

Reconstruction of Cyber Policing Law in the Prevention and Enforcement of Online Gambling through the Integration of Cyber Supervision and Digital Community Protection in Indonesia

Iwan Matthew Frans Kapojos*, Yundini Husni, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; imfkapojos@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; yundinihusni1@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6323>

*Correspondence: Iwan Matthew Frans

Kapojos

Email: imfkapojos@gmail.com

Received: 08/08/2026

Accepted: 27/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

Abstract: *The development of Indonesia's digital society has driven the transformation of conventional crime into modern cybercrime, one of which is online gambling, which has grown massively, anonymously, and transnationally through the use of information technology, social media, financial technology, cryptocurrency, and cross-border digital platforms. This study examines weaknesses in the legal framework and challenges in implementing cyber policing in the prevention and prosecution of online gambling in Indonesia. It also seeks to develop a reconstruction of cyber policing law through the integration of cyber surveillance and digital community protection. The research adopts a normative juridical method using statutory and conceptual approaches, analyzing various legal instruments, including the Criminal Code, the Electronic Information and Transactions Law, the Police Law, the Personal Data Protection Law, as well as relevant legal doctrines and theories. The results of the study indicate that the Indonesian legal system still has normative weaknesses, such as the absence of specific cyber policing regulations, weak regulations on cyber surveillance and digital evidence, limited cyber jurisdiction, and the suboptimal integration of digital transactions and cyberspace supervision between state institutions. The implementation of cyber policing also faces obstacles in the form of limited cyber investigators, minimal digital forensics infrastructure, weak cyber intelligence, and the low use of artificial intelligence in cyber*

surveillance. Therefore, a reconstruction of cyber policing law is needed through the establishment of comprehensive national regulations, strengthening of an integrated cyber monitoring system, the establishment of a national cyber command center, strengthening predictive policing based on artificial intelligence, harmonizing cross-sectoral regulations, and strengthening international cooperation to create a digital law enforcement system that is preventative, integrative, adaptive, and based on protecting the digital community in Indonesia.

Keywords: *cyber policing, online gambling, cyber surveillance, digital community.*

Introduction

The development of information and communication technology has given rise to a digital society, characterized by high internet penetration, smartphone use, social media, financial technology (fintech), and increased public activity in cyberspace. The digital transformation has changed patterns of social, economic, and cultural interactions, even public service systems, into electronic, internet-based forms (Rohmy, 2021). Indonesia, as one of the countries with the largest number of internet users in the world, has experienced

a significant acceleration of digitalization, especially since the development of the digital economy, electronic payment systems, and mobile application-based social media platforms (Siregar, 2025). While this situation provides easy access to information, transaction efficiency, and accelerated digital economic growth, it has also given rise to new forms of cybercrime, including online gambling, which has grown massively and is difficult to control through conventional law enforcement mechanisms.

Cyberspace has become a new social space that allows criminals to conduct activities across borders without jurisdictional boundaries (borderless crime), thus shifting the characteristics of criminal acts from conventional crimes to digital crimes that are anonymous, fast, massive, and transnational (Fairuzzen, 2024). Under Indonesian positive law, the prohibition on gambling is regulated in Article 303 and Article 303 bis of the Criminal Code (KUHP). However, these provisions are still oriented towards conventional forms of gambling and therefore do not fully encompass the complexities of digital gambling based on electronic platforms (Tuwo, 2016). On the other hand, Article 27 paragraph (2) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions regulates the prohibition on the distribution and access of electronic information containing gambling content. However, this norm is still general in nature and does not comprehensively regulate cyber policing, cyber patrols, or an integrated cyber surveillance system for preventing and prosecuting online gambling. This situation indicates that the development of the digital society has not been matched by legal reforms that are adaptive to the transformation of forms of cybercrime in Indonesia.

The development of online gambling in Indonesia demonstrates the increasing complexity of cyber-enabled gambling practices and their potential consequences for social order, economic security, and the protection of the digital community. Online gambling is no longer limited to conventional gambling websites but may operate through online slots, virtual casinos, digital sports betting, online lotteries, live gambling services, social media, mobile applications, streaming platforms, and digital communication groups. The expansion of internet access, digital payment instruments, e-wallets, virtual accounts, influencer promotion, and affiliate marketing has further transformed the operational environment of online gambling (Bakhtiar, 2024). Online gambling may also affect vulnerable groups, including children, students, and economically productive members of society, particularly where digital advertising and algorithmic distribution facilitate wider exposure.

From a modern criminological perspective, online gambling may generate multidimensional legal and social consequences, including economic crime, family disruption, digital addiction, poverty-related vulnerability, money laundering, and connections with other forms of transnational digital crime (Kesuma, 2023). Nevertheless, because this study employs a normative juridical method, it does not independently measure the statistical magnitude of online gambling growth, the precise number of cyber investigators, or the quantitative effectiveness of website blocking. References to these implementation conditions are used as contextual descriptions derived from documented academic and institutional discussions, while the principal object of analysis remains the

adequacy of existing legal norms in responding to the technological characteristics of online gambling.

The normative problem examined in this study is that the rapid transformation of online gambling through changing domains, foreign servers, VPN technology, anonymous hosting, cryptocurrency, and cross-border payment systems creates legal and procedural challenges for conventional enforcement mechanisms (Juhara, 2025). Likewise, electronic evidence involving encrypted systems, cloud computing, foreign servers, and cross-border transactions requires procedural standards that are more compatible with the technological characteristics of modern cybercrime. Although Article 5 of the Electronic Information and Transactions Law recognizes electronic information and electronic documents as legal evidence, questions concerning authentication, chain of custody, forensic integrity, and cross-border verification remain important areas for legal reconstruction (Mubarok, 2024).

The unique characteristics of online gambling are a major factor complicating law enforcement in Indonesia. Unlike conventional gambling, which has a physical location and easily identifiable perpetrators, online gambling operates in an anonymous, cross-jurisdictional digital system, utilizing high-tech technologies such as cryptocurrency, virtual private networks (VPNs), international payment gateways, bot automation systems, the dark web, cloud servers, and artificial intelligence. (Tumangger, 2025) Many online gambling platforms use servers located outside Indonesian jurisdiction, creating jurisdictional obstacles in the investigation and prosecution process. Furthermore, the use of nominee accounts, anonymous accounts, and encrypted digital transactions makes tracking perpetrators extremely complex. From a legal perspective, the electronic evidence system in Indonesia still faces various obstacles, particularly related to the validity of digital evidence, the chain of custody, forensic integrity, and cross-border authentication of electronic evidence. While Article 5 of the Electronic Information and Transactions Law recognizes electronic information and electronic documents as valid legal evidence, their implementation in judicial practice still faces numerous technical and normative problems. The Criminal Procedure Code (KUHP), which still focuses on conventional evidence, is not fully compatible with the nature of modern cybercrime, which utilizes encrypted digital systems and is based on cloud computing. (Mubarok, 2024) As a result, the process of proving online gambling crimes often encounters obstacles in obtaining digital evidence, identifying the main perpetrators, and proving the flow of cross-border electronic transactions. This situation indicates that the development of cybercrime has exceeded the capacity of the national criminal law system, which is still conventional and not yet fully based on cyber law enforcement. The problem is further complicated because the Indonesian legal system for combating online gambling remains partial, sectoral, and not yet integrated into the national cyber policing framework.

Regulations regarding gambling are scattered across various regulations, such as the Criminal Code, the Electronic Information and Transactions (ITE) Law, Law Number 2 of 2002 concerning the Indonesian National Police, the Telecommunications Law, the Personal Data Protection Law, and several administrative regulations regarding website blocking. (Fathor, 2024) However, these regulations do not provide a comprehensive legal basis for cyber patrol mechanisms, cyber surveillance, cyber intelligence, or digital monitoring systems in combating online gambling. The lack of legal norms regarding cyber policing

often leads law enforcement officials to act reactively and lack clear national operational standards for conducting cyber patrols and digital surveillance. Furthermore, there is overlapping authority between the Indonesian National Police, the Ministry of Communication and Digital, the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), and Bank Indonesia in overseeing digital transactions related to online gambling. Site blocking regulations also tend to be administrative in nature and fail to address the roots of the digital gambling ecosystem, which involves electronic transactions, promotional algorithms, and cross-border digital financial networks. (Kanda, 2024) From a modern legal perspective, this situation demonstrates a legal gap between the development of digital technology and the national regulatory system. The country lacks specific regulations governing the use of artificial intelligence surveillance, predictive policing, digital intelligence gathering, or integrated cyber command as modern and adaptive cyber law enforcement instruments to address the development of digital crime.

At the implementation level, the problematic cyber policing by the Indonesian National Police (Polri) still faces various structural, technical, and human resource obstacles. Handling online gambling crimes requires digital forensics, cyber intelligence, data analytics, blockchain tracing, and artificial intelligence monitoring skills, which are not yet fully possessed by law enforcement officers. The limited number of cyber investigators, the lack of digital forensics infrastructure, the low capacity for AI-based monitoring, and the lack of international cooperation are factors that hinder the effectiveness of online gambling enforcement (Anugrahi, 2024). Furthermore, the still predominantly repressive approach to law enforcement has resulted in the ineffectiveness of cyber surveillance-based prevention strategies. Cyber patrols and cyber intelligence remain incidental and have not been conducted in real time and integrated across institutions. In practice, digital transaction monitoring has also not been fully capable of detecting the flow of gambling funds using nominee accounts, cryptocurrencies, and cross-border electronic payment systems. Despite Article 13 of the National Police Law affirming the Polri's function of maintaining public security and order, law enforcement, and community protection, which in the context of a digital society should be interpreted progressively to include the protection of national cyberspace (Siregar, 2025). The limited effectiveness of cyber policing in addressing the growth of online gambling may weaken state legitimacy in safeguarding digital security and expand opportunities for organized cybercrime in Indonesia.

Based on these various issues, an integrative, adaptive, and digital society-based cyber policing legal reconstruction is needed as part of national legal reform in the digital society era. This legal reconstruction must be directed at establishing an integrated cyber monitoring system involving the Indonesian National Police (Polri), the Ministry of Communication and Digital, the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), Bank Indonesia, electronic system providers, and international cooperation within the framework of cybersecurity governance. Regulations on cyber patrols, cyber intelligence, artificial intelligence-based surveillance, predictive policing, and digital evidence systems are also needed to ensure that law enforcement against online gambling is not only repressive but also preventive and based on early detection. From the perspective of legal protection theory and social defense

theory, the state has an obligation to build a legal system capable of protecting the public from the increasingly complex threat of digital crime. Digital society protection is also in line with the concept of digital constitutionalism, which places cyberspace security as part of citizens' constitutional rights. Therefore, updating cyber policing laws is urgent and cannot be postponed any longer, as the current legal system is unable to address the complexities of digital technology-based online gambling. This legal reconstruction must be directed at harmonizing cross-sectoral regulations, strengthening national cyber jurisdiction, developing a national cyber command center, optimizing international cooperation, and establishing a digital law enforcement model capable of ensuring legal certainty, effective enforcement, and protecting Indonesia's digital community.

Methodology

This study employs a normative juridical research method by combining statutory and conceptual approaches. The normative juridical approach is used to examine legal norms related to cyber policing in combating online gambling in Indonesia through an analysis of relevant laws and regulations, legal principles, legal theories, and legal doctrines. The statutory approach is carried out by examining various regulations related to gambling, information technology, cyber law enforcement, and digital community protection, including the Criminal Code, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, Law Number 2 of 2002 concerning the Indonesian National Police, Law Number 27 of 2022 concerning Personal Data Protection, the Criminal Procedure Code, and various other regulations related to cyber surveillance and electronic transaction systems. Meanwhile, a conceptual approach is used to analyze the concepts of cyber policing, cyber surveillance, digital society, digital community protection, cyber security, and criminal law reform from the perspective of a modern rule of law. The legal materials used consist of primary, secondary, and tertiary legal materials obtained through library research. Furthermore, all legal materials are analyzed qualitatively using descriptive-analytical and prescriptive methods to identify weaknesses in existing regulations and formulate an integrative, adaptive, and digital community protection-based reconstruction of cyber policing law in combating online gambling in Indonesia.

Result and Discussion

Weaknesses in Legal Regulations for Combating Online Gambling in the Digital Society Era in Indonesia

The development of online gambling as a form of modern cybercrime demonstrates that the Indonesian legal system still faces various normative weaknesses in regulating and combating digital-based gambling practices. Gambling regulations in Indonesian positive law are still primarily based on Articles 303 and 303 bis of the Criminal Code (KUHP), which prohibit the organization and involvement in gambling. However, the norms within these provisions were primarily designed to regulate conventional gambling, which requires a physical space, easily identifiable perpetrators, and material evidence. In practice, online gambling has developed through electronic systems utilizing digital platforms, overseas servers, anonymous accounts, cryptocurrencies, and virtual payment systems, which

cannot be effectively resolved through conventional criminal law approaches. Article 303 of the KUHP also does not specifically regulate the responsibilities of electronic system operators, digital platforms, or third parties facilitating online gambling operations. The situation indicates a legal vacuum in the national legal system regarding cyberpolicing and cyberspace oversight of digital gambling practices. Although the new Criminal Code, through Law Number 1 of 2023, has updated national criminal law, regulations regarding cybercrime, particularly online gambling, still do not provide a comprehensive formulation regarding cyber surveillance systems, cyber patrols, and information technology-based digital enforcement mechanisms (Herawati, 2025).

In addition to the Criminal Code, regulations regarding online gambling are also stipulated in Article 27 paragraph (2) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which states that any person who intentionally and without authority distributes, transmits, or makes accessible electronic information and/or electronic documents containing gambling content is prohibited by law. This provision is reinforced by the criminal sanctions set out in Article 45, paragraph (3) of the ITE Law. However, the provision remains general and focuses primarily on the distribution of electronic content, without detailed regulation on cyber surveillance mechanisms, cyber intelligence, digital investigation, or the responsibilities of digital platforms in preventing the spread of online gambling. The ITE Law also lacks explicit provisions regarding the authority of law enforcement officers to conduct cyber patrols, the use of artificial intelligence surveillance for early detection of digital gambling activity, and the real-time monitoring mechanism for electronic transactions related to online gambling. Consequently, law enforcement against online gambling tends to be repressive after the crime has occurred, and has failed to establish an effective cyber-monitoring-based prevention system. From a modern legal perspective, this situation demonstrates that national regulations still lag behind the development of digital technology and the operational patterns of cybercrime, which are evolving rapidly in the digital era (Amelia, 2024).

Another normative weakness is evident in the absence of specific regulations regarding cyber policing in the Indonesian legal system. Law Number 2 of 2002 concerning the Indonesian National Police (Polri) does authorize the National Police (Polri) to maintain public security and order, enforce the law, and provide public protection, as stipulated in Article 13. However, these regulations are still general in nature and do not provide an operational legal basis for cyber patrols, cyber intelligence, digital surveillance, or artificial intelligence-based predictive policing in handling cybercrime. However, the borderless nature of online gambling requires a digital law enforcement model that differs from conventional crime. The absence of specific regulations regarding cyber policing limits law enforcement officers' ability to conduct cyber patrols, real-time monitoring, digital infiltration, and to oversee electronic systems used by online gambling networks. Furthermore, the use of digital surveillance technology also has the potential to raise privacy rights issues and abuse of authority if not clearly regulated through adequate regulations. Thus, the weaknesses in cyber policing regulations not only impact the effectiveness of law

enforcement but also create legal uncertainty regarding the use of cyber surveillance technology by state officials (Firmansyah, 2025).

Another fundamental problem lies in the weak regulation of electronic evidence and legal jurisdiction in handling cross-border online gambling. Article 5, paragraph (1) of the ITE Law recognizes electronic information and electronic documents as valid legal evidence, but the implementation of this norm in judicial practice still faces various technical and normative obstacles. The Criminal Procedure Code (KUHAP), which forms the basis of the criminal evidence system in Indonesia, still focuses on conventional evidence and therefore is not fully able to accommodate the nature of digital evidence, which is electronic, encrypted, and stored in a cloud system. In law enforcement practice, the process of obtaining digital evidence from foreign servers is often hampered by differences in legal jurisdiction, limited mutual legal assistance, and the lack of effective international cooperation in handling online gambling. Furthermore, many online gambling platforms use virtual private networks (VPNs), cryptocurrency, anonymous hosting, and nominee accounts, making it difficult to identify the main perpetrators and track the flow of digital gambling funds. These weaknesses in regulations regarding digital evidence and cyber jurisdiction demonstrate that the national legal system is not fully prepared to face the complexities of modern cybercrime, which is developing transnationally and is based on high technology (Abror, 2025).

The system for monitoring and blocking online gambling sites in Indonesia remains fragmentary, administrative, and not yet effectively integrated. The government, through the Ministry of Communication and Digital, has indeed blocked access to gambling sites based on the ITE Law and regulations related to the implementation of electronic systems. However, this blocking mechanism is more reactive because it is implemented after a site is detected operating, while online gamblers can easily create new domains, use mirror sites, or utilize foreign servers to circumvent blocking. Furthermore, there is no comprehensive regulation governing the obligations of digital platforms, social media, payment gateway providers, and electronic system providers in detecting and preventing the spread of online gambling activities.

Monitoring of digital transactions by financial institutions also faces coordination challenges involving PPATK, OJK, Bank Indonesia, and law enforcement agencies. Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes may provide a relevant legal basis for analyzing financial flows connected with criminal activity, including online gambling-related proceeds (Ruslan, 2025). However, automated transaction monitoring must not assume that an unusual transaction is automatically evidence of online gambling.

A transaction should therefore be identified as requiring further examination only when objective and legally relevant indicators are present. Such indicators may include a verified connection with an identified gambling platform, repeated transfers to accounts previously established through lawful procedures as being associated with gambling activity, transaction patterns inconsistent with the stated purpose of an account, rapid circular fund movements linked to known gambling infrastructure, or other objectively

documented risk indicators. Automated systems should generate a risk alert, not an automatic finding of illegality.

Before account blocking, freezing, disclosure, or criminal action is initiated, the alert should undergo additional verification by the competent financial or law-enforcement authority. This approach is necessary to distinguish legitimate digital financial activity from transactions that have a sufficiently substantiated connection with suspected online gambling and to prevent disproportionate interference with lawful economic activity.

The weakness of the Indonesian legal system in combating online gambling is also evident in the suboptimal regulations regarding the use of artificial intelligence surveillance and cyber intelligence in cyber law enforcement. The development of artificial intelligence technology has enabled law enforcement officials in various countries to use predictive policing, big data analytics, machine learning, and automated cyber monitoring to detect digital crime activity quickly and in real time. However, Indonesia currently does not have regulations specifically governing the use of artificial intelligence technology in cyber surveillance and cybercrime prevention. On the one hand, the use of AI surveillance is essential to address the rapid and digitally organized development of online gambling. However, on the other hand, without clear legal regulations, the use of digital surveillance technology has the potential to violate the right to privacy, personal data protection, and human rights as guaranteed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia and Law Number 27 of 2022 concerning Personal Data Protection. Therefore, the weaknesses in current national regulations demonstrate the urgent need for reforms to cyber policing laws that are not solely focused on criminal prosecution but also on building an integrative, adaptive, modern technology-based cyber oversight system that still guarantees the protection of the constitutional rights of Indonesia's digital communities.

Problems in Implementing Cyber Policing in Preventing and Enforcing Online Gambling in Indonesia

The implementation of cyber policing in preventing and enforcing online gambling in Indonesia still faces various empirical problems, demonstrating the state's suboptimal ability to address the development of modern cybercrime. Online gambling is growing rapidly through the use of digital technology, social media, mobile applications, and electronic transaction systems, making it difficult to control using conventional law enforcement methods. In practice, the Indonesian National Police, as the primary law enforcement institution, faces significant challenges in overseeing the increasingly complex and dynamic cyberspace. Article 13 of Law Number 2 of 2002 concerning the Indonesian National Police grants the National Police the authority to maintain public order and security, enforce the law, and provide protection and services to the public. However, the development of digital crime, particularly online gambling, has created new threats that require a law enforcement model based on information technology and modern cyber surveillance systems. Cyber policing essentially requires not only repressive capabilities in carrying out criminal action but also preventive capabilities through cyber patrols, cyber intelligence, digital surveillance, and real-time monitoring of people's digital activities. Empirical conditions indicate that the institutional transformation and technological

capacity of law enforcement officials have not been able to keep pace with the rapid development of the online gambling ecosystem, which is transnational, anonymous, and based on artificial intelligence.

One of the main challenges in implementing cyber policing in Indonesia is limited human resources and the scarcity of cyber investigators with specialized competencies in digital forensics, blockchain tracing, artificial intelligence monitoring, and cyber intelligence. Conventional investigative methods are no longer sufficient in handling online gambling, as perpetrators utilize advanced technologies such as virtual private networks (VPNs), cloud servers, anonymous accounts, cryptocurrency, and automated bot systems to conceal their identities and transaction activities. In practice, law enforcement often struggles to track down major online gambling operators because their operational systems utilize overseas servers and encrypted digital networks. Furthermore, investigators' ability to understand cryptocurrency transaction patterns, digital payment gateways, and artificial intelligence algorithms remains very limited. As a result, investigations often only reach small-scale operators, while the main actors controlling transnational online gambling networks remain elusive. It proves that Indonesia's cyber policing education and training system is still not completely adapted to modern cybercrime developments. In the context of a digital society, law enforcement officials should possess high-tech capabilities to enable early detection, digital network mapping, and real-time, integrated electronic transaction monitoring.

The next problem lies in the limited digital forensics infrastructure and cyber surveillance systems available to law enforcement. Handling online gambling requires a modern digital forensics laboratory to perform electronic data extraction, metadata analysis, digital data recovery, electronic transaction flow tracking, and digital evidence authentication. However, in practice, digital forensics facilities in Indonesia remain limited both in terms of quantity and quality of the technology used. Many regional law enforcement units lack adequate cyber forensic equipment, making the investigation process highly dependent on specific units at the central level. Furthermore, the lack of an integrated cyber monitoring system means that oversight of online gambling activities remains partial and reactive. Government blocking of gambling sites is often ineffective because perpetrators quickly change domains, create mirror sites, or utilize offshore hosting to evade detection. Furthermore, the national digital surveillance system is not yet supported by artificial intelligence surveillance technology and big data analytics capable of automatically detecting patterns of online gambling activity. As a result, cyber policing in Indonesia tends to be manual, slow, and unable to anticipate the rapid and massive development of digital gambling networks in cyberspace.

The unique characteristics of online gambling also complicate the investigation and legal evidence process. Unlike conventional gambling, which has a physical location and relatively easy-to-identify perpetrators, online gambling operates in a digital system that is anonymous, cross-jurisdictional, and utilizes high-level encryption technology. Many online gambling platforms use servers located outside of Indonesian jurisdiction, creating jurisdictional obstacles for law enforcement. Furthermore, the use of cryptocurrency,

nominee accounts, virtual accounts, and international payment gateways makes tracking the flow of gambling funds extremely complex. From an evidentiary law perspective, these conditions also create difficulties in obtaining valid electronic evidence, as stipulated in Article 5 of the Electronic Information and Transactions Law. Although electronic information is recognized as valid legal evidence, the authentication, validation, and chain of custody processes for digital evidence often face technical and administrative challenges. Much digital evidence is stored on cloud servers overseas, requiring law enforcement officials to collaborate internationally through mutual legal assistance mechanisms, a time-consuming and ineffective process. This situation demonstrates that the national legal and investigative systems are not yet fully prepared to deal with the transnational and high-tech nature of cybercrime.

Problems in cyber policing implementation are also evident in weak cyber intelligence and the limited capacity for integrated digital transaction monitoring. In practice, online gambling involves not only digital gaming activities but is also closely linked to money laundering, the use of escrow accounts, digital financial transactions, and illegal financial technology activities. However, coordination between the Indonesian National Police, the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), Bank Indonesia, and electronic system providers remains suboptimal. Digital transaction monitoring by each agency remains sectoral and lacks a real-time, integrated data exchange system. As a result, many suspicious transactions related to online gambling cannot be quickly detected by law enforcement. Furthermore, collaboration with digital platforms and social media in detecting online gambling promotions remains very limited. This is even though online gambling networks currently utilize social media algorithms, affiliate marketing, digital influencers, and automated advertising systems to reach a wide audience. These cyber intelligence weaknesses demonstrate that the current law enforcement approach still focuses on taking action after the crime has occurred and does not prioritize predictive policing strategies based on artificial intelligence and big data analytics, which are capable of systematic prevention.

In addition to technical and institutional issues, the implementation of cyber policing to combat online gambling also faces a structural problem, namely the lack of a comprehensive, integrated national cyber oversight system. To date, there are no specific regulations or institutions that integrate the functions of cyber patrol, cyber surveillance, cyber intelligence, and digital investigation into a single, unified national oversight system. As a result, online gambling is often handled in a fragmented manner by various institutions without effective coordination. The Ministry of Communication and Digital focuses more on blocking websites, the National Police (Polri) carries out criminal prosecution, the Financial Transaction Reports and Analysis Center (PPATK) monitors suspicious transactions, while the Financial Services Authority (OJK) and Bank Indonesia oversee the digital financial system separately. Yet, the nature of online gambling requires an integrated, multi-sectoral approach, involving aspects of information technology, digital financial systems, personal data protection, and cross-border cooperation. It demonstrates that cyber policing in Indonesia remains reactive and has not yet developed into integrated

cybersecurity governance capable of providing effective protection for the digital society. Therefore, a fundamental transformation is needed in the implementation of cyber policing through institutional strengthening, modernization of cyber oversight technology, development of artificial intelligence-based cyber intelligence, and integration of the national digital oversight system to address the complexities of online gambling in the digital era.

Reconstruction of Cyber Policing Law in the Prevention and Enforcement of Online Gambling through the Integration of Cyber Supervision and Digital Community Protection in Indonesia

The reconstruction of cyber policing law in the prevention and prosecution of online gambling in Indonesia must begin with the establishment of a national regulatory framework specifically governing cyber policing as an operational system of digital law enforcement. Such a National Cyber Policing Law should not duplicate the substantive criminal prohibitions already contained in the Criminal Code, the Electronic Information and Transactions Law, or other cybercrime regulations. Rather, its primary function should be to regulate the authority, procedures, limits, accountability mechanisms, and institutional coordination involved in cyber law enforcement.

Article 303 and Article 303 bis of the Criminal Code primarily regulate gambling as prohibited conduct, while Article 27 paragraph (2) of Law Number 1 of 2024 concerning Electronic Information and Transactions addresses the distribution, transmission, or accessibility of electronic information containing gambling content. Law Number 2 of 2002 concerning the Indonesian National Police regulates the general functions and authority of the police, while Law Number 27 of 2022 concerning Personal Data Protection establishes general safeguards for personal-data processing. However, these instruments do not comprehensively regulate the operational framework for cyber patrols, AI-assisted surveillance, digital infiltration, automated risk analysis, real-time transaction monitoring, cross-border digital investigation, or the procedural limits applicable to such powers.

Therefore, the proposed National Cyber Policing Law should function as a procedural and institutional framework law rather than as a replacement for existing criminal, electronic-information, policing, or personal-data legislation. Its regulatory scope should include: (a) cyber patrol authority; (b) conditions for digital surveillance and infiltration; (c) AI-assisted monitoring and human oversight; (d) procedures for digital transaction analysis; (e) electronic evidence acquisition and preservation; (f) emergency and judicially reviewable account-freezing mechanisms; (g) cross-border cyber jurisdiction; (h) inter-agency coordination; and (i) safeguards for privacy, personal data, legality, proportionality, and due process of law.

Further legal reforms should focus on establishing an Integrated Cyber Monitoring System, a national cyber oversight system that integrates the Indonesian National Police, the Ministry of Communication and Digital, PPATK, the Financial Services Authority (OJK), Bank Indonesia, the Attorney General's Office, and electronic system providers. Currently, online gambling supervision remains sectoral and fragmented, resulting in delayed and ineffective legal action. Therefore, the development of a national data center based on cyber

intelligence capable of integrating information on digital transactions, social media activity, gambling site access patterns, and electronic fund flows in real time is crucial. Specifically, the government needs to establish a 24-hour National Cyber Monitoring Center, supported by artificial intelligence and big data analytics, to map online gambling networks, detect suspicious transactions early, and identify digital gambling promotion patterns through social media and electronic platforms.

The proposed legal reconstruction should not authorize permanent or unconditional automatic blocking or freezing merely because an algorithm identifies a transaction or account as suspicious. Instead, the law should establish an emergency temporary freezing mechanism applicable only where there is an objectively documented and reasonable basis to believe that an account, digital asset, or transaction is directly connected to an ongoing online gambling operation or related criminal activity and where delay creates a material risk of asset dissipation, evidence destruction, or continued criminal activity.

A temporary emergency freezing measure should be authorized by a legally designated authority based on documented evidentiary indicators and should be limited to a clearly defined initial duration. Continued freezing beyond the emergency period should require judicial or other legally independent review. The affected individual or entity should receive notification unless notification would demonstrably compromise the investigation, and should have access to an objection, appeal, or review mechanism.

Accordingly, financial institutions and digital platforms may implement temporary transaction holds when legally required, but final freezing, seizure, confiscation, or other substantial restrictions on property rights must remain subject to evidentiary verification, human authorization, proportionality, and procedural review. This model allows rapid intervention while protecting legitimate account holders from wrongful or algorithmically generated restrictions.

Strengthening cyber intelligence and artificial intelligence-based predictive policing is also a crucial part of reconstructing cyber policing law in Indonesia. The current proliferation of online gambling has utilized digital algorithms, bot automation systems, cryptocurrency, and artificial intelligence in its operations, rendering conventional law enforcement methods inadequate. Therefore, law enforcement officers must be guided by predictive policing models based on artificial intelligence technology to detect patterns of digital gambling activity before criminal activity becomes widespread. Specifically, the Indonesian National Police (Polri) needs to establish an Integrated Cyber Intelligence Directorate with specific functions in digital profiling, cyber infiltration, AI-based monitoring, and automated cyber patrols against online gambling activities in cyberspace. Furthermore, the government needs to invest significantly in the development of modern digital forensics laboratories at the central and regional levels so that investigations no longer rely on limited facilities at the national level. Mandatory training on blockchain tracing, cryptocurrency investigation, digital evidence handling, and cyber intelligence should also be provided regularly to law enforcement officers to ensure their technological capabilities are on par with the evolving modus operandi of digital crime. In this context, legal reform is not sufficient simply to create new regulations; it must also be accompanied

by institutional modernization and continuous improvement of the human resource capacity of law enforcement.

The reconstruction of cyber policing law must also be directed at strengthening the digital evidence system and updating criminal procedural law to be more adaptive to developments in modern cybercrime. Currently, the regulation of electronic evidence in Article 5 of the Electronic Information and Transactions Law has not been accompanied by a comprehensive reform of the criminal evidence system in the Criminal Procedure Code (KUHP), which still focuses on conventional evidence. Therefore, a reformulation of criminal procedural law is needed to specifically regulate digital evidence collection procedures, electronic chain of custody, cyber forensic authentication, and mechanisms for examining electronic evidence across borders. Specifically, the government needs to establish national standards for digital forensic procedures that apply uniformly to all law enforcement officials handling online gambling and other cybercrimes. Furthermore, a cyber court system is needed to enable the examination of electronic evidence more quickly, efficiently, and based on digital technology. The state must also strengthen international cooperation through mutual legal assistance, extradition agreements, and cybercrime treaties with other countries to expedite the process of tracking foreign servers, freezing digital assets, and arresting online gambling operators across jurisdictions. Thus, updating criminal procedural law is an important part of building an effective cyber policing system that is capable of addressing the complexities of transnational cybercrime.

From the perspective of digital community protection, the reconstruction of cyber policing law must place cyberspace security as part of citizens' constitutional rights in a modern rule of law. The state is not only obliged to take criminal action but also to build a digital space that is safe, healthy, and free from the threat of online gambling, as stipulated in Article 28D and Article 28G of the 1945 Constitution of the Republic of Indonesia. Therefore, legal reforms must be directed at strengthening digital community protection through a preventative approach based on digital literacy, social media monitoring, and protecting vulnerable groups such as children and adolescents from exposure to online gambling. Specifically, the government needs to require all digital platforms to implement artificial intelligence content filtering capable of detecting and automatically removing online gambling content. Furthermore, a parental cyber protection system is needed to enable parents and schools to control children's access to digital gambling sites. The state also needs to establish a national digital security literacy program involving educational institutions, civil society, and the mass media to raise public awareness of the dangers of online gambling and cybercrime. Thus, the concept of cyber policing should not only be understood as a repressive law enforcement instrument, but also as a digital community protection system oriented towards social security and national resilience in cyberspace.

The reconstruction of cyber policing law in Indonesia should aim to develop a preventive, integrated, and accountable digital law enforcement framework grounded in cross-sectoral and international cooperation. Because online gambling involves criminal activity, digital platforms, electronic transactions, financial institutions, and cross-border infrastructure, no single institution can effectively address the entire ecosystem. Therefore,

the establishment of a National Cyber Command Center should be based on a coordinated institutional model rather than the transfer of all sectoral authority to one institution.

The National Cyber Command Center should be established as a permanent national coordination mechanism with the Indonesian National Police exercising primary operational authority in relation to criminal investigation and cyber law enforcement. The Ministry of Communication and Digital should remain responsible for matters concerning electronic-system governance, platform coordination, and administrative measures within its legal competence; PPATK should retain its statutory authority concerning the analysis of suspicious financial transactions; OJK and Bank Indonesia should continue exercising sectoral supervisory authority over regulated financial institutions and payment systems. The Command Center should therefore coordinate information exchange and joint operational responses without replacing the statutory powers of participating institutions.

To prevent overlapping mandates, the proposed law should expressly establish a single-command coordination protocol for cases classified as nationally significant or transnational cybercrime. Operational decisions concerning criminal investigation must remain under the authority of legally competent investigators, while blocking, transaction analysis, financial supervision, and regulatory action must remain subject to the authority of the relevant institution. The Command Center should function as an integration, coordination, and escalation mechanism supported by a shared case-management protocol, defined institutional responsibilities, documented requests for data, and audit trails for every cross-agency action.

A structured regulatory model for cyber policing should contain at least eight interrelated components. First, the law should regulate cyber patrols by distinguishing monitoring of publicly accessible digital spaces from intrusive surveillance requiring specific authorization. Second, AI-assisted surveillance and predictive analysis should be limited to decision-support functions and governed by accuracy testing, bias assessment, explainability, human oversight, periodic auditing, and correction mechanisms for inaccurate identification. Third, digital transaction monitoring should operate through objective risk indicators and verified alerts rather than automatic determinations of illegality.

Fourth, emergency account or digital-asset freezing should require documented evidentiary grounds, authorization by a legally competent authority, a defined temporary duration, subsequent judicial or independent review, notification where appropriate, and an accessible objection or appeal mechanism. Fifth, electronic evidence should be regulated through mandatory standards concerning authentication, metadata preservation, forensic imaging, integrity verification, chain of custody, cloud evidence, foreign-server evidence, and qualified forensic examination. Sixth, cross-border cyber jurisdiction should permit Indonesian authorities to exercise jurisdiction where a substantial connection exists with Indonesia, including the location of victims, financial consequences, targeted digital services, or other legally relevant connecting factors, while remaining subject to international cooperation and applicable sovereignty principles.

Seventh, digital platforms, financial institutions, payment providers, and electronic system operators should be subject to proportionate due-diligence obligations concerning detection, preservation, lawful reporting, and cooperation with authorized investigations. Finally, all cyber-policing powers must be subject to safeguards for privacy, personal-data protection, legality, necessity, proportionality, transparency, independent oversight, and due process of law. Unauthorized access to personal data, misuse of surveillance powers, manipulation of electronic evidence, or unlawful disclosure of protected digital information should give rise to administrative, disciplinary, civil, or criminal accountability according to the seriousness of the violation.

Through this structured regulatory model, the proposed National Cyber Policing Law would not merely expand state surveillance powers, but would establish a legally controlled system balancing effective cybercrime prevention with constitutional rights and protection of the digital community.

Conclusion

The research discovers that the development of online gambling in the digital society era has developed a modern form of cybercrime that is growing massively, transnationally, and is difficult to control through conventional law enforcement systems in Indonesia. The national legal system has basically regulated the prohibition of gambling through Article 303 and Article 303 bis of the Criminal Code and Article 27 paragraph (2) of the Electronic Information and Transactions Law, but these regulations are still partial and have not been able to address the complexity of online gambling that utilizes foreign servers, cryptocurrency, anonymous accounts, digital payment gateways, artificial intelligence, and cross-border electronic transaction systems. The implementation of cyber policing by the Indonesian National Police also still faces various technical, structural, and institutional obstacles in the form of limited cyber investigators, minimal digital forensics infrastructure, weak cyber intelligence, suboptimal supervision of digital transactions, and low integration of cyber supervision between state institutions. These conditions indicate that the national legal system and law enforcement system have not been fully adaptive to the development of cybercrime in the digital society era. Therefore, a reconstruction of cyber policing law is needed through the creation of comprehensive national regulations, strengthening of an integrated cyber monitoring system, the establishment of a national cyber command center, strengthening artificial intelligence-based predictive policing, harmonizing cross-sectoral regulations, and strengthening international cooperation in handling transnational online gambling. This legal reconstruction must be directed not only at strengthening criminal law enforcement but also at protecting the digital community as part of citizens' constitutional rights in a modern state governed by the rule of law.

Based on these conclusions, this study recommends that the government and the House of Representatives immediately establish specific regulations regarding national cyber policing that regulate cyber patrol, cyber surveillance, cyber intelligence, digital investigation, and the use of artificial intelligence in combating cybercrime, particularly online gambling. The Indonesian National Police (Polri) also needs to undertake institutional transformation by establishing an integrated cyber policing system supported

by modern technology, a digital forensics laboratory, and increasing human resource capacity in the fields of cyber intelligence and digital evidence handling. Furthermore, an integrated cyber monitoring system is needed that connects the National Police, the Ministry of Communication and Digital, the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), Bank Indonesia, and electronic system providers to monitor digital transactions and cyberspace in real time. The government also needs to strengthen international cooperation in tracking foreign servers, freezing digital assets, and exchanging cyber intelligence data to address the borderless nature of online gambling. Furthermore, digital citizen protection must be strengthened through cybersecurity literacy, social media monitoring, child protection in the digital space, and requiring electronic platforms to implement automated detection systems for online gambling content. With these steps, the reconstruction of cyber policing law in Indonesia is expected to create a digital law enforcement system that is preventative, integrative, adaptive, and effective in providing legal protection for the digital citizen from the threat of online gambling in the era of global information technology development.

References

- Abror, M. M. (2025). Fenomena Judi Online Dalam Perspektif Hadis Tentang Tanggungjawab Dan Pengelolaan Harta. *Advances In Humanities And Contemporary Studies*, 88–95.
- Amelia, Y. G. (2024). Fenomena Judi Online Dan Degradasi Moral. *At-Tuhfah: Jurnal Studi Keislaman*, 56–67.
- Anugrahi, A. P. (2024). Fenomena Trend Judi Online Pada Remaja. *Prosiding Seminar Nasional Psikologi (Sinopsi)*.
- Bakhtiar, S. H. (2024). Fenomena Judi Online: Faktor, Dampak, Pertanggungjawaban Hukum. *Innovative: Journal Of Social Science Research*, 1016–1026.
- Fairuzzen, M. R. (2024). Perkembangan Hukum Dan Kejahatan Siber “Cybercrime” Di Indonesia. *Indonesian Journal Of Islamic Jurisprudence, Economic And Legal Theory*, 139–153.
- Fathor, K. A. (2024). Fenomena Iklan Judi Online Pada Platform Digital Generasi Z Di Indonesia. *Optimal Jurnal Ekonomi Dan Manajemen*, 184–189.
- Firmansyah. (2025). Kebijakan Hukum Pidana Mengenai Kejahatan Judi Online (Cyber Gambling) Di Indonesia. *Jurnal Hukum, Politik Dan Ilmu Sosial*, 54–62.
- Herawati, D. A. (2025). Indonesia Darurat Judi Online: Judi Online Sebagai Ancaman Nirmiliter Terhadap Ketahanan Nasional. *Citizen: Jurnal Ilmiah Multidisiplin Indonesia*, 1251–1261.
- Juhara, N. F. (2025). Efektivitas Penegakan Hukum Terhadap Judi Online Di Indonesia: Analisis Yuridis Dan Sosiologis. *Journal Of Contemporary Law Studies*, 153–164.
- Kanda, A. S. (2024). Dampak Fenomena Judi Online Terhadap Disorganisasi Sosial Pada Mahasiswa Di Bandung. *Jurnal Ilmiah Research Student*, 7–17.
- Kesuma, R. D. (2023). Penegakan Hukum Perjudian Online Di Indonesia: Tantangan Dan Solusi. *Jurnal Exact: Kajian Kemahasiswaan*, 34–52.
- Mubarok, Z. A. (2024). Dampak Dan Fenomena Maraknya Perjudian Online Bagi

- Mahasiswa Di Indonesia. *Smart Law Journal*, 13–30.
- Rohmy, A. M. (2021). Uu Ite Dalam Perspektif Perkembangan Teknologi Informasi Dan Komunikasi. *Dakwatuna: Jurnal Dakwah Dan Komunikasi Islam*, 309–339.
- Ruslan, M. I. (2025). Formulasi Hukum Pidana Dalam Menanggulangi Fenomena Judi Online Sebagai Patologi Sosial Di Indonesia. *Indonesian Journal Of Intellectual Publication*, 138–147.
- Siregar, D. Y. (2025). Fenomena Maraknya Judi Online Di Kalangan Masyarakat. *Adagium: Jurnal Ilmiah Hukum*, 15–27.
- Tumanggger, D. S. (2025). Analisis Kriminologis Terhadap Perkembangan Perjudian Online Di Indonesia. *Integrative Perspectives Of Social And Science Journal*, 15–27.
- Tuwo, C. P. (2016). Penerapan Pasal 303 Kitab Undang-Undang Hukum Pidana Tentang Perjudian. *Lex Crimen*.