International Journal of Sociology and Law

E-ISSN: 3047-0692
P-ISSN: 3047-1923

Research Article

Criminal Law Policy in Dealing With The Development of Transnational Cyber Crime

Saptha Nugraha Isa [1*], Rahmayanti [2], Paulus Purba [3], Krismanto Manurung [4]

[1] Program Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, email: saptha.tebingtinggi@gmail.com
[2] Program Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, email: rahmayanti@dosen.pancabudi.ac.id
[3] Program Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, email: Pauluspurba713@gmail.com
[4] Program Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, email: krismantomanru@gmail.com

* Corresponding Author : Saptha Nugraha Isa

Abstract: This abstract analyzes the urgency of criminal law policy in tackling the rapidly evolving transnational cybercrime. The rapid advancement of information and communication technology has created increasingly complex, cross-border, and difficult-to-detect cybercrime modus operandi. Indonesia, as part of the global community, faces serious challenges in formulating and implementing effective regulations to combat these crimes. This research aims to identify the challenges of criminal law in Indonesia in dealing with transnational cybercrime and to formulate adaptive strategies to strengthen the existing legal framework. Normative-empirical research methods are employed with a case study approach, legislative analysis, and international legal comparison. The findings indicate that the harmonization of national laws with international standards, enhancement of law enforcement capacity, and strengthening of inter-state cooperation are key. Innovation in criminal law approaches is also needed, focusing not only on prosecution but also on prevention and recovery of losses. The conclusion of this study emphasizes the necessity of comprehensive reform in criminal law policy, encompassing substantive, procedural, and institutional aspects, to create a system responsive to the dynamics of transnational cybercrime.

Keywords: Criminal Law, Cybercrime, Transnational, Legal Policy, International Cooperation.

Received: 19 May, 2025
Revised: 02 June, 2025
Accepted: 16 June, 2025
Published: 18 June , 2025
Curr. Ver.: 18 June, 2025

1. Introduction

The development of information and communication technology (ICT) has brought fundamental changes in various aspects of human life, from economics, social, culture, to politics. Such rapid digital transformation has opened the door to innovation and convenience, but on the other hand has also given birth to new threats in the form of cybercrime. This crime is no longer limited to the local scope, but has evolved into a transnational phenomenon that transcends the boundaries of state jurisdiction. Transnational cybercrime is a crucial issue that requires serious attention from every country, including Indonesia, considering its massive impact and the losses it causes.

The high level of global connectivity made possible by the internet has enabled cybercriminals to operate from anywhere in the world, targeting victims in any country. The modus operandi of these crimes is very diverse, ranging from online fraud, system hacking, spreading malware and ransomware, stealing personal data, to financial crimes and cyber terrorism. The anonymous, fast and cross-border characteristics of cybercrime pose a major challenge for traditional law enforcement, which tends to be tied to the principle of territoriality.

Indonesia, with its rapidly growing number of internet users, is a potential target for cybercriminals. Data shows a significant increase in the number of cyber attacks targeting

government institutions, private companies, and individuals in Indonesia. Financial losses caused by cybercrime are also increasing, not including non-financial impacts such as loss of public trust, reputational damage, and threats to national security.

Although Indonesia already has several relevant regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as amended by Law Number 19 of 2016, as well as regulations related to personal data protection, the existing criminal law framework still faces a number of challenges. These challenges include the suboptimal harmonization of national regulations with international standards, limited capacity of law enforcement in handling sophisticated cybercrime, and minimal effective cross-border cooperation in prosecuting and extraditing perpetrators .

The gap between the dynamic development of transnational cybercrime and the relatively slow adaptation of criminal law policies is a fundamental problem. The legislative process, which is often not as fast as the pace of technological innovation, and the complexity of proving cyber cases that require special expertise, also worsen the condition. Therefore, a comprehensive review of existing criminal law policies is needed, as well as the formulation of adaptive strategies to face this challenge.

It is important to understand that transnational cybercrime is not just a technical problem, but also a complex legal and social issue. Handling cannot only rely on a technical approach, but must also involve a strong and responsive legal approach. Criminal law policy must be able to provide a clear legal framework, firm sanctions, and effective law enforcement mechanisms for deterrence and prosecution.

In addition, international cooperation is a key pillar in combating transnational cybercrime. This crime knows no borders, so handling it must involve coordination and collaboration between countries. Indonesia's active participation in international conventions such as the Budapest Convention on Cybercrime, as well as the implementation of extradition and mutual assistance agreements in criminal matters, is crucial.

Thus, the urgency of this research lies in the effort to analyze in depth how criminal law policies in Indonesia can be optimized to face the challenges of transnational cybercrime. This research is expected to provide theoretical and practical contributions in formulating more effective, adaptive, and sustainable policy recommendations in maintaining a safe cyberspace for all citizens.

2. Formulation Of The Problem

Based on the background that has been described, the formulation of the problem in this study is as follows:

- What are the challenges of criminal law in Indonesia in responding to and overcoming the development of transnational cybercrime, especially related to jurisdiction, evidence, and regulatory harmonization?
- How can an adaptive and comprehensive criminal law policy model be formulated to increase the effectiveness of law enforcement against transnational cybercrime in Indonesia, including through international cooperation ?

3. Research Methods

This study uses a normative-empirical legal research method (socio-legal research). The normative approach is carried out to analyze relevant laws and regulations, legal doctrines, and international conventions related to cybercrime and international criminal cooperation . The empirical approach is used to collect data and information on the implementation of criminal law policies in the field, including the obstacles faced by law enforcement.

The types of data used include:

- Primary data: Obtained through interviews with competent sources, such as law enforcers (Police, Prosecutors), cyber law experts, academics, and information technology practitioners involved in handling cybercrime. This data aims to obtain information on law enforcement practices, operational challenges, and perspectives on existing policies.
- Secondary data: Obtained from primary legal materials (Laws, Government Regulations, Court Decisions), secondary legal materials (books, scientific journals, research results, reports, articles), and tertiary legal materials (legal dictionaries, encyclopedias). Secondary data also includes statistical data on cybercrime cases and technological developments.

The data collection techniques used are:

- Library research: Conducted to collect secondary data by searching literature, laws and regulations, and related documents.
- Interviews: Conducted in a structured or unstructured manner with predetermined sources to obtain primary data.
- Case study: Analyzing several cases of transnational cybercrime that have occurred in Indonesia to identify patterns, evidentiary challenges, and legal responses given.

The data analysis technique used is qualitative analysis. The collected data will be analyzed descriptively-analystically by identifying patterns, trends, and relationships between variables. This analysis also involves legal interpretation and comparison between theory and practice, as well as between national regulations and international standards. The discussion will be carried out systematically to answer the formulation of the problems that have been set.

4. Discussion

4.1. Criminal Law Challenges in Dealing with Transnational Cybercrime in Indonesia

Criminal law policy in Indonesia faces various significant challenges in responding to the dynamics of transnational cybercrime. These challenges are not only technical in nature, but also involve aspects of jurisdiction, evidence and regulatory harmonization.

- Jurisdiction Issues

  One of the biggest challenges is determining jurisdiction. Transnational cybercrime often involves perpetrators located in one country, victims in another country, and servers or data stored in a third country. Indonesian criminal law generally adheres to the principle of territoriality, where a country's laws apply to crimes committed within its territory.

  However, the borderless nature of cybercrime makes determining the location of the crime ambiguous. For example, did the crime occur where the perpetrator carried out the attack, where the victim suffered the loss, or where the data was processed? These limitations make it difficult for Indonesian law enforcement to prosecute perpetrators who are abroad, unless there is an extradition treaty or effective mutual legal assistance. Article 5 of the ITE Law does expand jurisdiction through the principles of passive nationality and universality, but its implementation still faces bureaucratic obstacles and the sovereignty of other countries.
- Complexity of Proof

  Proof in transnational cybercrime cases is very complex. Digital evidence (electronic evidence) is vulnerable, easily altered, and can be spread across jurisdictions. Law enforcement must face challenges in obtaining, securing, analyzing, and presenting valid digital evidence in court.

  The absence of uniform, internationally recognized digital forensics standards, as well as differences in criminal procedure rules between countries, exacerbate this problem. In addition, the speed of erasing digital traces by perpetrators is also an obstacle. Reliance on foreign service providers to obtain traffic data or activity logs is also often hampered by differences in data protection laws and information sovereignty between countries.
- Regulatory Harmonization and Legal Gaps

  Indonesia already has the ITE Law and several other related regulations. However, there are still legal gaps and a lack of harmonization of regulations with international standards such as the Budapest Convention on Cybercrime. This convention provides a comprehensive legal framework for combating cybercrime, including provisions on jurisdiction, investigation, evidence and international cooperation .

  Although Indonesia is not a party to the Budapest Convention, its principles are often used as a global reference. The lack of adaptation to these international standards causes difficulties in cross-border cooperation , especially in terms of data requests, asset tracking, or extradition. In addition, existing regulations are often lagging behind technological developments and the ever-evolving modus operandi of crimes.
- Law Enforcement Capacity

  The capacity of law enforcement in Indonesia, both in terms of human resources and infrastructure, still needs to be improved. Handling cybercrime requires specialized expertise in digital forensics, cyber analysis, and a deep understanding of information technology. Continuous training, procurement of sophisticated equipment, and increased

coordination between law enforcement agencies are crucial. Budget and resource constraints are often barriers to developing this capacity.

4.2 Adaptive and Comprehensive Criminal Law Policy Model

To face the challenges of transnational cybercrime, Indonesia needs to formulate an adaptive and comprehensive criminal law policy model. This model must include aspects of legislation, law enforcement, and international cooperation .

- Legislative Reform
  The government needs to consider comprehensive legislative reform. This includes:
  - Harmonization of the ITE Law with international standards: Reviewing and adapting provisions in the ITE Law and other related regulations to align with the principles of the Budapest Convention or other international legal instruments. This includes expanding the definition of cybercrime, clearer jurisdictional arrangements, and strengthening provisions on electronic evidence.
  - Strengthening procedural aspects: Updating the Criminal Procedure Code (KUHAP) to accommodate the special characteristics of digital evidence and cyber investigation processes, including mechanisms for more effective cross-border preservation orders and production orders.
  - Comprehensive personal data protection: The new Personal Data Protection Law (PDP Law) is a step forward, but its implementation and harmonization with other sectoral regulations must be further strengthened to prevent misuse of data, which is a major target of cybercrime.
- Law Enforcement Capacity Building
  Increasing the capacity of law enforcement is key. Strategies that can be implemented include:
  - Specialized skills development: Train and develop law enforcement personnel who specialize in cyber forensics, cyber intelligence, and cybercrime investigations.
  - Technology investment: Allocate sufficient budget for the procurement of state-of-the-art digital forensics equipment and software.
  - Establishment of special units: Strengthen or establish special units within the Police and Prosecutor's Office that focus on handling transnational cybercrime, equipped with adequate resources.
  - cooperation : Encourage cooperation between law enforcement, cyber experts, academics, and the private sector to share knowledge and experience in handling cybercrime.
- Strengthening International Cooperation
  International cooperation is a fundamental aspect. Indonesia must:
  - Increase participation in international forums: Actively participate in regional and global forums that discuss cybercrime, such as the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), INTERPOL, and the United Nations Office on Drugs and Crime (UNODC).
  - Enhance bilateral and multilateral cooperation : Establish more mutual legal assistance treaties in criminal matters (MLATs) and extradition agreements with other countries. This will facilitate the exchange of information, evidence, and the surrender of perpetrators.
  - Consideration of accession to the Budapest Convention: Although not a requirement, considering accession to the Budapest Convention could provide a clear and globally recognized legal framework for international cooperation in combating cybercrime.

4.3 Examples of Transnational Cybercrime Cases and Legal Responses

To illustrate the challenges and need for adaptive policies, let us look at some relevant examples of transnational cybercrime cases:

- WannaCry Ransomware Case (2017)
  Case in point: The WannaCry ransomware attack in 2017 spread globally, encrypting data on thousands of computers in more than 150 countries, including Indonesia. The perpetrators demanded a ransom in bitcoin to decrypt the data. These attacks

targeted a variety of institutions, including hospitals, companies, and government agencies. Although there are strong indications that these attacks originated from a North Korean-affiliated group, determining the perpetrators and prosecuting them is extremely difficult due to the transnational nature and anonymity of the perpetrators. Many countries have difficulty in bitcoin tracking and cross-border coordination.

Legal Response and Challenges: In Indonesia, the incident prompted an emergency response from the government and cybersecurity sector, with a focus on technical mitigation and prevention. However, from a criminal law perspective, directly prosecuting the main perpetrators is very difficult because they are outside of Indonesia's jurisdiction and there is no direct extradition mechanism applicable to this case. Key challenges include overlapping jurisdictions, the difficulty of tracking blockchain in real time, and the lack of mutual legal assistance treaties specific to transnational ransomware cases. The case highlights the need for greater cross-border digital forensics cooperation and faster exchange of cyber intelligence.

- Cross-border Online Fraud Cases (Love Scam/Romance Scam)

  Case Study: Many online fraud cases in Indonesia involve transnational networks. For example, love scams or romance scams, where perpetrators, often from African or Eastern European countries, establish romantic relationships with victims in Indonesia through social media. Once the victim believes them, the perpetrators will ask for money under various pretexts (e.g., travel expenses, hospital bills, or customs fees for packages). The money is then transferred through a bank account or international payment platform.

  Legal Response and Challenges: Indonesian law enforcement is often successful in catching perpetrators who are in Indonesia or who have entered Indonesia. However, challenges arise when money has been transferred abroad, or when the masterminds of the crime are in another country. The process of freezing assets and repatriating funds from abroad is complex and time-consuming, often hampered by differences in legal systems and the absence of effective mutual legal assistance treaties. Proving criminal intent and identifying principal perpetrators who are abroad are major challenges. Cases such as these highlight the importance of international police cooperation (through INTERPOL) and coordination between cybercrime units in different countries.
- Cross-Border Data Breach Case (Global Platform User Data Theft)

  Case Example: A global e-commerce company or social media platform operating in Indonesia experienced a massive user data leak. The personal data of millions of users, including Indonesian citizens, was stolen and sold on the dark web. The perpetrators could be a group of hackers from another country who have no physical connection to Indonesia.

  Legal Response and Challenges: While Indonesian citizens' personal data is affected, prosecution of perpetrators is often hampered by jurisdiction. The company experiencing the data breach may be based in another country , and the perpetrator may be in another country. Indonesia, with its new PDP Law, has the legal basis to sue companies for negligence in protecting data, but prosecuting cybercriminals based abroad remains a major challenge. Strong coordination between data protection authorities and law enforcement across borders is needed to track perpetrators, freeze assets, and ensure the exchange of valid digital evidence. This case demonstrates the need for clear regulations on cross-border data breach reporting obligations and global accountability mechanisms.

5. Conclusions

Criminal law policy in Indonesia faces significant challenges in combating transnational cybercrime, particularly related to overlapping jurisdictional issues, the complexity of proving electronic evidence spread across borders, and the limited harmonization of national regulations with international legal standards. In addition, the capacity of law enforcement in Indonesia also still requires significant improvement to be able to effectively tackle the increasingly sophisticated and dynamic modus operandi of cybercrime.

To improve the effectiveness of law enforcement against transnational cybercrime, Indonesia needs to formulate and implement an adaptive and comprehensive criminal law policy model. This model should include legislative reform through harmonization of the ITE Law with international principles, increasing the capacity of law enforcement through training and technology investment, and strengthening international cooperation through increased

participation in global forums and the establishment of broader mutual legal assistance agreements. This approach will enable Indonesia to be more responsive and proactive in dealing with the threat of transnational cybercrime.

References

[1]Ahmad, F. (2018). Cyber Criminal Law: A Comparative Review. Jakarta: Rajawali Pers.
[2]Andayani, A. (2019). "Challenges of Law Enforcement Against Cybercrime in Indonesia". Ius Quia Iustum Law Journal, 26(1), 1-18.
[3]Asmadi, EA (2020). Cybercrime: Theory and Practice of Law Enforcement. Yogyakarta: Thafa Media.
[4]National Cyber and Crypto Agency (BSSN). (2023). Indonesian Cyber Security Annual Report 2022. Jakarta: BSSN. (For example, you can search for the latest relevant report)
[5]Brown, I., & Korff, D. (2018). The EU Data Protection Regulation and Cybercrime. London: Springer.
[6]Casey, E. (2019). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. San Diego: Academic Press.
[7]Dahlan, M. (2017). "Legal Aspects of Proving Cyber Crime". Jurnal Mimbar Hukum, 29(1), 12-25.
[8]European Union Agency for Cybersecurity (ENISA). (2021). ENISA Threat Landscape 2021. Greece: ENISA. (For example, you can search for the latest relevant reports)
[9]Ghani, A. (2019). Cybercrime and International Law: A Comparative Study. New York: Routledge.
[10]International Telecommunication Union (ITU). (2023). Global Cybersecurity Index 2020. Geneva: ITU. (For example, you can search for the latest relevant report)
[11]European Commission. (2001). Convention on Cybercrime (Budapest Convention). CETS No. 185. Strasbourg: Council of Europe.
[12]Lesmana, A. (2021). "The Role of International Cooperation in Eradicating Transnational Cybercrime". Journal of Legal Studies, 10(2), 201-215.
[13]Moeljatno. (2008). Principles of Criminal Law. Jakarta: Rineka Cipta.
[14]Negara, SW (2022). Cyber Law and Challenges in the Digital Era. Jakarta: Sinar Grafika.
[15]Rachmad, Z. (2020). "The Urgency of Harmonizing National Legislation with the Budapest Convention in Handling Cybercrime". Journal of Law and Development, 50(3), 578-592.
[16]Setyawan, H. (2018). Information Technology Crimes. Bandung: Citra Aditya Bakti.
[17]United Nations Office on Drugs and Crime (UNODC). (2022). Global Study on Cybercrime 2022. Vienna: UNODC. (For example, you can search for the latest relevant report)
[18]Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016.
[19]Law Number 27 of 2022 concerning Personal Data Protection.
[20]Wasiati, N. (2021). "Legal Analysis of Jurisdictional Challenges in Handling Cross-Border Cybercrime". Journal of Criminal Law and Criminology, 5(1), 45-60.