention (Laras & Rusdiyanta, 2025). From the perspective of Regional Security Complex Theory, this state of undersecuritization among ASEAN member states prevents the formation of a unified regional agenda necessary to counter these threats (Novianto & Asri, 2026).

The experience of the Philippines further illustrates the limitations and unintended consequences of permissive regulatory environments. Philippine Offshore Gaming Operators (POGOs) developed into a substantial online gambling industry before concerns regarding their links to organized crime, money laundering, human trafficking, and other illicit activities contributed to the government's decision to prohibit them nationwide in 2024 through Executive Order No. 74 (Sriyai & Arugay, 2025). The Philippine case demonstrates how legally tolerated or insufficiently regulated digital gambling ecosystems can potentially be exploited by criminal networks and subsequently generate significant governance, security, and financial risks. Collectively, these developments across Southeast Asia highlight the importance of examining illegal online gambling through a regional and transnational framework rather than treating it exclusively as a domestic criminal-law issue.

Nevertheless, the existing literature remains fragmented across several disciplinary domains. Legal studies tend to focus primarily on the interpretation and application of national gambling regulations,

while cybersecurity research emphasizes technological vulnerabilities and digital investigation. Financial-crime research, in contrast, focuses on suspicious transactions and money-laundering mechanisms, whereas studies of transnational organized crime emphasize criminal networks and cross-border operations. Consequently, there remains a need for an integrated analysis connecting regulatory frameworks, law-enforcement effectiveness, digital-financial flows, and the transnational structure of illegal online gambling networks in Indonesia and Southeast Asia. In particular, insufficient attention has been given to how regulatory fragmentation and technological adaptation interact with cross-border financial mechanisms to undermine national enforcement efforts.

This study addresses this gap by systematically reviewing and comparatively analyzing the regulatory and law-enforcement dimensions of illegal online gambling in Indonesia and Southeast Asia. It examines three interrelated questions: (1) how existing legal and regulatory frameworks address illegal online gambling and its associated economic crimes; (2) what institutional, technological, and jurisdictional factors limit the effectiveness of law enforcement; and (3) how illicit financial flows associated with online gambling are connected to money laundering and transnational cybercrime across Southeast Asia. By integrating a normative legal approach with a systematic review and comparative regional analysis, the study seeks to move beyond a narrow examination of gambling prohibition and provide a broader understanding of illegal online gambling as a form of cyber-enabled economic crime.

METHODOLOGY

Research Approach

This study employs a normative legal research approach combined with a comparative legal analysis. Normative legal research is appropriate for examining legal norms, statutory provisions, regulatory frameworks, legal principles, and institutional policies governing illegal online gambling and its associated cyber-enabled economic crimes. The study focuses primarily on the analysis of existing legal instruments and authoritative legal and policy documents rather than on the collection of primary empirical data.

The normative approach is complemented by a comparative perspective to examine how Indonesia's regulatory and law-enforcement framework addresses illegal online gambling in comparison with selected Southeast Asian jurisdictions. This comparative analysis is intended to identify similarities, differences, regulatory gaps, and potential areas for policy harmonization in addressing the transnational nature of illegal online gambling.

The study also incorporates relevant empirical and institutional evidence, including financial-intelligence reports, government publications, and reports from international organizations, to provide contextual support for the legal analysis. Accordingly, the research does not treat illegal online gambling solely as a conventional criminal-law issue but examines it as a cyber-enabled economic crime involving regulatory, technological, financial, and transnational dimensions.

Legal and Documentary Sources

The sources analyzed in this study consist of three principal categories.

- First, primary legal sources include Indonesian legislation and other authoritative legal instruments relevant to online gambling, cybercrime, financial crime, and law enforcement. These include the Indonesian Criminal Code (KUHP), Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), as amended by Law No. 1 of 2024, Presidential Decree No. 21 of 2024 concerning the Task Force for the Eradication of Online Gambling, and other relevant laws and regulations governing financial transactions, money laundering, electronic systems, and digital activities.
- Second, secondary legal and academic sources include scholarly books, peer-reviewed

journal articles, legal commentaries, academic publications, and previous research concerning illegal online gambling, cybercrime, money laundering, transnational organized crime, digital financial crime, and law enforcement in Indonesia and Southeast Asia. Particular attention is given to literature published between 2019 and 2025 to capture recent developments in digital technology, criminal practices, and regulatory responses.

- Third, authoritative institutional and policy sources include official reports and publications issued by Indonesian government institutions and reputable international organizations. These include reports from the Indonesian Financial Transaction Reports and Analysis Center (PPATK), relevant Indonesian ministries and government institutions, the United Nations Office on Drugs and Crime (UNODC), the ISEAS–Yusof Ishak Institute, and the Center for Strategic and International Studies (CSIS). These sources are used to contextualize the legal analysis with evidence concerning financial flows, criminal networks, enforcement challenges, and regional developments.

Priority is given to authoritative and verifiable sources, particularly official legislation, government documents, institutional reports, and peer-reviewed academic publications.

Legal Material Collection

Legal materials and supporting documents were collected through examination of official legal databases, government websites, institutional repositories, and academic publications. Relevant Indonesian legislation was obtained primarily from official government legal information portals, while institutional reports were accessed through the official websites of the organizations concerned.

The identification of relevant legal materials was guided by key legal and conceptual terms, including *illegal online gambling*, *online gambling regulation*, *cybercrime*, *cyber-enabled economic crime*, *money laundering*, *illicit financial flows*, *online gambling law enforcement*, and *transnational organized crime*.

The collected materials were subsequently classified according to their legal status and substantive relevance. Primary legal materials were distinguished from secondary academic literature and supporting institutional documents to ensure that legal conclusions were grounded primarily in authoritative legal sources.

Legal Analysis

The analysis was conducted using qualitative juridical analysis. The collected legal materials were examined through interpretation of statutory provisions, identification of relevant legal principles, and assessment of the relationship between different regulatory instruments.

The analysis focused on four principal dimensions:

- Regulatory framework: examining the legal provisions governing illegal online gambling and associated cyber and financial crimes.
- Law-enforcement effectiveness: assessing the extent to which existing legal provisions can be implemented effectively by relevant law-enforcement institutions.
- Illicit financial flows: examining the legal and institutional mechanisms available for identifying, tracing, freezing, and disrupting financial proceeds associated with online gambling.
- Transnational dimensions: analyzing the challenges created by cross-border gambling networks, foreign digital infrastructure, international financial transfers, and differences between national regulatory regimes.

The analysis does not rely solely on the existence of statutory provisions but also considers their practical implementation and the institutional conditions affecting their enforcement. This enables the study to distinguish between formal legal adequacy and practical enforcement effectiveness.

Comparative Legal Analysis

A comparative legal approach is employed to place Indonesia's regulatory framework within the broader Southeast Asian context. Selected jurisdictions, particularly countries that have experienced significant challenges associated with illegal online gambling and related cybercrime, are examined for their regulatory approaches, institutional responses, and enforcement mechanisms.

- The comparison considers several dimensions, including:
- legal status and regulation of online gambling;
- criminal liability and applicable sanctions;
- institutional mechanisms for enforcement;
- regulation of digital and financial transactions;
- anti-money-laundering mechanisms;
- cross-border cooperation;
- approaches to online gambling platforms and operators; and
- regulatory responses to organized criminal networks.

The comparative analysis is not intended to establish that one national legal system is universally superior to another. Rather, it is used to identify regulatory patterns, institutional strengths and weaknesses, and practices that may provide useful lessons for strengthening Indonesia's legal and policy framework.

RESULTS AND DISCUSSION

Regulatory Framework and Law-Enforcement Effectiveness in Addressing Illegal Online Gambling in Indonesia and Southeast Asia

Indonesia's Regulatory Framework

Indonesia has established a multilayered legal framework to prohibit and combat illegal online gambling. At the level of general criminal law, Articles 303 and 303 bis of the Indonesian Criminal Code (KUHP) have long provided the legal basis for prosecuting gambling offenses. With the emergence of digital technologies, the cyber dimension of gambling has subsequently been addressed through Article 27(2) of the Law on Electronic Information and Transactions (ITE Law), which prohibits the distribution, transmission, or making available of electronic information containing gambling content. The latest amendment, introduced through Law No. 1 of 2024, further strengthens the applicable sanctions and expands the range of potentially liable actors, including individuals who promote or endorse online gambling activities and operators or owners of gambling websites (Achmadi & Suciyani, 2026). However, persistent discrepancies between the provisions of the Criminal Code and the Electronic Information and Transactions Law continue to generate legal uncertainty, thereby impeding the efficacy of law enforcement efforts (Adlina, 2025). Furthermore, these challenges are compounded by systemic obstacles in inter-agency coordination and technological limitations that hinder the identification and prosecution of complex digital gambling syndicates (Saputra & Arianto, 2025).

Despite the existence of these multiple legal instruments, the literature indicates that Indonesia's regulatory framework continues to face significant challenges arising from legal fragmentation and regulatory disharmony. The new Criminal Code, which is scheduled to enter into full effect in 2026, regulates gambling offenses under Articles 426 and 427. However, these provisions do not explicitly establish gambling operators or bookmakers as the primary category of offenders whose prosecution should receive particular priority. This may weaken the capacity of the criminal justice system to target the dominant actors who organize and financially benefit from online gambling networks (Achmadi & Suciyani, 2026). Moreover, the absence of specific legal definitions regarding online participants complicates the prosecution of users, creating a significant enforcement gap that undermines the

deterrent impact of current sanctions (Arum & Sumardiana, 2025). Consequently, addressing these loopholes requires a cohesive integration of the Electronic Information and Transactions Law with the upcoming Criminal Code to ensure comprehensive liability for both platform operators and individual facilitators (Mahmudi et al., 2025; Samosir et al., 2025).

At the same time, Article 27(2) of the ITE Law places substantial emphasis on the distribution and accessibility of electronic gambling content rather than comprehensively addressing the broader criminal structure underlying online gambling operations. This creates considerable room for differing interpretations in law-enforcement practice (Silalahi et al., 2024). The resulting fragmentation can generate inconsistencies in prosecution, particularly when investigators and prosecutors must determine whether a case should primarily be pursued under the KUHP, the ITE Law, or through the combined application of both legal instruments. These operational difficulties are further exacerbated by the cross-border nature of these digital networks, which frequently utilize foreign infrastructure to bypass domestic blocking attempts (Fadhli, 2024). Furthermore, the reliance on website blocking often proves insufficient as a deterrent due to the rapid emergence of mirror sites and decentralized hosting solutions that complicate permanent digital forensic intervention (Juhara et al., 2025).

This issue is particularly important because online gambling networks are structurally different from conventional gambling activities. A single operation may involve platform owners located in one jurisdiction, technical infrastructure hosted in another, financial intermediaries operating elsewhere, and promoters or agents located within Indonesia. Consequently, a regulatory framework that focuses primarily on the immediate act of distributing gambling content may have limited effectiveness in identifying and prosecuting the individuals who control the broader criminal ecosystem.

In response to the escalation of online gambling, the Indonesian government has introduced a more coordinated institutional mechanism. Presidential Decree No. 21 of 2024 established the Task Force for the Eradication of Online Gambling, bringing together multiple ministries and government institutions, including the Ministry of Communication and Informatics, the Indonesian National Police, PPATK, the Financial Services Authority (OJK), and the State Intelligence Agency (BIN). The Task Force has three principal responsibilities: strengthening prevention and law enforcement; improving inter-agency coordination and international cooperation; and formulating strategic policy recommendations. This multisectoral approach aims to address the inherent difficulties in tracing illegal digital transactions and bypassing cross-border jurisdictional barriers that have historically impeded successful investigations (Elthaufani & Cumbrandika, 2026).

The establishment of the Task Force represents an important institutional shift from fragmented enforcement toward a more integrated model of digital-crime governance. Its operational outcomes also demonstrate substantial enforcement activity. Between July 2023 and July 2024, the Directorate of Informatics Application Control reportedly blocked more than 2.6 million items of online gambling content and submitted requests for the blocking of approximately 573 electronic-wallet accounts and 6,199 bank accounts to Bank Indonesia and the OJK. These measures demonstrate the government's increasing use of administrative, technological, and financial interventions alongside conventional criminal enforcement.

However, the scale of blocking activity should not automatically be interpreted as evidence of successful eradication. Content blocking can disrupt access to gambling platforms, but it does not necessarily dismantle the underlying financial infrastructure, criminal organizations, or cross-border networks responsible for operating those platforms. The continued emergence of new domains, accounts, payment channels, and mirror websites suggests that online gambling networks possess considerable adaptive capacity.

Empirical evidence from the Medan City Police further illustrates this enforcement dilemma. Reported online gambling cases declined from 40 cases in 2020 to only 5 cases in 2023, partly in

the context of shifting law-enforcement priorities during the COVID-19 pandemic and limited public reporting. However, reported cases subsequently increased to 40 cases in 2024 and reached 46 cases in 2025, representing an increase of approximately 820% compared with 2023. This volatility indicates that reported case numbers alone cannot be interpreted as a straightforward measure of either the prevalence of online gambling or the success of law enforcement. Instead, the fluctuations may reflect changes in enforcement intensity, reporting behavior, investigative priorities, and the adaptability of criminal networks (Ahyani et al., 2024).

These findings reveal weaknesses across several dimensions. At the level of legal substance, overlapping and partially fragmented provisions may create uncertainty in enforcement. At the level of law-enforcement institutions, inter-agency coordination remains essential because online gambling simultaneously involves criminal law, telecommunications, financial transactions, cybersecurity, and intelligence. In terms of facilities and infrastructure, digital-forensic capabilities and real-time financial tracing remain critical. Finally, the societal and cultural dimensions of law effectiveness indicate that enforcement cannot rely exclusively on blocking websites and prosecuting individual offenders; sustained public awareness, digital literacy, and mechanisms for reporting suspicious activities are also necessary (Atkins & Huang, 2013; Collier et al., 2023; Popoola et al., 2024). Ultimately, addressing the root causes requires an integrated strategy that moves beyond reactive digital interventions to include proactive socioeconomic education and robust international collaboration to counteract the decentralized nature of these syndicates (Sunarto et al., 2025; Wijaya, 2025).

Therefore, Indonesia's principal challenge is no longer simply the absence of legal prohibitions. Rather, the central issue is the capacity to translate an extensive formal legal framework into coordinated, technologically capable, financially informed, and transnationally effective enforcement.

Comparative Regulatory Approaches in Southeast Asia

At the regional level, Southeast Asia presents a highly fragmented regulatory landscape for online gambling. Differences in national legislation, licensing regimes, enforcement capacity, and attitudes toward gambling create regulatory asymmetries that can be exploited by organized criminal networks. The Centre for Strategic and International Studies (CSIS) noted in its 2024 analysis that online gambling presents serious risks to individual ASEAN member states and to the region as a whole, primarily because of the transnational nature of these operations, weaknesses in national governance, and fragmentation within the ASEAN regulatory environment (Azis & Azhari, 2025). These inconsistencies allow operators to relocate server infrastructures and financial clearinghouses to jurisdictions with more permissive legal environments, thereby complicating regional cooperation (Firmansyah, 2025; Saripudin et al., 2025). Consequently, the absence of a harmonized regional framework necessitates the development of specialized cross-border data-sharing agreements and unified standards for digital financial monitoring to mitigate the exploitation of these jurisdictional gaps (Sulthanah & Ginting, 2025).

This regulatory fragmentation creates what may be described as a jurisdictional arbitrage problem. Criminal networks can relocate their servers, financial operations, personnel, and corporate structures to jurisdictions where regulatory oversight is weaker or enforcement is less effective. Consequently, stronger regulation in one country may simply displace rather than eliminate the underlying criminal activity.

The Philippines provides one of the most instructive examples of the consequences of a relatively permissive regulatory environment. The Philippine Offshore Gaming Operators (POGO) framework was initially promoted as a source of tax revenue and employment. However, the sector subsequently became associated with allegations and investigations involving organized crime, cyber fraud, kidnapping, human trafficking, and money laundering. Philippine authorities reported that the economic contribution of POGOs was considerably smaller than initially anticipated, while the associated social, security, and reputational costs became increasingly significant. The government ultimately moved toward a

nationwide prohibition, with President Ferdinand Marcos Jr. announcing the ban in his 2024 State of the Nation Address, followed by the formalization of the policy through Executive Order No. 74 later that year (Sriyai & Arugay, 2025). This shift underscores the inherent difficulties of balancing state economic interests against the rising security threats posed by transnational criminal syndicates, which frequently exploit the “ASEAN Way” to maintain operations amidst uneven national legal landscapes (Bangun & Kinanti, 2025; Wiwoho et al., 2023). This evolution in state policy highlights that such criminal enterprises now exhibit advanced industrialization and comprehensive platformization, rendering traditional localized enforcement insufficient (Gao & Zhilin, 2025).

The Philippine experience demonstrates an important regulatory lesson: economic incentives associated with digital gambling must be evaluated against the potential externalities generated by criminal exploitation of the sector. A licensing framework may generate legitimate fiscal benefits, but if regulatory oversight is insufficient, the same infrastructure can potentially be appropriated by criminal organizations for money laundering, fraud, trafficking, and other illicit activities. Furthermore, the strategic implementation of international standards—such as those promoted by the Financial Action Task Force—serves as a critical mechanism to mitigate these vulnerabilities by forcing states to prioritize legislative tightening and oversight (Morse, 2022).

Thailand presents a different but related regulatory challenge. The country has periodically considered the legalization of gambling as a means of generating economic and tourism-related benefits. Although the legalization initiative gained significant momentum in 2025, political uncertainty subsequently disrupted the legislative process. At the enforcement level, Thailand faces challenges similar to those encountered elsewhere in Southeast Asia: many illegal online gambling operations do not maintain their physical infrastructure within Thailand itself but operate from border areas or relocate periodically across jurisdictions (Sriyai & Arugay, 2025). This geographic mobility makes conventional territorial enforcement increasingly ineffective and highlights the importance of cross-border investigative and intelligence-sharing mechanisms. The necessity for such cooperation is underscored by the region’s broader struggle with cybercrime, where disparate legal frameworks and varying technological capacities continue to impede effective regional coordination (Sulubara et al., 2025).

Vietnam, by contrast, has historically adopted a restrictive regulatory approach to online gambling and does not provide a broad licensing framework for full-scale online casino operations (Luong, 2020; Tuan, 2026). Although this model limits the scope of legally authorized online gambling, it does not eliminate demand or prevent illegal operators from reaching Vietnamese users through offshore platforms, unauthorized websites, and encrypted digital channels. In practice, restrictive domestic regulation may displace rather than suppress the underlying activity when enforcement capacity, technological resources, and cross-border cooperation remain inadequate. Vietnam’s economic integration and digital connectivity can therefore be exploited by transnational criminal networks to conceal gambling operations, move illicit proceeds, and facilitate related forms of scam-forced criminality. The limited availability of timely mutual legal assistance further enables these networks to operate across jurisdictions and evade coordinated intervention (Luong, 2025). Vietnam’s experience consequently demonstrates that prohibition or restrictive regulation, although normatively strong, cannot by itself address online gambling when criminal infrastructure, financial flows, and digital evidence extend beyond national borders.

Singapore represents a distinct regulatory model based on strictly controlled legalization rather than broad prohibition or permissive licensing. Under the Gambling Control Act 2022, online gambling is subject to extensive regulatory controls, and only authorized operators may provide specified forms of remote gambling services. Unauthorized gambling websites and associated access channels are subject to blocking and other enforcement measures (Sriyai & Arugay, 2025). This model demonstrates that limited legal authorization can be combined with strong regulatory supervision, financial controls, and targeted action against unlicensed operators. Nevertheless, Singapore’s comparatively robust domestic framework cannot fully insulate it from the consequences of regional regulatory fragmentation. Illicit

entities may exploit weaker regulatory environments in neighboring jurisdictions, operate offshore, and use cross-border digital and financial infrastructure to circumvent domestic access restrictions (Yang & Li, 2025). Singapore therefore illustrates both the value and the limits of stringent national regulation: effective domestic controls can reduce exposure and disrupt access, but they cannot by themselves eliminate criminal operations that are organized and financed beyond the state's territorial jurisdiction. The Singaporean experience consequently reinforces the broader argument that online gambling enforcement requires not only national regulatory capacity but also coordinated regional measures addressing offshore platforms, illicit payment channels, and cross-border criminal networks.

Taken together, the experiences of Indonesia, the Philippines, Thailand, Vietnam, and Singapore demonstrate that Southeast Asia does not have a unified regulatory approach to online gambling. Instead, the region contains a spectrum ranging from strict prohibition and restrictive regulation to controlled authorization and historically permissive licensing models. This divergence creates opportunities for criminal networks to exploit differences between jurisdictions. This regulatory inconsistency is further compounded by disparities in technological expertise and law enforcement training, which frequently hinder effective collaboration even when legal frameworks nominally align (Xiao et al., 2026).

The comparative evidence therefore suggests that the effectiveness of national regulation depends not only on the strength of domestic legislation but also on the degree of regional regulatory coordination. A criminal network operating across several jurisdictions can exploit the weakest point in the regional enforcement chain. Consequently, strengthening Indonesia's domestic regulatory framework, while necessary, is unlikely to be sufficient without mechanisms for cross-border financial intelligence, digital evidence sharing, coordinated investigations, extradition or mutual legal assistance, and joint disruption of criminal infrastructure.

From a transnational perspective, illegal online gambling should consequently be understood as a regional governance problem rather than a collection of isolated national offenses. The Southeast Asian experience indicates that regulatory fragmentation, technological mobility, and cross-border financial networks interact to create an environment in which criminal enterprises can rapidly adapt to enforcement pressure. Effective countermeasures therefore require a combination of domestic legal reform, institutional capacity building, technological enforcement, financial intelligence, and sustained regional cooperation.

Patterns of Illicit Financial Flows from Illegal Online Gambling and Their Nexus with Cross-Border Cyber-Economic Crime

Scale and Characteristics of Illicit Financial Flows in Indonesia

Data reported by the Indonesian Financial Transaction Reports and Analysis Center (PPATK) reveal the alarming scale of financial flows associated with illegal online gambling in Indonesia. Between 2017 and mid-2024, the total value of transactions suspected to be associated with online gambling reached hundreds of trillions of Indonesian rupiah, with one of the most significant increases occurring in 2021, when the reported turnover reached approximately IDR 57.9 trillion, representing a 267% year-on-year increase. During the first half of 2024 alone, transactions associated with online gambling reached approximately IDR 174.56 trillion. This figure indicates that intensified law-enforcement measures had not yet produced a proportionate reduction in the volume of financial transactions generated by illegal online gambling.

The structure of these financial flows exhibits characteristics commonly associated with organized cyber-enabled economic crime. Criminal actors systematically rotate online gambling websites, bank accounts, electronic wallets, and other payment channels to disrupt financial tracing and reduce the likelihood of detection. The proceeds may also be commingled with funds generated through apparently legitimate businesses, allowing illicit revenue to be disguised as legitimate commercial activity (Berry et al., 2023; Levi, 2015). Such practices complicate the identification of the original source of funds and

create significant challenges for financial-intelligence and law-enforcement agencies.

The transnational nature of these financial flows further increases the complexity of enforcement. PPATK has reported that suspicious funds associated with online gambling do not remain exclusively within Indonesia but may be transferred to other Southeast Asian jurisdictions, including Thailand, Cambodia, and the Philippines, as well as to offshore financial jurisdictions and tax havens. The use of multiple jurisdictions creates additional obstacles to financial tracing, asset freezing, confiscation, and repatriation because investigators must overcome differences in legal systems, evidentiary requirements, financial regulations, and institutional procedures.

In response, PPATK has taken financial-disruption measures, including the blocking of more than 5,000 accounts associated with online gambling involving funds valued at more than IDR 600 billion. It has also supported the National Anti-Money Laundering Movement as part of a broader strategy to restrict the financial infrastructure available to criminal actors. These interventions demonstrate the increasing importance of financial intelligence as a component of online gambling enforcement. Nevertheless, account blocking alone is unlikely to dismantle sophisticated criminal networks when operators can rapidly establish replacement accounts, employ third-party intermediaries, use alternative payment mechanisms, or shift transactions across national borders. Moreover, the widespread adoption of e-wallets and decentralized payment methods further enables operators to facilitate rapid, anonymous transactions that circumvent traditional banking surveillance and jurisdictional oversight (Solihin, 2026).

The evidence, therefore, suggests that the financial dimension of illegal online gambling represents one of the most important areas for strengthening enforcement. Rather than focusing exclusively on identifying individual gamblers or blocking gambling websites, enforcement strategies should increasingly target the financial architecture that enables gambling networks to operate, accumulate profits, transfer proceeds, and conceal the origins of illicit funds.

The Nexus between Illegal Online Gambling and Transnational Money Laundering

The relationship between illegal online gambling and transnational money laundering in Southeast Asia has been extensively documented by the United Nations Office on Drugs and Crime (UNODC). A UNODC report published in January 2024 identified online casinos and related businesses as mechanisms increasingly exploited by major organized-crime groups to transfer and launder substantial volumes of both fiat currency and cryptocurrency. This development demonstrates that online gambling platforms can function not only as venues for illegal betting but also as components of broader financial-crime infrastructures.

Money laundering associated with online gambling can be understood through the conventional three-stage model of placement, layering, and integration. During the placement stage, proceeds derived from criminal activities are introduced into gambling-related platforms or financial channels. During layering, funds are moved through multiple betting transactions, accounts, payment intermediaries, or digital-asset transfers in an attempt to obscure their origin. During integration, the funds may re-enter the formal economy and be presented as legitimate gambling winnings, business revenue, investment proceeds, or other apparently lawful income (Bonato & Szava, 2025; Levi & Soudijn, 2020).

The digitalization of financial services has expanded the range of mechanisms available to facilitate these activities. The increasing use of cryptocurrencies and virtual-asset exchange platforms can make the identification and tracing of illicit proceeds more complex, particularly where service providers operate across jurisdictions with different regulatory standards (Chitsungo, 2024; Turner et al., 2020). UNODC has highlighted the rapid growth of high-risk Virtual Asset Service Providers (VASPs) in the region, some of which can effectively provide financial services resembling an underground banking system for criminal organizations.

Cryptocurrency does not inherently provide complete anonymity, since many blockchain transactions

can be traced through appropriate forensic techniques. However, the combination of pseudonymous addresses, cross-border transfers, decentralized services, mixers or obfuscation mechanisms, and rapidly changing digital wallets can create substantial investigative challenges. Criminal organizations can therefore exploit the technological characteristics of digital assets to increase the complexity and cost of financial investigations (Chitsungo, 2024; Khrabrykh & Observatory, 2026).

The emergence of large-scale illicit online marketplaces has further expanded this criminal ecosystem. One prominent example is Huione Guarantee, subsequently associated with the name Haowang, which has been identified by UNODC as a major illicit marketplace in the region (Loughlin, 2026). Such platforms have reportedly facilitated access to a broad range of criminal services and tools, including fraud-related materials, phishing resources, malware, and money-laundering services. Their significance lies not simply in individual transactions but in their ability to provide an interconnected commercial infrastructure that allows criminal groups to outsource specialized functions and operate at scale. By leveraging such platforms, criminal actors effectively intertwine illicit financial flows with legitimate commercial activity, thereby obscuring the ultimate origin of laundered assets (Azero et al., 2024).

The relationship between online gambling and money laundering is therefore increasingly characterized by functional integration. Gambling platforms can provide an apparent commercial justification for financial transactions, while cryptocurrency and alternative payment systems can facilitate cross-border movement of proceeds. At the same time, illicit digital marketplaces can supply the technological and operational resources necessary to maintain these networks. The resulting ecosystem blurs the boundaries between gambling-related offenses, cybercrime, financial crime, and transnational organized crime.

The Indonesia–Cambodia Corridor and Regulatory Arbitrage

Research examining the Indonesia–Cambodia corridor provides further evidence of the transnational character of this nexus. Transnational criminal organizations can exploit regulatory differences between the two countries, use digital recruitment mechanisms to target Indonesian nationals, and employ cryptocurrency-based financial systems that are difficult to detect through conventional law-enforcement mechanisms (Laras & Rusdiyanta, 2025). This illustrates how regulatory arbitrage can become a strategic resource for criminal organizations: differences in regulatory standards and enforcement capabilities allow criminal actors to locate particular components of their operations in jurisdictions where detection and prosecution are more difficult.

Criminal networks also demonstrate considerable operational adaptability by relocating their activities to Special Economic Zones (SEZs) and other jurisdictions characterized by limited regulatory capacity. In such environments, complex corporate structures, opaque ownership arrangements, and regulatory gaps can potentially be exploited to disguise criminal operations as legitimate foreign investment or commercial activity. Such adaptive strategies often involve the deliberate engineering of hybrid financial infrastructures that link illicit and licit domains, effectively allowing these groups to maintain resilience through structural redundancy (Ramadhan, 2026). Furthermore, this strategic shifting of operations allows syndicates to leverage existing smuggling routes and corrupt networks, demonstrating a persistent pattern of crime convergence that transcends traditional national jurisdictions (Uhm & Siegel, 2021). These fluid, decentralized network structures increasingly replace rigid hierarchies, allowing for ad hoc coalitions that rapidly exploit emerging vulnerabilities in state institutional frameworks (Moreto & Uhm, 2021).

This phenomenon presents a significant challenge for conventional approaches to criminal enforcement. Domestic authorities may successfully identify an illegal gambling platform or financial account within their jurisdiction while remaining unable to establish the complete ownership structure, financial beneficiaries, or operational leadership located abroad. Consequently, effective enforcement

requires the ability to connect digital evidence, financial intelligence, corporate information, and cross-border investigative cooperation.

Transnational Organized Crime Networks in Southeast Asia

The Mekong subregion, particularly Myanmar, Laos, and Cambodia, has emerged as a major center of transnational organized-crime networks that exploit online gambling and related digital platforms as operational infrastructure. The rapid expansion of transnational criminal activity in the region has been partly associated with a displacement effect, whereby intensified law enforcement in China encouraged criminal organizations to relocate certain operations to Mekong jurisdictions characterized by higher levels of corruption, weaker governance, and more limited institutional oversight (Kamalludin, 2025). This regional transformation has been further catalyzed by the proliferation of industrial-scale cyber-fraud centers and synthetic drug production hubs, which now function as a sprawling, interconnected ecosystem of human traffickers, data brokers, and money launderers (Campbell, 2024).

A similar displacement dynamic became evident following Cambodia's prohibition of online gambling in 2019. Rather than eliminating the underlying criminal ecosystem, the regulatory change reportedly encouraged some operators previously concentrated in Sihanoukville to relocate to other jurisdictions with more permissive regulatory environments while transferring elements of their existing criminal infrastructure (Jeselyn & Lynn, 2025). This demonstrates an important limitation of purely territorial enforcement: when criminal networks possess substantial financial and technological mobility, national prohibition may displace criminal activity geographically without necessarily eliminating it.

The humanitarian consequences associated with these networks are equally serious. UNODC has identified Sihanoukville as an important concentration point for scam compounds in the region and has estimated that approximately 100,000 workers have been subjected to coercive conditions described as resembling modern slavery (Kamalludin, 2025). The exploitation of workers demonstrates that the online gambling ecosystem can intersect with human trafficking, forced labor, and other forms of severe exploitation.

Illegal online gambling networks in Southeast Asia have evolved beyond platforms for illicit betting into strategic infrastructures through which transnational criminal organizations facilitate and conceal money laundering, labor exploitation, and human trafficking. Indonesian nationals have reportedly constituted one of the groups significantly affected by these operations (Hutagalung, 2025; Kamalludin, 2025; Rofii & Ardiyansah, 2026). The involvement of the same digital platforms, financial channels, recruitment mechanisms, and cross-border networks in both profit generation and human exploitation demonstrates that these activities are not isolated offenses but interconnected components of a broader criminal ecosystem. Accordingly, illegal online gambling should not be analyzed exclusively as a financial or regulatory offense; it should be understood as an enabling infrastructure that allows illicit finance, cyber-enabled fraud, and human exploitation to reinforce one another across jurisdictions.

Evidence concerning illicit financial flows in Myanmar adds another dimension to this analysis. The intersection of online gambling-related fraud and transnational organized crime has contributed to sophisticated fraud schemes, including pig-butcher scams, which can produce substantial financial and psychological harm to victims (Thura & Tar, 2025). These operations typically exploit digital communication, social engineering, investment narratives, and cryptocurrency or other financial mechanisms to manipulate victims into transferring funds.

More recent analysis by UNODC in 2025 further warns that the problem is being intensified by the strategic infiltration of organized criminal groups into vulnerable jurisdictions through what it describes as "criminal foreign direct investment." Under this model, investments may appear legitimate on the surface but are allegedly structured to establish or strengthen infrastructure that supports criminal activities. This development is particularly significant because it demonstrates the increasing sophistication of organized crime: criminal organizations are not necessarily operating outside the formal economy but

may seek to embed themselves within legitimate commercial, financial, and investment structures.

Taken together, the evidence demonstrates that illegal online gambling in Southeast Asia has evolved into a multilayered cyber-economic crime ecosystem. Its financial dimension is characterized by large-scale transactions, rapidly changing payment channels, cross-border transfers, and increasingly sophisticated money-laundering mechanisms. Its technological dimension is supported by digital platforms, cryptocurrencies, encrypted communications, and online marketplaces. Its organizational dimension involves transnational criminal networks capable of relocating operations across jurisdictions. Finally, its social dimension extends into human trafficking, forced labor, fraud, and other forms of exploitation.

The central implication is that conventional enforcement strategies focused primarily on website blocking and individual prosecution are insufficient to address the structural foundations of the problem. The evidence instead points toward the need for a financially focused, intelligence-led, technologically capable, and transnational enforcement model.

For Indonesia, this means that efforts to combat illegal online gambling should extend beyond the removal of gambling content to include systematic tracing of beneficial ownership, real-time monitoring of suspicious financial transactions, cryptocurrency forensics, asset freezing and confiscation, investigation of corporate structures, and disruption of cross-border financial networks. At the regional level, stronger mechanisms for intelligence sharing, mutual legal assistance, coordinated investigations, and asset recovery are necessary because criminal networks can exploit the weakest regulatory and institutional links within the region.

Accordingly, the effectiveness of Indonesia's response to illegal online gambling should ultimately be assessed not merely by the number of websites blocked or accounts suspended, but by the extent to which enforcement agencies can identify and dismantle the financial, technological, and organizational infrastructure that sustains transnational online gambling networks.

CONCLUSION

Based on a normative legal review and comparative analysis of relevant legislation, scholarly literature, and institutional reports, this study concludes that Indonesia has established a relatively comprehensive legal framework for addressing illegal online gambling through the Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and specialized government enforcement measures; however, its effectiveness remains constrained by regulatory disharmony, limited digital-forensic capacity, inadequate enforcement resources, low public legal awareness, and fragmented regional regulations that enable jurisdictional arbitrage by transnational criminal networks. At the regional level, the evidence further indicates that illegal online gambling has evolved beyond conventional gambling transactions into an integrated cyber-economic crime ecosystem involving money laundering, illicit financial flows, cyber fraud, human trafficking, and transnational organized crime, facilitated by cryptocurrencies, high-risk or inadequately regulated virtual asset service providers, offshore operations, special economic zones, and increasingly sophisticated digital technologies. These challenges require a shift from conventional website blocking and account suspension toward intelligence-led, financially focused, and technologically capable enforcement. Accordingly, this study recommends three priorities: harmonizing the KUHP, ITE Law, and Anti-Money Laundering Law to close regulatory gaps and strengthen liability for gambling operators and financiers; substantially enhancing law-enforcement capacity in digital forensics, cryptocurrency tracing, electronic evidence, and cross-border financial investigations; and strengthening binding ASEAN legal and operational cooperation, including information sharing, mutual legal assistance, coordinated investigations, and asset recovery, to ensure a coordinated regional response capable of dismantling the financial, technological, and organizational infrastructure of transnational illegal online gambling networks.

REFERENCES

- Achmadi, R. Z., & Suciyan. (2026). Masalah penegakan hukum bandar judi online: Perspektif KUHP baru dan hukum Islam. *Judge: Jurnal Hukum*, 6(8), 1405–1425. <https://doi.org/10.54209/judge.v6i8.2200>
- Adlina, N. A. (2025). Efektivitas penegakan hukum perjudian online di Indonesia: Mengatasi hambatan regulasi dan implementasi. *Journal of Contemporary Law Studies*, 2(2), 197–208. <https://doi.org/10.47134/lawstudies.v2i2.3670>
- Ahyani, H., Harahap, A. M., Solehudin, E., Adnan, N. I. M., Mutmainah, N., Siripipatthanakul, S., Lousada, S. A. N., Putra, H. M., & Novita, D. (2024). Effectiveness of law enforcement against online gambling practices in Indonesia in supporting the achievement of SDGs. *Journal of Lifestyle and SDGs Review*, 5(1). <https://doi.org/10.47172/2965-730x.sdgsreview.v5.n01.pe03686>
- Anggoro, T. C., & Santoso, B. B. (2025). Politik kriminal integratif dalam penanggulangan perjudian online di Indonesia. *Jurnal USM Law Review*, 8(3), 1643–1664. <https://doi.org/10.26623/julr.v8i3.12541>
- Arum, N. S., & Sumardiana, B. (2025). Implementasi Pasal 303 Kitab Undang-Undang Hukum Pidana terhadap pembaruan regulasi perjudian online di Indonesia (Studi Putusan Nomor 111/Pid.B/2022/PN.Bkt). *Amnesti Jurnal Hukum*, 7(1), 81–94. <https://doi.org/10.37729/amnesti.v7i1.6166>
- Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*, 1(3), 23–32. <https://doi.org/10.4236/jss.2013.13004>
- Azero, M. A., Abdullah, S. N. A. K., Zakaria, Z., Haris, H., & Yusoff, Y. H. (2024). The nexus of cybercrime and money laundering: A conceptual paper. *Accounting and Finance Research*, 13(2), 167. <https://doi.org/10.5430/afr.v13n2p167>
- Azis, A. A., & Azhari, M. (2025). Illegal online gambling in Indonesia: Assessing state securitization and its effectiveness. *Jurnal Hubungan Internasional*, 14(1), 1–14. <https://doi.org/10.18196/jhi.v14i1.27827>
- Bangun, B. H., & Kinanti, F. M. (2025). The urgency of combating human trafficking for online scams in Indonesia. *Brawijaya Law Journal*, 12(1), 82–102. <https://doi.org/10.21776/ub.blj.2025.012.01.05>
- Bentara, B., Iskandar, I., Setianingrat, E., Permana, D. Y., & Dikrurahman, D. (2025). Legal responsibility for perpetrators of online gambling crimes. *Journal of World Science*, 4(5), 512–521. <https://doi.org/10.58344/jws.v4i5.1408>
- Berry, M., Salinas, M., & Gundur, R. V. (2023). Financial risk management strategies of small to medium illicit drug enterprises: Considering low-level money laundering. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-023-09501-5>
- Bonato, A., & Szava, A. (2025). Network embedding analysis for anti-money laundering detection [Preprint]. *arXiv*. <https://doi.org/10.48550/arXiv.2509.10715>
- Budairti, & Patodongi, A. M. (2025). Government policy on the phenomenon of online gambling in Indonesia: An integrative analysis of law, technology, and siyasah syar'iyah. *International Journal of Research and Innovation in Social Science*, 9(11), 461–471. <https://doi.org/10.47772/IJRISS.2025.91100037>
- Campbell, J. R. (2024). Criminal threats to security. In *Criminal threats to security* (pp. 87–103). Routledge. <https://doi.org/10.4324/9781003473206-6>
- Chitsungo, C. (2024). Harnessing digital strategies to combat cryptocurrency-enabled crimes: Addressing money laundering, illicit trade, and cyber threats. *American Journal of International Relations*, 9(7), 77–106. <https://doi.org/10.47672/ajir.2523>
- Collier, H., Morton, C., Alharthi, D., & Kleiner, J. (2023). Cultural influences on information security. *European Conference on Cyber Warfare and Security*, 22(1), 143–150. <https://doi.org/10.34190/eccws.22.1.1127>
- Elthaufani, L., & Cumbrandika, C. (2026). The role of the police in combating online gambling crimes (A case study of Decision Number 217/Pid.Sus/2025/PN.JKT.SEL). *POSTULAT*, 4(1), 72–79. <https://doi.org/10.37010/postulat.v4i1.2113>

- Fadhli, M. (2024). Penegakan hukum terhadap tindak pidana perjudian online. *Indragiri Law Review*, 2(2), 68–73. <https://doi.org/10.32520/ilr.v2i2.61>
- Firmansyah, F. (2025). Kebijakan hukum pidana mengenai kejahatan judi online (Cyber gambling) di Indonesia. *Jurnal Hukum Politik dan Ilmu Sosial*, 4(3), 54–62. <https://doi.org/10.55606/jhps.v3i4.4473>
- Fräsilä, A. (2025). The digital era and its impact on money laundering. *European Financial Resilience and Regulation*, 133. <https://doi.org/10.47743/eufire-2025-1-11>
- Gao, R., & Zhilin, L. (2025). A study on the new forms and governance dilemmas of cross-border fraud crimes in Southeast Asia (pp. 393–404). <https://doi.org/10.46793/CrossrCL.393B>
- Gulyamov, S. (2025). The dark web economy: Legal and investigative challenges in combatting hidden online markets. *Uzbek Journal of Law and Digital Policy*, 3(4), 1–12. <https://doi.org/10.59022/ujldp.352>
- Haribowo, J., Sudirman, A. S., Kartiyoso, A. G., & Mursito. (2025). Tackling online gambling through criminal law: Law enforcement strategies against cybercrime in Indonesia. *Research Horizon*, 5(6), 2935–2944. <https://doi.org/10.54518/rh.5.6.2025.949>
- Huang, R.-T., Shih, C.-H., Lin, T.-C., & Lin, W. (2022). The study on illegal online gambling investigation in Taiwan. *Procedia Computer Science*, 207, 2901–2910. <https://doi.org/10.1016/j.procs.2022.09.348>
- Hutagalung, R. E. P. (2025). Triangular synergy model to enhance the Indonesian National Police's (POLRI) strategy in handling human trafficking of cyber-based slavery. *Journal of Information Systems Engineering & Management*, 10, 27–34. <https://doi.org/10.52783/jisem.v10i49s.9805>
- Jeselyn, & Lynn, G. D. (2025). *Transnational crime in Cambodia and Indonesia: Strengthening regional and national responses*. Nanyang Technological University. <https://hdl.handle.net/10356/201651>
- Juhara, N. F., Amalia, M., & Mulyana, A. (2025). Efektivitas penegakan hukum terhadap judi online di Indonesia: Analisis yuridis dan sosiologis. *Journal of Contemporary Law Studies*, 2(2), 153–164. <https://doi.org/10.47134/lawstudies.v2i2.3353>
- Kamalludin, I. (2025). Pencucian uang, eksploitasi tenaga kerja, dan perdagangan orang dalam lingkaran judi online. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism*, 3(2), 197. <https://doi.org/10.59593/amlcft.2025.v3i2.230>
- Khrabrykh, S., & Observatory, A. (2026). *Blockchain as a tool of financial crime: The myth of full transparency and the real mechanisms of concealment*. Zenodo. <https://doi.org/10.5281/zenodo.18328480>
- Laras, F. P., & Rusdiyanta, R. (2025). Modus operandi of transnational online gambling syndicates in the Indonesia-Cambodia region: Analysis in the perspective of transnationalism. *Journal of Social Research*, 4(6). <https://doi.org/10.55324/josr.v4i6.2570>
- Levi, M. (2015). Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research*, 21(2), 275–297. <https://doi.org/10.1007/s10610-015-9269-7>
- Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice*, 49, 579–631. <https://doi.org/10.1086/708047>
- Loughlin, N. (2026). Digital crime, dirty money and the state: Southeast Asia's illicit political economy and the rise of cybercrime. *Development and Change*. <https://doi.org/10.1111/dech.70071>
- Luong, H. T. (2020). Transnational crime and its trends in South-East Asia: A detailed narrative in Vietnam. *International Journal for Crime, Justice and Social Democracy*, 9(2), 88–101. <https://doi.org/10.5204/ijcjsd.v9i2.1147>
- Luong, H. T. (2025). "Simple job, high salary": Unveiling the complexity of scam-forced criminality in Southeast Asia. *Humanities and Social Sciences Communications*, 12(1). <https://doi.org/10.1057/s41599-025-05605-1>
- Mahmudi, H. C., Widarto, J., & Kantikha, I. M. (2025). Pertanggungjawaban pidana terhadap pelaku penyebaran situs judi online. *Khatulistiwa Jurnal Pendidikan dan Sosial Humaniora*, 5(4), 998–1013. <https://doi.org/10.55606/khatulistiwa.v5i4.10340>

- Mawardi, R., Nuraeni, V., Jasman, J., Trihatmoko, H., Sorongan, F. A., Aripin, S., & Malik, S. M. (2026). Digital financial compliance challenges: Applying routine activity theory to online gambling networks analysis. *Emerging Science Journal*, 10(1), 315–332. <https://doi.org/10.28991/esj-2026-010-01-015>
- Moreto, W. D., & van Uhm, D. (2021). Nested complex crime: Assessing the convergence of wildlife trafficking, organized crime and loose criminal networks. *The British Journal of Criminology*, 61(5), 1334–1353. <https://doi.org/10.1093/bjc/azab005>
- Morse, J. C. (2022). Fighting illicit financing in Southeast Asia. In *Cornell University Press eBooks* (pp. 139–164). Cornell University Press. <https://doi.org/10.7591/cornell/9781501761515.003.0007>
- Novianto, D. G., & Asri, D. P. B. (2026). Kegagalan ASEAN dalam menanggulangi judi online: Perspektif regional security complex theory. *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, 4(3), 19573–19578. <https://doi.org/10.31004/jerkin.v4i3.5185>
- Okta, S. L., & Vera. (2026). Criminal liability of platform organizers in online gambling cases in Indonesia: Between normative voids and the need for special regulations. *International Journal of Humanities Law and Politics*, 3(4), 152–158. <https://doi.org/10.46336/ijhlp.v3i4.251>
- Pasha, A. K., & Mulyana, Y. (2025). Tantangan penegakan hukum terhadap fraud perbankan dalam industri judi online. *Wajah Hukum*, 9(2), 857. <https://doi.org/10.33087/wjh.v9i2.1947>
- Popoola, O. A., Akinsanya, M. O., Nzeako, G., Chukwurah, E. G., & Okeke, C. D. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: Comparative analysis of African and U.S. initiatives. *International Journal of Applied Research in Social Sciences*, 6(5), 819–827. <https://doi.org/10.51594/ijarss.v6i5.1104>
- Ramadhan, S. (2026). *How organised crime systems adapt: Opportunity, resilience, and laundering connectivity in transnational criminal networks* [Preprint]. Research Square. <https://doi.org/10.21203/rs.3.rs-8582804/v1>
- Rofii, M. S., & Ardiyansah, R. F. (2026). Human trafficking within Southeast Asia's online gambling industry: International resilience and policing challenges. *Jurnal Ilmu Kepolisian*, 20(1). <https://doi.org/10.35879/jik.v20i1.706>
- Samosir, J. C., Ramadani, S., & Ismaidar, I. (2025). Legal review of the responsibility of online gambling criminal acts in Indonesia. *International Journal of Sociology and Law*, 2(2), 71–82. <https://doi.org/10.62951/ijsl.v2i2.603>
- Samphy, Shawin, & Mai. (2025). Combating illicit finance in digital payment services: The role of data analytics and technology in preventing payment fraud and scams. *World Scientific Annual Review of Fintech*, 3. <https://doi.org/10.1142/S2811004825300054>
- Saputra, A. D., & Arianto, H. (2025). Studi perbandingan penegakan hukum tindak pidana judi online di Indonesia dan Kamboja. *Jurnal Paris Langkis*, 6(1), 127–138. <https://doi.org/10.37304/parislangkis.v6i1.22919>
- Saripudin, A., Arafat, Z., & Abas, M. (2025). Penegakan hukum terhadap tindak pidana judi online di Indonesia: Analisis normatif. *Jurnal Ilmiah Advokasi*, 13(3), 972–984. <https://doi.org/10.36987/jiad.v13i3.7577>
- Silalahi, D. G. P., Ismunarno, I., & Lukitasari, D. (2024). Pengaturan hukum positif di Indonesia terkait promosi judi online di media sosial. *Aliansi*, 1(2), 317–330. <https://doi.org/10.62383/aliansi.v1i2.150>
- Solihin, J. (2026). Analisis yuridis kriminologis judi online e-wallet dan pemblokiran situs Komdigi nasional. *Bandung Conference Series: Law Studies*, 6(1). <https://doi.org/10.29313/bcsls.v6i1.22895>
- Sriyai, S., & Arugay, A. A. (2025). *Casinos and consequences: A comparative lens on Thailand and the Philippines*. ISEAS – Yusof Ishak Institute. <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2025-56-casinos-and-consequences-a-comparative-lens-on-thailand-and-the-philippines>
- Sulthanah, M. Y., & Ginting, R. (2025). Analisis problematika penegakan hukum terhadap tindak pidana perjudian online di Indonesia. *Jembatan Hukum*, 2(2), 1–15. <https://doi.org/10.62383/jembatan.v2i1.1438>

- Sulubara, S. M., Tasril, V., & Nurkhalisah. (2025). Legal and technological approaches to cybercrime risk mitigation: A case study of cyber law and cybersecurity implementation in Southeast Asia. *Open Society Conference*, 3, 606–613. <https://doi.org/10.33830/osc.v3i1.7023>
- Sunarto, A., Simarmata, L. E., Maharani, M., & Adnan, M. A. (2025). The effectiveness of law enforcement against online gambling in the digital era in Medan City. *Journal of Law, Politic and Humanities*, 5(6), 5049–5062. <https://doi.org/10.38035/jlph.v5i6.2340>
- Thura, Z., Thant, & Tar, K. M. S. T. (2025). *Cybercrimes and the illicit financial flows in Myanmar*. Zenodo. <https://doi.org/10.5281/zenodo.15467435>
- Tuan, T. V. (2026). The offence of gambling under Vietnamese criminal law: Challenges in the context of digital technology and cross-border activities. *Veredas do Direito: Direito Ambiental e Desenvolvimento Sustentável*, 23(3). <https://doi.org/10.18623/rvd.v23.n3.4535>
- Turner, A., McCombie, S., & Uhlmann, A. J. (2020). Analysis techniques for illicit Bitcoin transactions. *Frontiers in Computer Science*, 2. <https://doi.org/10.3389/fcomp.2020.600596>
- van Uhm, D., & Siegel, D. (2021). Organised crime and animals. *Trends in Organized Crime*, 24(4), 419–424. <https://doi.org/10.1007/s12117-021-09440-z>
- van Uhm, D., & Zhang, M. (2022). Illegal wildlife trade in two special economic zones in Laos: Underground–open-sale fluctuations in the Golden Triangle borderlands. *Frontiers in Conservation Science*, 3. <https://doi.org/10.3389/fcosc.2022.1030378>
- Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions. *Magna Scientia Advanced Research and Reviews*, 11(1), 68–83. <https://doi.org/10.30574/msarr.2024.11.1.0075>
- Widijowati, R. D., Pecson, R. C., & Kristiawanto, K. (2025). The online gambling as a criminal offense which disturbs society on legal perspective. *Jurnal Hukum*, 41(2), 461. <https://doi.org/10.26532/jh.v41i2.43373>
- Wijaya, F. A. (2025). Upaya penegakan hukum terhadap pelaku tindak pidana perjudian online. *Jurnal Hukum Politik dan Ilmu Sosial*, 4(3), 63–73. <https://doi.org/10.55606/jhpis.v3i4.4474>
- Wiwoho, J., Pratama, A. M., Pati, U. K., & Pranoto, P. (2023). Examining cryptocurrency use among Muslim affiliated terrorists: Case typology and regulatory challenges in Southeast Asian countries. *AL-IHKAM: Jurnal Hukum & Pranata Sosial*, 18(1), 102–124. <https://doi.org/10.19105/al-lhkam.v18i1.7147>
- Xiao, L. Y., Demetrovics, Z., Deery, C., Heath, C., Király, O., King, D., & Czakó, A. (2026). Global review of assessments of online gambling policies affecting youths: Bans, legalisation, advertising restrictions, and “responsible gambling.” *Current Addiction Reports*, 13(1). <https://doi.org/10.1007/s40429-026-00748-w>
- Yang, B., & Li, M. (2025). Offshore embeddedness beyond the wall: Chinese cloud providers in Southeast Asia’s data governance landscape. *Politics and Governance*, 13. <https://doi.org/10.17645/pag.10437>