DE LEGA LATA Jurnal Ilmu Hukum
Volume 10 Nomor 2, July-December 2025
E-ISSN: 2477-7889 I ISSN: 2477-653X I Akreditasi: SINTA 3, SK No: 28/E/KPT/2019
http://jurnal.umsu.ac.id/index.php/delegalata

Law Enforcement of Transnational Cybercrime: Case Study in Indonesia

Martono[1], **M. Gary Gagarin Akbar**[2], **Y Rahmatiar**[3]
[1,2,3] Universitas Buana Perjuangan Karawang, Indonesia
Email: hk21.martono@mhs.ubpkarawang.ac.id (Corresponding Author)

Accepted: 10-05-2025. Revised: 25-06-2025 Approved: 25-06-2025 Published: 01-07-2025
DOI: 10.30596/dll.v10i2.24627

How to cite:
Martono. (2025). "Law Enforcement of Transnational Cybercrime: Case Study in Indonesia", De Lega Lata: Jurnal Ilmu Hukum, Volume 10 (2): p. 279-286

Abstract

Transnational cybercrime is a common problem in governance amidst digitalization and even across national borders, thus requiring a fast, adaptive, and international cooperation-based legal response. The purpose of this study is to analyze the Indonesian national legal system in responding to transnational cybercrime, including identifying emerging obstacles and institutional responses and multinational cooperation that have been formed. The approach used is normative juridical, by analyzing primary and secondary legal materials that refer to the case and perception approaches to legal regulations. The results of this study are that Indonesia already has a number of legal instruments used to prosecute cybercrime, such as the ITE Law, the Criminal Code, and international legal instruments such as the Mutual Assistance Law (MLA) and Indonesia's participation in the United Nations Convention Against Transnational Organized Crime (UNTOC). On the institutional side, the existence of the Cyber Crime Directorate, BSSN, and other related agencies is an important foundation in detection and enforcement efforts, but there are still obstacles such as limited jurisdiction, lack of harmonization of international regulations, and limited technology and human resources. One of the case studies analyzed revealed the complexity in the law enforcement process for cybercrime involving perpetrators from abroad and causing major financial losses in Indonesia.

Keywords: *International Law, Indonesia, Cybercrime, Jurisdiction.*

INTRODUCTION

Digitalization in the era of modern society has brought about massive changes in aspects of human life. On the one hand, digital technology drives efficiency and global connectivity, but on the other hand, it opens up new space for the emergence of various forms of crime whose boundaries are difficult to recognize. One form of modern crime that is increasingly disturbing is cybercrime, namely a criminal act that utilizes the information technology system as the main means in carrying out its actions that have an impact across national borders. The phenomenon of cybercrime is increasingly complex when carried out across national jurisdictions. Cybercriminals can be in one country, while their victims are in another country, thus creating serious challenges in national law enforcement, thus requiring an adaptive and collaborative legal approach between countries (Djanggih & Qamar, 2018). djaThese challenges are not only

technical, but also involve complex legal issues, such as differences in law, extradition treaties, and legal recognition between countries.

Indonesia, as the country with the fourth largest number of internet users in the world, is not immune from cross-border cybercrime attacks. These crimes do not only target individuals, but also institutions, government agencies, and even vital national infrastructure (Khoirunnisa & Jubaidi, 2024). In this case, the principle of extraterritoriality in international criminal law becomes relevant, where a country can claim jurisdiction over a crime that occurs outside its territory if the crime has a direct impact on its national interests (Hiariej, 2024). Then, the implementation of this principle also requires strong international legal support and effective bilateral and multilateral cooperation. Therefore, it is crucial for Indonesia to have a law enforcement strategy that is not only responsive, but also adaptive and participatory to the dynamics of global threats that continue to develop (Safitra et al., 2023).

One real example of the complexity of cross-border cybercrime in Indonesia is the case of an international online fraud syndicate led by a Chinese citizen with the initials ZS. This syndicate operated from abroad, precisely in Dubai, United Arab Emirates, with the modus operandi of fake job vacancies as office workers related to computers abroad who were willing to pay high salaries. Then the victims were made operators to operate an online fraud network with the "paid click like" mode. Victims were promised payment for liking certain content online, but were asked to make a deposit first. After depositing funds, the victim did not receive the promised reward, and the funds that had been deposited were not returned. In addition to Indonesian citizens, suspect ZS also committed online fraud in three other countries, including Thailand, India, and China, which overall caused losses of up to hundreds of billions of rupiah. However, because the crime was committed outside the jurisdiction, Indonesian law enforcement officers could not immediately take action against the perpetrators. ZS was only successfully secured after entering Indonesian territory in June 2024 (Chaterine & Ihsanuddin, 2024). This case shows the jurisdictional obstacles that require international cooperation in a manner such as Mutual Legal Assistance (MLA), which in practice is often slow and marked by complex administrative and procedural obstacles.

Although normatively Indonesia has taken legal steps through various instruments, the challenges of law enforcement against transnational cybercrime are still very significant. The main instruments used are Undang-Undang Nomor 11 Tahun 2008 about Informasi dan Transaksi Elektronik (UU ITE), according to the changes to be Undang-Undang Nomor 1 Tahun 2024. Besides that, Peraturan Pemerintah Nomor 71 Tahun 2019 about Implementation of Electronic Systems and Transactions also underlines how important electronic system security, data protection, and the obligation to be able to secure the system as an effort to maintain the integrity of information technology. Then to support international collaboration in eradicating international scale crime, Indonesia has also ratified Undang-Undang Nomor 1 Tahun 2006 about Bantuan Timbal Balik dalam Masalah Pidana (Mutual Legal Assistance/MLA). Then, Indonesia has also become part of United Nations Convention Against Transnational Organized Crime (UNTOC) which was ratified through Undang-Undang Nomor 5 Tahun 2009, as a form of global commitment to handling transnational organized crime, including cybercrime. However, limited legal jurisdiction and less than optimal cooperation mechanisms between countries are still the main obstacles to enforcing the law against cross-border cybercrime in Indonesia.

Referring to the above explanation, it can be concluded that transnational cybercrime is a global legal phenomenon that requires a multi-dimensional approach. Coordination is needed between aspects of national law, international law, cybersecurity policy, and increasing institutional capacity. Referring to this phenomenon, researchers are interested in studying in depth the law enforcement against transnational cybercrime in Indonesia, as well as knowing

the obstacles or constraints faced by Indonesian law enforcement officers in handling transnational cybercrime.

METHOD RESEARCH

The research approach uses normative juridical. Data collection with document studies, which includes the collection and analysis of applicable legal regulations supported by relevant literature to understand the concept of law enforcement related to cross-border cybercrime in Indonesia (Soekanto & Mamudji, 2012). This approach aims to provide a legal analysis of the effectiveness of the applicable legal system. In this study, several legal approaches are used to obtain a comprehensive understanding. The first legal approach will use statute rules, which focuses on analyzing relevant laws and regulations that are in line with the legal issues to be studied.

The second approach is a conceptual approach, which aims to explain and understand the underlying theory or concept related to law enforcement for transnational cybercrime. In addition, the third approach is a case approach, which will be carried out to analyze criminal acts on a cross-country scale that have occurred previously to describe their practice in the Indonesian legal system. In this study, the main data sources come from primary and secondary data. Primary data includes laws and regulations in handling transnational cybercrime, as well as examples of settlement cases involving the concept. While secondary data is obtained from a study of journals, previous research, and relevant literature sources to enrich the analysis of law enforcement for transnational cybercrime.

DISCUSSION

1. Law Enforcement of Transnational Cyber Crimes

In the increasingly connected digital era, cybercrime has become one of the most worrying forms of contemporary crime. Its emergence cannot be separated from the rapid digitalization that has an impact on the advancement of technology and communication that has become a necessity for various aspects of human life. This crime is no longer limited to physical space, it moves dynamically in the limitless virtual space. It can be explained that cybercrime is generally defined as "a crime committed through or against computer networks and the internet."(Bego et al., 2025). This reflects the basic character of cybercrime that operates through digital media and often exploits gaps in technological systems.

The digital transformation that was originally intended to make human life easier has now become a new means for criminals to carry out their actions more subtly and are difficult to detect. In concrete terms, the forms of cybercrime are very diverse. Not only limited to hacking or breaking into computer systems, but also include online fraud, the spread of malware, digital identity theft, and cyber attacks on the country's critical infrastructure systems such as energy, financial, and transportation networks (Bego et al., 2025). Any form of crime that is not only detrimental to individuals or institutions and can create vulnerabilities to national security.

In a global context, cybercrime is categorized as a form of criminal act between countries or transnational crime. This means that this crime has a nature and impact that goes beyond the jurisdiction of one country. The perpetrators, victims, and consequences of the crime can be in different geographic locations, making it difficult to enforce the legal process. There are three main characteristics that make transnational cybercrime difficult to prosecute effectively: first, this act is carried out anonymously, making it difficult to track the identity of the perpetrator; second, digital evidence is very fragile and can easily be lost if not immediately secured; and third, the geographical element of this crime involving more than one country creates significant jurisdictional challenges (Aini & Lubis, 2024). Jurisdictional constraints are one of the most fundamental problems in law enforcement against cross-border cybercrime.

When the perpetrator of the crime is domiciled in one country, while the victim is in another country, the law enforcement process cannot be carried out immediately. The reason is that there are differences in legal systems, regulations, and enforcement mechanisms in each country. Not all countries have specific or equivalent legal instruments in dealing with cybercrime, so international cooperation is an absolute requirement. This cooperation can be realized in the form of *Mutual Legal Assistance*/MLA (Bantuan Hukum Timbal Balik), extradition agreement, as well as Indonesia's involvement in *United Nations Convention Against Transnational Organized Crime* (UNTOC).

In terms of law enforcement on transnational cybercrime in Indonesia, it can cover two main areas, namely national legal instruments and international cooperation. From the domestic side, a number of regulations have been drafted to respond to the complexity of cybercrime. One of the main regulations is UU Nomor 11 Tahun 2008 on Information and Electronic Transactions (UU ITE) which has now been revised twice, most recently through UU Nomor 1 Tahun 2024. The legislation is the central legal framework used to handle cybercrime in Indonesia because it specifically regulates various acts that are classified as crimes in the digital space.

Provisions regarding cybercrime are substantively regulated in Pasal 27 hingga Pasal 36 UU ITE, which includes acts such as the distribution of content that violates morality, defamation and harassment, hoaxes, hacking, illegal wiretapping, and manipulation and destruction of electronic systems. The sanctions for these acts are detailed in Pasal 45 sampai dengan Pasal 52, with a range of sentences ranging from 2 years to 12 years in prison, as well as fines that can reach tens of billions of rupiah, depending on the type of crime and the impact caused. These provisions are then used as a basis by law enforcement officers in taking action against cybercriminals (UU No 1 tahun 2024 UU ITE). Based on provisions Pasal 2 UU ITE, The legal provisions in this law apply to anyone who commits a crime as regulated therein, whether the perpetrator is within or outside the jurisdiction of Indonesia, as long as the act causes harm to the interests of Indonesia.

In addition UU ITE, Kitab Undang-Undang Hukum Pidana (KUHP) also remains a general reference that can be used in the context of cybercrime, especially against conventional criminal acts committed through electronic media. For example, Pasal 378 KUHP about fraud can be implemented against online fraudsters who use trickery to gain illegal profits. Likewise, Pasal 362 KUHP regarding theft can be imposed on perpetrators who illegally take digital data or information that has economic value. In an effort to complement the normative aspect, Indonesia has also regulated the administrative aspects and responsibilities of electronic system organizers through Peraturan Pemerintah Nomor 71 Tahun 2019 on the Implementation of Electronic Systems and Transactions (PP PSTE). The regulation emphasizes the implementation of electronic security and systems with integrity and reliability, as well as the obligation of system providers to implement reliable information security standards.

Specifically, Pasal 20 Peraturan Pemerintah Nomor 71 Tahun 2019 explains that the electronic system organizer is required to implement a reliable and secure system and can be accounted for in its operational system. If this obligation is ignored and causes losses, the organizer can be held accountable in the legal context, both civil and criminal. Several institutions have also been formed, such as the Directorate of Cyber Crime (Dittipidsiber) of the Criminal Investigation Unit of the Indonesian National Police which is primarily responsible for carrying out the investigation and inquiry process for various special crimes related to cybercrime. This includes violations in the field of information and electronic transactions, as well as crimes in the telecommunications sector, including transnational cybercrime.

In carrying out these duties, Dittipidsiber also carries out strategic functions, namely conducting investigations and inquiries into cybercrime, including transnational crimes, and formulating policies related to the implementation of these tasks in the context of law

enforcement in the cyber realm. Then Badan Siber dan Sandi Negara (BSSN) has been formed, but still faces challenges in terms of coordination, technical capacity, and human resources. Efforts to update laws and adjust policies based on international best practices are important steps that must continue to be developed. In addition, Kominfo, The National Crypto Agency, and even financial authorities are involved in handling and supervising cross-sectoral cyber aspects. At the international level, Indonesia has ratified UU No. 1 Tahun 2006 about *Mutual Legal Assistance*/MLA) and Undang Undang No. 5 Tahun 2009 about Approval *United Nations Convention Against Transnational Organized Crime* or the UN Convention to combat transnational criminal acts, one of the substances of which is related to extradition agreements with friendly countries.

2. Obstacles in Law Enforcement

One of the major issues in enforcing the law on transnational cybercrime is the issue of jurisdiction. Jurisdiction in cybercrime faces major challenges due to its cross-border nature, which often involves perpetrators, victims, and evidence spread across multiple countries (Hapsoro et al., 2022). The study also noted that gaps in different legal and regulatory mechanisms in each country would be an obstacle to effective international cooperation (Tobing et al., 2024).

In addition to jurisdictional issues, the evidentiary aspect of cybercrime is also a serious challenge. Unlike conventional crimes that often leave physical traces, cybercrime relies on digital evidence that is temporary and easily changed. Log files, metadata, and traces of online activity must be immediately secured by competent authorities so that they can be used as legally valid evidence. However, technological limitations, lack of digital forensic experts, and slow reporting processes from the public often make digital evidence invalid in court. Indonesia, as a developing country with a high level of digital adoption, also faces this complexity. The case of a cross-border online fraud syndicate led by a Chinese citizen with the initials ZS highlights several significant challenges. One of the main obstacles is the limited legal jurisdiction. This crime was committed from abroad, specifically Dubai. Meanwhile, the victims are spread across several countries including Indonesia. ZS was only successfully secured after entering Indonesian territory in June 2024 (Chaterine & Ihsanuddin, 2024). In this context, Indonesian law enforcement does not have the authority to conduct investigations or arrests directly in other countries. Cross-border legal processes also require cooperation through Mutual Legal Assistance (MLA) procedures that are often slow and full of administrative challenges.

In addition, the complexity of international coordination and cooperation is another major challenge. Handling this case involves many countries, each with different legal systems, policies, and national interests. This often hampers the law enforcement process because not all countries have extradition agreements or adequate bilateral cooperation in the field of cybercrime (Ginanjar, 2022). Furthermore, the modus operandi of this syndicate is also very sophisticated and difficult to detect. They utilize popular applications such as WhatsApp and Telegram, and recruit workers under the guise of legitimate job vacancies. The use of encryption technology and servers located abroad makes it increasingly difficult to track the digital footprints of the perpetrators. Fraud modes based on psychological manipulation of victims or social engineering also continue to develop, making them increasingly difficult to prevent (Farhan et al., 2023).

The next challenge lies in the capacity of cyber law enforcement in Indonesia. Although law enforcement officers have succeeded in uncovering this case, there are still limitations in the number and competence of human resources with digital forensic expertise. In addition, the cyber law enforcement technology infrastructure in Indonesia is still not fully optimal, both in

terms of software, support systems, and budget. All of these problems show that combating transnational cybercrime is not just a matter of technology, but also includes legal, social, diplomatic, and humanitarian aspects that are interrelated and require cross-sectoral solutionsTobing, Surya, And Selvias, "Globalisasi Digital Dan Cybercrime : Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas.".

In order to answer these challenges, it is necessary to prioritize preventive and repressive steps simultaneously and in an integrated manner. From the preventive side, increasing digital literacy in society is the main step. Public socialization and education regarding digital security must be carried out massively to equip the public with basic skills in recognizing and avoiding cyber threats (Judijanto & Nugroho, 2025).

In addition, national regulations must be aligned with international legal standards. This legal harmonization is important to prevent jurisdictional conflicts and provide legal certainty in cross-border cooperation. Another preventive measure that needs to be strengthened is the implementation of proactive cyber patrols by law enforcement officers, especially the National Police's Cyber Crime Directorate, to detect suspicious online activities that have the potential to violate the law early.

From the repressive side, increasing the capacity of human resources for law enforcement in the field of digital forensics and cyber law is very urgent. They must have the technical ability to identify, collect, and analyze digital evidence legally and accurately. In addition, strengthening international cooperation, both in bilateral and multilateral contexts, needs to be intensified. This cooperation can take the form of exchanging intelligence data, joint training, and accelerating the mutual legal assistance process through the Mutual Legal Assistance (MLA) scheme. This strategy is expected to accelerate the extradition process, tracking digital assets, and providing evidence in court, so that transnational cybercriminals can no longer hide behind national jurisdictional boundaries. With a combination of adaptive and coordinated preventive and repressive strategies, Indonesia will be better prepared to face the challenges of increasingly complex, sophisticated and globally widespread transnational cybercrime.

Conclusion

Law enforcement against transnational cybercrime in Indonesia is a complex challenge that includes legal, technological, and international cooperation aspects. Cybercrime has unique characteristics that distinguish it from conventional crimes, such as the anonymity of the perpetrator, the difficulty of obtaining digital evidence, and overlapping jurisdictions between countries. In responding to this threat, Indonesia has formed various national legal instruments, such as Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) along with its implementing regulations, as well as strengthening institutions through the formation of Direktorat Tindak Pidana Siber Bareskrim Polri dan Badan Siber dan Sandi Negara (BSSN). The presence of these regulations and institutions is an important pillar in eradicating and enforcing cyber law violations.

However, the effectiveness of law enforcement still faces various obstacles, especially in terms of cross-border jurisdiction, limited technology and expertise, and suboptimal international coordination. Case studies of cross-border online fraud involving international perpetrators show that the legal process becomes complicated when the perpetrators are outside Indonesia's jurisdiction. This situation makes it clear that combating cross-border cybercrime cannot rely solely on a legal-formal approach, but must be complemented by collaborative, adaptive strategies that are oriented towards strengthening bilateral relations between countries.

Suggestion

There are several strategic steps that can be taken. First, it is necessary to build a structured and massive digital literacy system in society as a preventive measure against the

potential of becoming a victim of cybercrime. Second, national regulations must be aligned more systematically with international legal standards and instruments in order to strengthen Indonesia's position in global cooperation. Third, improving human resources for law enforcement, especially those who have expertise in digital forensics and cyber law. Fourth, bilateral and multilateral cooperation needs to be expanded and optimized, especially in the form of intelligence information exchange, mutual legal assistance, and joint training between countries. These steps are key in dealing with the dynamics of cybercrime that are increasingly complex, sophisticated, and transnational.

REFERENCES

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *05*(02), 55–63. https://doi.org/10.54209/judge.v5i02.566

Bego, K. C., Aziz, F. R., Rahmad, R. A., & Sunarto, H. B. (2025). Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya (Desember 2024). *Jurnal Kolaboratif Sains*, *8*(1), 506–511. https://doi.org/10.56338/jks.v8i1.6740

Chaterine, R. N., & Ihsanuddin. (2024). *Bareskrim Usut WNA Lain Dalam Kasus Penipuan Online Modus Lowongan Kerja*. Kompas.Com. https://nasional.kompas.com/read/2024/07/19/17382501/bareskrim-usut-wna-lain-daalm-kasus-penipuan-online-modus-lowongan-kerja.

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Farhan, M., Syaefunaldi, R., Hidayat, D. R. D., & Hosnah, A. U. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. *Kultura: Jurnal Hukum, Sosial, Dan Humaniora*, *1*(6), 8–20.

Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara. *Jurnal Dinamika Global*, *7*(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Hapsoro, W., Aidjili, M., & Budijanto, H. A. (2022). Yurisdiksi Hukum Pidana Dalam Pembatasan Informasi Hoaks Terkait Dengan Kejahatan Cybercrime. *RISTEK : Jurnal Riset, Inovasi Dan Teknologi Kabupaten Batang*, *7*(1), 11–19. https://doi.org/10.55686/ristek.v7i1.124

Hiariej, E. O. S. (2024). *Prinsip-Prinsip Hukum Pidana Edisi Penyesuaian KUHP Nasional*. PT. Rajagrafindo Persada.

Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum Dan HAM*, *3*(3), 118–124. https://doi.org/10.58812/shh.v3.i03

Khoirunnisa, K., & Jubaidi, D. (2024). Indonesia's Digital Security Strategy: Countering the Threats of Cybercrime and Cyberterrorism. *Politeia : Journal of Public Administration and Political Science and International Relations*, *2*(2), 62–82. https://doi.org/10.61978/politeia.v2i2.211

Kitab Undang-Undang Hukum Pidana (KUHP).

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. In *Sustainability (Switzerland)* (Vol. 15, Issue 18). https://doi.org/10.3390/su151813369.

Soekanto, S., & Mamudji, S. (2012). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. PT Raja Grafindo Persada.

Tobing, C. I., Surya, T. M., & Selvias, L. R. (2024). Globalisasi Digital Dan Cybercrime : Tantangan Hukum Dalam Menghadapi Kejahatan Siber Lintas Batas. *JURNAL HUKUM SASANA*, *10*(2), 105–123. https://doi.org/10.31599/sasana.v10i2.3170

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 1 Tahun 2006 tentang Bantuan Timbal Balik dalam Masalah Pidana.

Undang-Undang Nomor 5 Tahun 2009 tentang Pengesahan United Nations Convention Against Transnational Organized Crime.