

LAW ENFORCEMENT AGAINST CYBER CRIME IN ELECTRONIC TRANSACTIONS IN INDONESIA

Tegar Harbriyana Putra¹, Sunny Ummul Firdaus²

¹Faculty of Law, Boyolali University

²Faculty of Law, Sebelas Maret University Surakarta

Email : tegarharbriyanaputra@gmail.com, firdaussunny@yahoo.com

ABSTRACT

Law enforcement against cyber crime in electronic transactions in Indonesia is an increasingly crucial issue in the current digital era. The increasing use of information and communication technology has driven the growth of the digital economy, but has also given rise to various threats, including cyber crime. This article examines the law enforcement efforts carried out by the Indonesian government to overcome cyber crimes related to electronic transactions. This study analyzes existing regulations, including the Information and Electronic Transactions Law (UU ITE), as well as the role of law enforcement agencies in tackling cyber crime. Apart from that, this research also identifies challenges faced in the law enforcement process, such as limited resources, lack of coordination between agencies, and gaps in technological understanding among law enforcement officers. The research results show that although there has been significant progress in the legal and policy framework related to cyber crime, there are still many obstacles that reduce the effectiveness of law enforcement. Therefore, continuous efforts are needed to strengthen the capacity of law enforcement institutions, increase international cooperation, and update regulations so that they are in line with technological developments. Thus, it is hoped that law enforcement against cyber crime in electronic transactions in Indonesia can be more optimal in protecting the public and maintaining the integrity of the digital economy.

Keywords: cyber crime, electronic transactions, law enforcement, ITE Law.

INTRODUCTION

Information and communication technology has changed the behavior of society and human civilization globally. In addition, the development of information technology has caused the world to become borderless and caused significant social changes to take place so quickly. Information technology is currently a double-edged sword, because in addition to contributing to the improvement of welfare, progress and human civilization, it is also an effective means of unlawful acts.

Information technology as part of the Information, Communication and Technology sector (hereinafter referred to as ICT), where ICT is the entire technology that is interrelated with the retrieval, processing, acquisition, presentation and storage of information. Article 28C of the 1945 Constitution of the Republic of Indonesia is the basic foundation that philosophically underlies the development of technology in Indonesia. The full nomenclature of Article 28C paragraph (1) of the 1945 Constitution reads:

“Everyone has the right to develop themselves through the fulfillment of their basic needs, have the right to education and benefit from science and technology, arts and culture, in order to improve the quality of their lives and for the welfare of mankind.”

The regulation of information technology implemented by a country applies to everyone who performs his actions both within the territory of the country and outside the country if the action has consequences in Indonesia. Goodhue and Thompson Task-Technology Fit Theory (also known as TTF) which emphasizes the construction of the fit of a task with technology, where there must be a match between technological capabilities and existing job demands.

Society is building a new culture in cyberspace known as Cyberspace. Cyberspace creates a new form of crime, as a form of crime caused by the development and advancement of information and telecommunications technology, namely crimes related to internet applications, which in foreign terms are called cyber crimes. One of the most troubling cybercrime issues that has received attention from both the national and international community is Cyber Terrorism. Cyber Terrorism in the field of cybercrime is often interpreted as an act of terrorism crime that uses electronic technology and information, with the aim of paralyzing national infrastructure, such as energy, transportation, to suppress/intimidate government activities or civil society.

Cybercrime is a term that covers all the ways in which computers and other types of portable electronic devices such as cell phones and PDAs capable of connecting to the internet are used to break the law and cause damage. Cyber Law is a legal aspect whose term is derived from cyberspace law whose scope covers every aspect related to individuals or legal subjects who use and utilize internet technology starting at the time of going online and entering cyber space or cyberspace.

The term cyber law comes from cyberlaw, which is currently internationally used for legal terms related to the utilization of Information Technology. Other terms also used are Law of Information Technology, Virtual World Law and Mayantara Law. Other terminologies for the same purpose include The Law of the Internet, Law and the Information Superhighway, Information Technology Law, The Law of Information, Lex Informatica.

Indonesia as a state of law seeks to make regulations in handling information technology crimes, especially in the management of information and electronic transactions along with infrastructure and arrangements. Electronic Information and Transaction Law The government's policy will be strengthened by several articles contained in the new Criminal Code Bill, all done by the government to maintain the security of the State and protect its citizens from acts of terrorism crimes that are realized in real space. Cyber Law is needed because internet-based cyber activities cannot be limited by state territory and can be conducted at any time. Although the evidence is virtual and electronic, cyber activities are virtual activities that have real impact.

METHODS

This research uses a normative juridical approach, qualitative research with descriptive methods. This approach aims to describe, explain, and describe in detail the problems to be studied. The descriptive analytical research used will attempt to provide a description or description of the object of study systematically by looking at the causal relationship between the variables, both the independent and dependent variables.

RESULTS AND DISCUSSION

1. Concept of Cyber Crime Law Enforcement in Electronic Transactions

The development of information technology has had a significant impact on various aspects of life, including in the fields of economics and trade. One form of transformation that is striking is electronic transactions that make it easier for consumers and business actors to

carry out various types of transactions. In the 1980s, especially countries in Europe and North America began to criminalize new acts along with the use of computer technology in committing conventional criminal acts. In the 1990s, several countries in various parts of the world began to regulate cyber crimes such as entering computer systems illegally, damaging data in computer systems and spreading viruses. Cyber criminals have the ability and opportunity to commit criminal offenses from a country that will cause harm to someone in several places in other countries.

Abdulkadir Muhammad argues that “law enforcement can be formulated as an effort to implement the law as it should, supervise its implementation so that no violations occur, and if a violation occurs, restore the violated law so that it is enforced again”. Law enforcement is closely related to obedience for users and implementers of laws and regulations, in this case both the community and state administrators, namely law enforcement “.

Law enforcement against cyber crime, especially those related to electronic transactions, is a challenge in itself. In Indonesia, this law enforcement is regulated through several regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) which has been amended by Law Number 19 of 2016. This paper aims to discuss in more depth the law enforcement of cybercrime in electronic transactions, the challenges faced, and the solutions that can be taken to improve the effectiveness of law enforcement.

The definition of cyber crime refers to criminal acts that use computer technology as a tool, target, or place of crime. In the context of electronic transactions, cyber crime can occur in various forms, such as:

1. Hacking of banking or e-commerce systems.
2. Phishing that tricks users into providing sensitive information.
3. Identity theft for use in illegal transactions.
4. Carding or credit card fraud.
5. Ransomware or attacks that demand ransom in the context of businesses or individuals.

Law enforcement regulations in Indonesia used to deal with cybercrime in electronic transactions in Indonesia are governed by several important regulations:

1. Law No. 11/2008 on Electronic Information and Transactions (UU ITE), which is the main regulation in handling cases related to cybercrime.
2. Law Number 19 Year 2016 on the Amendment of ITE Law, which provides strengthening of law enforcement in the scope of cyber crime.
3. CRIMINAL CODE.
4. Duties and Functions of Law Enforcement Institutions Institutions such as the Indonesian National Police (Polri), the National Cyber and Crypto Agency (BSSN), and the Financial Services Authority (OJK) have an important role in law enforcement efforts against cyber crime cases. Cooperation between law enforcement agencies and financial institutions and technology companies is needed to tackle this crime.

In the context of Indonesian law, this enforcement is based on Law Number 11/2008 on Electronic Information and Transactions (UU ITE), which was later strengthened by Law Number 19/2016. This regulation is the main foundation in protecting electronic transactions from crimes such as hacking, identity theft, and online fraud. The global nature of cybercrime demands cross-border cooperation, so national regulations need to be integrated with international legal frameworks, such as the Budapest Convention on Cybercrime (2001). This convention provides guidance on electronic evidence collection, crime prevention, and international collaboration in law enforcement.

The concept of Cyber Crime Law Enforcement in Electronic Transactions covers several important aspects involving legal action against crimes that occur through or are related to electronic transactions. Cyber crime in this context refers to illegal acts committed by utilizing digital or internet technology, such as identity theft, online fraud, hacking, or misuse of personal data.

It can be concluded that several concepts can be used in law enforcement related to cyber crime in electronic transactions, among others, related to several things that need more attention from the government in order to handle cyber crime, especially in Indonesia:

1. Applicable Legal Framework

In Indonesia, law enforcement of cybercrime in electronic transactions is regulated under Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which was later updated with Law No. 19 of 2016. Some other relevant provisions include the Criminal Code (KUHP) for general criminal offenses as well as personal data protection regulations.

2. Types of Cyber Crime in Electronic Transactions

- a. Phishing and Online Fraud: The use of psychological manipulation techniques to steal a victim's personal or financial information through digital platforms.
- b. Identity Theft: The misuse of an individual's identity to conduct illegal transactions.
- c. Hacking and System Hacking: Illegal access to computer systems or networks to steal, alter or destroy data.
- d. Fraud in E-Commerce: Fraud that occurs in online buying and selling transactions, such as the use of stolen credit cards or product-related fraud.

3. Law Enforcement Process

Cyber crime law enforcement requires collaboration between several parties among law enforcement agencies, among others:

- a. Cyber Police: In Indonesia, the handling of cybercrime cases is generally carried out by the Cyber Crime Directorate unit of the National Police Criminal Investigation Unit.
- b. Law Enforcement Agencies: The involvement of prosecutors, judges, and courts in processing cybercrimes.
- c. Ministry of Communication and Information (Kominfo): Supervision of sites or platforms used for electronic transactions and enforcement of rules related to data protection.

4. Challenges in Law Enforcement

- a. Jurisdiction: Cybercrime often involves cross-border actors, making law enforcement complex in terms of jurisdictional authority.
- b. Offender Anonymity: Cybercriminals can hide their identities by using various technologies, such as VPNs or anonymous networks, which makes tracking difficult.
- c. Lack of Digital Evidence: The process of collecting electronic evidence (digital forensic) often requires specialized techniques and tools.
- d. Technology Development: Technology is evolving so fast that laws and law enforcement systems often lag behind in responding to new modes of crime.

5. Victim Protection

- a. Public Education: Increase public awareness of the risks of cybercrime through socialization of safe online transactions.
- b. Loss Recovery: Legal efforts to recover financial or non-financial losses suffered by victims through civil and criminal channels.

- c. Personal Data Protection Regulation: In some countries, personal data protection is an important focus, and Indonesia is developing a Personal Data Protection Bill to protect citizens' privacy rights.

6. International Approach

As cybercrime is often transnational in nature, it is important that there is international cooperation in law enforcement. Organizations such as Interpol and the United Nations Office on Drugs and Crime (UNODC) play a role in facilitating collaboration between countries to track and tackle global cybercrime.

With a comprehensive approach, law enforcement against cybercrime in electronic transactions aims to provide justice to victims, prevent criminal acts, and maintain public confidence in the use of technology and the internet in economic activities.

2. Concept of Law Enforcement of Cyber Crime as Transnational Crime

Cyber crime is a crime that can be considered as a new crime, because cyber crime has very specific characteristics when compared to conventional crimes. Cyber crime emerged along with the advancement of information technology. By paying attention to the types of cybercrime discussed in the previous chapter, it can be illustrated that cybercrime has specific characteristics, namely:

- a. non-violent;
- b. involves little physical contact;
- c. using equipment;
- d. utilizing global telematics (telecommunications, media, and informatics) networks.

Looking at the 3rd and 4th characteristics, it is clear that cybercrime can be done anywhere, anytime, and have an impact anywhere, like borderless. This condition results in the place where cyber crime occurs, the perpetrators, the victims, and the consequences that arise can occur in several countries, this is where the aspect of transnational cyber crime can be seen.

The ITE Law is the first cyberlaw in Indonesia that specifically regulates information and electronic transactions, after the presence of the previous telecommunications law. The material of ITE Law can be grouped into 2 (two) major parts:

1. Regulation of information and electronic transactions;
2. Regulation of prohibited acts (cybercrime).

The cybercrime provisions in the ITE Law refer to the EU Convention Cybercrime (CoC) which is an international instrument used by many countries.²⁷ The CoC regulates two types of cybercrime, namely:

1. Cybercrime in the sense of regulated computer crime is a crime aimed at the confidentiality, integrity, and availability of data and computer systems and includes this category is illegal access, illegal interception, data interference, system interference, and misuse of devices.
2. Cybercrime in the sense of computer-related crime, the scope of this is computer-related forgery and computer-related fraud.

Transnational crimes are intended to indicate the existence of crimes that are actually national (within national borders), but in some way related to the interests of other countries. Its transnational nature covers almost all national and international aspects, both private and public, political and non-political. Therefore, combating cyber crime requires serious handling and involves international cooperation, both regional and multilateral.

In criminal offenses that do not cross state borders, three types of jurisdiction are known:

1. Legislative jurisdiction (jurisdiction to prescribe), which is the power to make regulations or laws that regulate the relationship or legal status of people or legal

events within its territory. Such authority is usually exercised by the legislature so it is often referred to as legislative or prescriptive jurisdiction.

2. Judicial jurisdiction (jurisdiction to adjudicate), namely the power of the court to try people (legal subjects) who violate regulations or legislation.
3. Executive jurisdiction (jurisdiction to enforce), namely the power of the state to impose or enforce (enforce) so that legal subjects obey the law. This coercive action is carried out by the executive body of the state which is generally seen in economic fields, for example the power to refuse or give licenses, contracts, and others.

Referring to the general principle in international law, that every country has sovereignty in its territory, so that a country cannot override its sovereignty in carrying out an action within the territory of another country. The application of criminal jurisdiction of a sovereign state under international law is carried out based on several principles of jurisdiction, among others:

1. Territorial Principle, Can apply its national jurisdiction to all persons (whether citizens or foreigners), legal entities and all objects located therein. The territorial principle is the main jurisdictional principle implemented in exercising the jurisdiction of the State.
2. Active National Principle, Principle based on nationality or citizenship. In this case the nationality of the perpetrator of the crime. Here the nationality of the perpetrator becomes the link point for the application of the jurisdiction of the country of origin. Based on this principle, the State has jurisdiction over its citizens who commit criminal offenses within the jurisdiction of another State.
3. Passive National Principle, a principle based on the nationality of the victim of the crime. Based on this principle, a State has jurisdiction to prosecute perpetrators of criminal offenses abroad that harm its citizens.
4. The Principle of International Legal Protection states that a country can apply its national law to the perpetrator of a crime even though the crime was committed outside the territory of the country, where the crime committed is an act that can threaten the interests of the country concerned.
5. The Universal Principle basically does not require a relationship, so it can be concluded that a criminal law can be applied if a criminal offense committed by a person is contrary to universal values in a country and against the interests of society at large.

The application of universal jurisdiction against criminal offenders is not easy to implement, this limitation is also recognized by experts, as follows:

“Refers to jurisdiction established over a crime without reference to the place of perpetration, the nationality of the suspect or the victim or any other recognized linking point between the crime and the prosecuting State. It is a principle of jurisdiction limited to specific crimes”.

In cyber crime, a regional convention has been established that regulates the need for criminalization policy (legal policy) against cyber crime. The regional convention is the Convention on Cybercrime in 2001 produced by the Council of Europe. This convention was born with the idea of “global internet, global law” which means that global internet problems are resolved by global law (international regime).

“Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation.”

Cyber crime as a transnational criminal offense refers to cybercrime that crosses national borders, where the perpetrators, victims, and impacts of the crime are located in different jurisdictions. In this context, law enforcement faces great challenges due to differences in regulations, legal systems, and technological capabilities between countries.

Law enforcement against transnational cyber crime must refer to national and international legal frameworks. In Indonesia, regulations regarding cybercrime have been regulated in Law Number 11/2008 on Electronic Information and Transactions (ITE) and its amendment in Law Number 19/2016. However, since cybercrime often involves cross-border, international legal frameworks such as the Budapest Convention on Cybercrime become an important reference for cooperation between countries in handling these cases.

Some important elements in law enforcement of cybercrime as a transnational criminal offense are:

1. **International Cooperation:** Given the transnational nature of this crime, law enforcement requires cross-border cooperation, whether in the form of extradition agreements, mutual legal assistance (MLA), or exchange of information and technology between law enforcement officials. Interpol, ASEANAPOL, and Europol are examples of international organizations that help facilitate such coordination.
2. **Legal Harmonization:** Differences in regulations and laws between countries often become obstacles in cracking down on cross-border cybercriminals. Therefore, legal harmonization between countries, especially those that are members of international organizations, is needed so that each country has the same standards in defining and handling cybercrimes.
3. **Jurisdiction:** In the context of cyber crime, the issue of jurisdiction becomes complex because the perpetrators and victims are often located in different countries. Therefore, international law recognizes the concept of universal jurisdiction for certain cases where a country can prosecute perpetrators who commit crimes that have a global impact.
4. **Role of International Organizations:** Organizations such as the United Nations Office on Drugs and Crime (UNODC) also play a role in providing guidance and training to countries in dealing with transnational cybercrime cases, including the development of relevant policies and capacity building of law enforcement.

Cyber crime is a form of criminal offense committed through information and communication technology, especially the internet. This crime includes various illegal activities such as hacking, identity theft, online fraud, and cyber attacks on critical infrastructure. Due to the cross-border nature of the internet, cyber crime is often categorized as a transnational crime.

Law enforcement against cybercrime as a transnational crime requires a multi-level approach involving international cooperation, advanced technology, legal harmonization, and policies that protect privacy and state sovereignty. Without this integrated approach, it will be difficult to tackle the increasingly complex global threat of cybercrime.

CONCLUSIONS

1. The concept of law enforcement related to cyber crime in electronic transactions, among others, is related to several things that need more attention from the government in order to handle cyber crime, especially in Indonesia, which are related to:
 - 1) Applicable Legal Framework
 - 2) Types of Cyber Crime in Electronic Transactions
 - 3) Law Enforcement Process

- 4) Challenges in Law Enforcement
- 5) Victim Protection
- 6) International Approach

With a comprehensive approach, law enforcement against cyber crime in electronic transactions aims to provide justice to victims, prevent criminal acts, and maintain public confidence in the use of technology and the internet in economic activities.

2. Law enforcement against cybercrime as a transnational crime requires a multi-level approach involving international cooperation, advanced technology, legal harmonization, and policies that protect privacy and state sovereignty. Without this integrated approach, it will be difficult to tackle the increasingly complex global threat of cybercrime. Law enforcement against transnational cybercrime has its own challenges, considering that these crimes often involve perpetrators, victims, and infrastructure spread across various countries.

REFERENCES

- Majda El Muhtaj. 2015. Hak Asasi Manusia dalam Konstitusi Indonesia dari UUD 1945 sampai dengan Perubahan UUD 1945 Tahun 2002 Edisi Kedua. Jakarta; Kencana Prenada Media Group.
- Ni'matul Huda, Hukum Tata Negara Indonesia, Jakarta: RajaGrafindo Persada, 2007.
- Iskandar, Pranoto. 2010. Hukum HAM Internasional, Sebuah Pengantar Kontekstual. Malang: IMR Press.
- Simmons, Beth A. *Mobilizing for Human Rights: International Law in Domestic Politics*. Cambridge: Cambridge University Press, 2009.
- Satya Arinanto, , Hak Asasi Manusia dalam Transisi Politik di Indonesia, Jakarta: Pusat Studi HTN FHUI, 2003.
- Jimly Asshiddiqie, Model-Model Pengujian Konstitusional di Berbagai Negara, (Jakarta: Konpress, 2005), hal. 6 – 9.
- Asshiddiqie, Jimly. "The Constitutional Court and Democracy in Indonesia." *Journal of Southeast Asian Constitutional Law* 12, no. 2 (2015): 45-67.
- Jimly Asshiddiqie, dalam Janedjri M. Gaffar, "Peran Putusan Mahkamah Konstitusi dalam Perlindungan Hak Asasi Manusia terkait Penyelenggaraan Pemilu", Jurnal Konstitusi, Volume 10, Nomor 1, Maret 2013, hal. 7. Yang ditulis dalam buku "Pengantar Ilmu Hukum Tata Negara Jilid II", Jakarta: Sekretariat Jenderal dan Kepaniteraan MKRI. 2006.
- Manan, B., & Harijanti, S. D. (2016). Artikel Kehormatan: Konstitusi dan Hak Asasi Manusia. *Padjadjaran Journal of Law*, 3(3), 448-467
- Majelis Permusyawaratan Rakyat RI, Panduan Pemasyarakatan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 dan Ketetapan Majelis Permusyawaratan Rakyat Republik Indonesia, Jakarta: Sekretariat Jenderal MPR RI, 2011, hal. 166
- Moh. Mahfud M.D., "Statuta Roma Dan Politik Hukum Hak Asasi Manusia", Makalah disampaikan dalam sambutan peluncuran Buku Prof. Dr. Muladi, Statuta Roma 1998 dan Perkembangan Hukum Hak Asasi Manusia, Jakarta, 2012.
- Nawas, A. (2021). The position and authority of the Constitutional Court as actors judicial power. *Iblam Law Review*, 1(2), 157–168. <https://doi.org/10.52249/ilr.v2i2.22>
- Vicenzo, R., & Sitabuana, T.H. (2002). Kedudukan dan Peran Mahkamah Konstitusi dalam sistem kenegaraan. *Prosiding serina*, 2(1), 139-146. <https://journal.untar.ac.id/index.php/PSERINA/article/view/18520>.
- United Nations. (1966). **International Covenant on Civil and Political Rights**. Retrieved from <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

Samuels, K. (2017). **Constitutional Reforms and Human Rights Protections in Post-Authoritarian States**. *International Journal of Human Rights*, 21(2), 305-324.