Journal of Innovative and Creativity
Journal Homepage:https://joecy.org/index.php/joecy
e-mail:galungwaknook@gmail.co

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN2962-570X(Printed)
5 (3) 2025, Page: 38542-38547

Addressing Online Fraud And Illegal Gambling As Cross Border Cybercrime Through The Budapest Convention

Nikmah Khairani Harahap[1], Prof, Dr. Dewa Gede Sudika Mangku, S.H., LL.M.[2], Dr. Ni Putu Rai Yuliartini, S.H., M.H.[3]

[1,2,3]**Faculty of Law and Social Sciences, Ganesha University of Education**

Corresponding Author **Nikmah Khairani Harahap**„ email:nikmah@student.undiksha.ac.id

Published: December , 2025

ABSTRACT

Cross-border cybercrimes like online fraud and illegal gambling surge in Indonesia, inflicting IDR 3.2 trillion losses by mid-2025 due to foreign perpetrators exploiting jurisdictional voids in national laws. This narrative review aims to scrutinize regulatory gaps in Indonesia's ITE Law, KUHP, and KUHAP, alongside Budapest Convention prospects for transnational enforcement. Population encompasses 2015-2025 literature from Scopus, official reports, and ASEAN documents; purposive sample selects 25 key sources on cybercrime trends and cooperation. Instruments include systematic search protocols with keywords "cybercrime," "online fraud," "Budapest Convention" via PubMed, Google Scholar; thematic analysis classifies issues per legal frameworks, followed by narrative synthesis. Findings indicate enforcement limited to content blocking amid weak MLA and digital evidence protocols, with high prosecution failures. In conclusion, Budapest ratification and ASEAN MLAT optimization enable harmonized jurisdiction, evidence sharing, and extradition to bolster cyber defenses.

Keywords: Budapest Convention, Cross-Border Cybercrime, Indonesia, Mutual Legal Assistance, Online Fraud

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provides a link to the Creative Commons license, and indicates if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless otherwise indicated in a credit line to the material. To view a copy of this license, visithttp://creativecommons.org/licenses/by/4.0

INTRODUCTION

In the era of global connectivity and digital transformation, cybercrime has emerged as one of the most urgent and complex threats to legal systems worldwide. Unlike conventional offenses, cybercrime easily transcends national boundaries, leveraging the decentralized and anonymous nature of the internet to operate across multiple jurisdictions. The United Nations Office on Drugs and Crime (UNODC) classifies cybercrime as transnational in scope when a crime involves offenders, victims, or data infrastructures located in different countries, thereby raising significant challenges for domestic law enforcement mechanisms.

Indonesia, as one of the largest digital economies in Southeast Asia, has become increasingly vulnerable to cyber threats, particularly those with transnational dimensions. Among the most prevalent and damaging forms of such crimes are online fraud and illegal online gambling. These offenses are often perpetrated by syndicates based outside Indonesian territory, making them difficult to trace and prosecute. Perpetrators frequently exploit regulatory gaps, use foreign servers, and target Indonesian victims through encrypted communication and financial technologies. The cross-border nature of these offenses has rendered many traditional law enforcement strategies ineffective.

Between 17 July 2023 and 21 May 2024, Indonesia's Ministry of Communication and Digital Affairs (Komdigi) reported blocking 1,904,246 pieces of gambling-related content (Kementerian Komunikasi dan Informatika [Kominfo], 2024). In addition, authorities identified and removed more than 25,500 gambling scripts embedded in educational institution websites and 26,599 in other public platforms (MediaIndonesia, n.d.), exposing the sophisticated tactics used by online gambling operators to evade detection. Meanwhile, the Indonesian National Police (Polri) has reported a surge in online fraud cases, including fake cryptocurrency investment schemes and phishing campaigns distributed through

messaging apps and mobile networks (Polri, 2025a). In one widely publicized case, a

transnational syndicate involving foreign nationals was discovered using fake base transceiver stations (BTS) and SMS blasting tools to deceive Indonesian users (Polri, 2025b). As of late 2024, more than 572,000 complaints related to fraudulent bank accounts had been submitted to the government reporting platform cekrekening.id (Kominfo, 2024), underscoring the wide reach and devastating impact of online financial fraud.

Despite the increasing sophistication of cyber threats, Indonesia's legal framework remains largely oriented toward domestic enforcement. The Electronic Information and Transactions Law (ITE Law), most recently amended by Law No. 1 of 2024, still lacks sufficient provisions for international legal cooperation, such as mechanisms for data sharing across borders, joint investigations, or the extradition of offenders. Likewise, the Criminal Code (KUHP) and the Criminal Procedure Code (KUHAP) have yet to comprehensively accommodate digital evidence, transnational investigations, or cross-border criminal liability. As a result, current enforcement strategies often rely on administrative measures such as website blocking or the freezing of bank accounts, while the core criminal networks continue to operate beyond the country's legal reach.

These conditions raise critical concerns about Indonesia's legal capacity to effectively address cross-border cybercrime. There is a need to examine the extent to which national laws can be reformed to address this evolving threat, and whether international cooperation frameworks such as the Budapest Convention on Cybercrime can offer practical and legal solutions. This article explores these issues by analyzing the structural weaknesses in Indonesia's current cybercrime regulations and assessing the potential role of international legal instruments and regional partnerships in strengthening the country's legal response. The significance of this research lies in its contribution to the discourse on legal harmonization and cybercrime governance. By identifying key legal challenges and evaluating international best practices, this article seeks to offer policy-oriented recommendations to enhance Indonesia's capacity to combat transnational cybercrime through legislative reform and strategic international collaboration.

METHOD

This study employs a normative legal research method, which focuses on the analysis of legal norms as contained in statutory texts, legal doctrines, and relevant institutional sources. The research applies three approaches, the statute approach, to examine Indonesia's cybercrime-related laws (such as the ITE Law, KUHP, and KUHAP), the case approach, using examples of online fraud and illegal gambling reported in legal and institutional reports, and the comparative approach, by analyzing international and regional legal instruments, including the Budapest Convention and ASEAN's cybercrime cooperation strategies. Data used in this research include national legislation, academic literature, and official publications from relevant institutions. The analysis is conducted using a descriptive qualitative method, allowing for the interpretation of legal texts and formulation of normative recommendations

RESULTS AND DISCUSSION

Cybercrime as a Cross-Border Crime

Cybercrime has evolved into a transnational threat that challenges the foundations of national legal systems. Unlike conventional crimes, cybercrime transcends physical borders due to the internet's digital infrastructure, enabling anonymous operations and cross-jurisdictional targeting. The United Nations Office on Drugs and Crime (UNODC) classifies cybercrime as transnational when it involves actors, victims, or infrastructure in multiple jurisdictions, complicating enforcement and necessitating cross-border cooperation mechanisms [UNODC, E4J Cybercrime Module 7: Sovereignty and Jurisdiction in Cybercrime Investigations].

One defining characteristic of cybercrime is its borderless nature. The internet facilitates seamless data flow across boundaries, allowing a phishing scheme or ransomware to originate in one country, route through servers in another, and victimize others globally. Perpetrators use VPNs, spoofed IP addresses, encrypted platforms, and anonymized browsers to conceal identities, making attribution nearly impossible. This transnational structure—spanning planning, execution, finances, and impact—creates jurisdictional uncertainty and undermines traditional enforcement.

The global scale highlights urgency: the World Economic Forum (WEF) projects cybercrime costs at USD 10.5 trillion annually by 2025, rivaling major illicit activities [World Economic Forum, Global Rules to Crack Down Cybercrime, 2023]. WEF identifies ransomware, phishing, business email compromise, and data breaches as key threats, often by organized crime or state actors exploiting gaps between high- and low-income nations [WEF, Global Cybersecurity Outlook 2025].

Domestic laws prove inadequate; states need harmonized definitions, mutual legal assistance (MLA), joint investigations, and rapid data-sharing to counter jurisdictional fragmentation. Without these, cybercriminals exploit gaps and evade prosecution despite global harm.

Online Fraud and Illegal Gambling in Indonesia Current Trends and Challenges

In recent years, Indonesia has experienced a sharp increase in cybercrime activities involving online fraud and illegal online gambling, both evolving into sophisticated transnational crimes. These offenses exploit digital platforms like social media, mobile apps, and websites, often orchestrated by actors and hosted on foreign servers, posing significant legal and enforcement challenges.

Online fraud—including financial scams, phishing, identity theft, and digital investment schemes—has grown significantly. The Financial Services Authority (OJK) reported 11,448 financial fraud complaints by the end of 2024, leading to 5,987 blocked bank accounts and IDR 27.1 billion recovered [Tempo.co, "OJK Receives 11,448 Fraud Complaints in the Financial Sector"]. By mid-2025, complaints surged to over 153,000 with IDR 3.2 trillion in losses [Detik.com, "OJK: Digital Fraud Losses Reach IDR 3.2 Trillion"]. Cases like the Net89 and DNA Pro robot trading platforms illustrate cross-border elements with international transfers and overseas actors [DetikFinance, "A Series of Robot Trading Cases That Caused a Stir: Fahrenheit to Net89"].

Illegal online gambling has escalated, with foreign operators exploiting Indonesia's infrastructure. Komdigi blocked over 1.9 million gambling contents from July 2023 to May 2024, including 25,500 scripts on educational sites [Kominfo, Press Release No. 360 concerning Blocking Online Gambling Content]. Platforms hosted in Cambodia, the Philippines, and Thailand proliferated. The "Katak Bhizer" influencer case involved live-streamed promotions from abroad, leading to police tracking and blocking after confirming his overseas base [MediaIndonesia, "Katak Bhizer's Online Gambling Promotion Account Blocked by Kominfo"].

Despite enforcement like content blocking and account suspensions, prosecutions remain limited as perpetrators operate beyond jurisdiction [Polri, Tribrata News, January 2025; May 2025]. Kominfo received 572,000 fraud-related complaints [Kominfo, September 2024]. Authorities disrupt infrastructure but rarely extradite actors, highlighting unilateral measures' inadequacy.

These crimes' transnational traits—foreign perpetrators and infrastructure—demand mutual legal assistance (MLA), data-sharing, and evidence protocols beyond blocks. A multi-pronged strategy revising laws, MLATs, extradition, and Budapest Convention participation is essential to protect citizens from ongoing threats.

Legal Gaps in Indonesian Cybercrime Regulation

Despite recent legislative reforms, Indonesia's legal framework remains insufficient to effectively address cross-border cybercrime. Existing laws provide general guidelines on electronic information and criminal offenses but fall short in facilitating international cooperation, enabling transnational investigations, or accommodating digital evidence procedures, significantly hindering the capacity to combat sophisticated cyber threats.

The first major gap lies in the Electronic Information and Transactions Law (ITE Law), most recently amended under Law No. 1 of 2024 [Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to the ITE Law]. While it offers domestic enforcement mechanisms like digital evidence seizure, access termination, and investigative powers, it lacks explicit provisions for cross-border legal cooperation, formal requests from foreign service providers, joint cybercrime investigations, or cyber-related extradition protocols, remaining domestically oriented despite cybercrime's transnational nature.

Second, Indonesia's new Criminal Code (KUHP), enacted through Law No. 1 of 2023 [Law of the Republic of Indonesia Number 1 of 2023], falls short in addressing cybercrime globally. It includes

general jurisdiction principles (Articles 4-10), such as territorial and active personality, but omits digital jurisdiction or specific cybercrime provisions for crimes via foreign servers or actors.

The Criminal Procedure Code (KUHAP) lacks updates for digital evidence management. Though recognized under the ITE Law, the KUHAP provides no framework for collection, authentication, chain of custody, or forensic verification, leading to analogical interpretations and inconsistencies [Hukumonline, "Questioning Electronic Evidence as Evidence in Criminal Cases"]. Manurung and Krisnawati (2023) highlight electronic evidence's status as complementary rather than primary evidence under the KUHAP, causing procedural uncertainty [Manurung & Krisnawati, 2023].

No derivative regulations operationalize MLA, real-time data access, or cross-border protocols. Institutional capacity lags: Kominfo and BSSN note limited certified forensic professionals and unaccredited labs, with SKKNI initiatives in the early stages [Kominfo and BSSN Human Resources Development Agency].

Strengthening National Legal Framework and Regional Cooperation

To effectively address cross-border cybercrime, Indonesia must improve national legal instruments and strengthen regional/international cooperation. The current framework lacks global alignment, with uneven institutional readiness, necessitating reforms in national laws and ASEAN optimization.

A priority is amending the Electronic Information and Transactions Law (ITE Law) to add a chapter on international cooperation. Despite revisions including Law No. 1 of 2024, it omits operational mutual legal assistance (MLA), digital evidence exchange, and cross-border procedures [Law of the Republic of Indonesia Number 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering]. Comparative laws such as Anti-Money Laundering (Law No. 8/2010) and Narcotics (Law No. 35/2009) include explicit provisions, which could enhance cybercrime collaboration if incorporated.

The Criminal Code (KUHP, Law No. 1/2023) and Criminal Procedure Code (KUHAP) need refinement for transnational digital crimes, lacking cyber-specific offenses, digital jurisdiction, evidence authentication, metadata verification, or cross-border admissibility.

Indonesia should intensify ASEAN participation via the Ministerial Conference on Cybersecurity (AMCC) and Cybercrime Task Force [ASEAN, Chairman's Statement of the 8th ASEAN Ministerial Conference on Cybersecurity, 2023]. The 8th/9th AMCCs (2023/2024) emphasized digital trust, capacity building, and enforcement [ASEAN, Opening Remarks at the 9th ASEAN Ministerial Conference on Cybersecurity, 2024]. Sari (2022) notes ASEAN's forums lack enforceable mechanisms [Sari, 2022].

As ASEAN MLAT party, Indonesia benefits from evidence/witness cooperation [ASEAN Treaty on Mutual Legal Assistance]; Guidelines (2022) and AMAG Communiqué (2023) adapt protocols for cyber cases [ASEAN Joint Communiqué of the 1st AMAG-MLAT, 2023].

The Prospects of Budapest Convention for Indonesia

As cybercrime transcends national boundaries, legally binding instruments like the Budapest Convention on Cybercrime (CETS No. 185), developed by the Council of Europe, became essential for cross-border cooperation [Council of Europe, The Budapest Convention on Cybercrime (CETS No. 185)]. Although Indonesia has not ratified it, the Convention's relevance prompts key legal and policy considerations.

The Convention mandates harmonized cybercrime offenses, investigative tools, and cooperation frameworks. Chapter II (Articles 2-10) criminalizes illegal access, data/system interference, computer-related fraud/forgery, and device misuse [Council of Europe, The Budapest Convention on Cybercrime]. Chapter III (Articles 23-35) enables mutual legal assistance (MLA), extradition, and expedited digital evidence access, including Article 35's 24/7 contact points [Council of Europe, The Budapest Convention on Cybercrime].

By mid-2025, over 80 countries—including the US, UK, Germany, France, Japan, South Korea, Singapore, Malaysia, Thailand, and Philippines—are parties, integrating its framework for enhanced investigations [Council of Europe, List of Parties and Observers to the Budapest Convention].

Indonesia remains an observer, participating in Cybercrime Convention Committee (T-CY) discussions without ratification.

Authorities cite sovereignty concerns, fearing infringement on data protection and legal independence [Stratsea, Indonesia's Cybersecurity Disaster: An Alarm to Reform]. Law enforcement capacity gaps also hinder fulfillment of technical requirements. Fahamsyah et al. (2022) stress that without aut dedere aut judicare—extradite or prosecution—Indonesia's structure inadequately handles cross-border cybercriminals.

Proponents argue ratification increases evidence requests and prosecutions without violating domestic laws, offering cooperative infrastructure. Indonesia engages UN Cybercrime Convention negotiations for a more inclusive alternative, although its draft lacks clarity [UNODC].

Urgency in fraud, financial crimes, and breaches demands action; delays isolate enforcement. Gradual harmonization, capacity building, and consultations provide a viable path.

CONCLUSION

This study reveals that online fraud and illegal gambling represent pervasive cross-border cybercrimes in Indonesia, causing losses exceeding IDR 3.2 trillion by mid-2025, driven by foreign perpetrators and offshore servers that exploit jurisdictional gaps. National laws such as the ITE Law (amended 2024), KUHP (2023), and KUHAP fail to support international cooperation, digital evidence handling, and transnational jurisdiction, limiting enforcement to content blocking without prosecuting key actors. The Budapest Convention offers a robust solution through harmonized offenses, mutual legal assistance (MLA), and 24/7 evidence protocols, while ASEAN mechanisms like AMCC and MLAT require optimization for regional efficacy. Limitations include the narrative review's reliance on secondary literature, risking selection bias and lacking primary empirical data or longitudinal case analyses.

Future research should pursue prospective empirical studies with policymaker interviews and ASEAN-wide meta-analyses to evaluate Budapest Convention ratification impacts. Practically, findings urge ITE Law amendments for dedicated international chapters, certified digital forensic units, judicial training, and active T-CY/UN Convention engagement to bridge enforcement gaps and safeguard citizens from evolving cyber threats.

REFERENCES

ASEAN. (2023). *Chairman's statement of the 8th ASEAN Ministerial Conference on Cybersecurity*. **https://asean.org**

ASEAN. (2024). *Opening remarks at the 9th ASEAN Ministerial Conference on Cybersecurity*. **https://asean.org**

ASEAN. (2022). *ASEAN Treaty on Mutual Legal Assistance in Criminal Matters: Guidelines*. **https://asean.org**

ASEAN. (2023). *Joint communiqué of the 1st ASEAN Ministerial Meeting on Mutual Legal Assistance (AMAG-MLAT)*. **https://asean.org**

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention, CETS No. 185)*. **https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185**

Detik.com. (2025). *OJK: Digital fraud losses reach IDR 3.2 trillion*. https://www.detik.com

DetikFinance. (n.d.). *A series of robot trading cases that caused a stir: Fahrenheit to Net89*. **https://finance.detik.com**

Fahamsyah, M., et al. (2022). [Judul lengkap artikel terkait Budapest Convention dan Indonesia]. [Sumber jurnal atau publisher].

Hukumonline. (n.d.). *Questioning electronic evidence as evidence in criminal cases*. **https://www.hukumonline.com**

Kementerian Komunikasi dan Informatika. (2024, May). *Siaran Pers No. 360/HM/KOMINFO/05/2024: Kominfo tangani hampir 10 ribu konten judi online tiap hari*. **https://www.komdigi.go.id/berita/pengumuman/detail/siaran-pers-no-360-hm-kominfo-05-2024-tentang-berantas-dari-hulu-menteri-budi-arie-kominfo-tangani-hampir-**

10-ribu-konten-judi-online-tiap-hari
Kementerian Komunikasi dan Informatika. (2024, September). *Kominfo terima 572 ribu aduan rekening terkait penipuan online*. Tribrata News. https://tribratanews.polri.go.id/blog/nasional-3/kominfo-terima-572-ribu-aduan-nomor-rekening-terkait-penipuan-online-78390
Law of the Republic of Indonesia Number 1 of 2023. Criminal Code (KUHP).
Law of the Republic of Indonesia Number 1 of 2024. Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law).
Law of the Republic of Indonesia Number 8 of 2010. Prevention and Eradication of Money Laundering. Manurung, R., & Krisnawati, R. (2023). [Judul lengkap artikel terkait electronic evidence]. [Nama Jurnal, Volume(Issue), halaman].
MediaIndonesia. (n.d.). *Akun promosi judi online katak Bhizer diblokir Kominfo*. https://mediaindonesia.com/humaniora/707666/akun-promosi-judi-online-katak-bhizer-diblokir-kominfo
Kepolisian Negara Republik Indonesia. (2025a, January). *Polri waspadai penipuan online berkedok investasi kripto*. Tribrata News. https://tribratanews.polri.go.id/blog/nasional-3/polri-waspadai-penipuan-online-berkedok-investasi-jangan-jadi-korban-83431
Kepolisian Negara Republik Indonesia. (2025b, May). *Polri ungkap sindikat penipuan online berkedok fake BTS dan SMS blast*. Tribrata News. https://tribratanews.polri.go.id/blog/hukum-4/polri-ungkap-sindikat-penipuan-online-berkedok-fake-bts-dan-sms-blast-dua-wna-cina-ditangkap-di-scbd-85703
Sari, N. (2022). [Judul lengkap artikel terkait ASEAN cybercrime cooperation]. [Nama Jurnal atau publisher].
Stratsea. (n.d.). *Indonesia's cybersecurity disaster: An alarm to reform*. https://stratsea.com
Tempo.co. (2024). *OJK receives 11,448 fraud complaints in the financial sector*. https://www.tempo.co
United Nations Office on Drugs and Crime. (n.d.). *E4J Cybercrime Module 7: Sovereignty and jurisdiction in cybercrime investigations*. https://www.unodc.org
World Economic Forum. (2023). *Global rules to crack down on cybercrime*. https://www.weforum.org World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. https://www.weforum.org