



THE ROLE AND FUNCTION OF THE STATE IN CONDUCTING SUPERVISION AND RISK MITIGATION IN ELECTRONIC TRANSACTION CRIMES

¹HASSANAIN HAYKAL, ²DEMSON TIOPAN, ³SHELLY KURNIAWAN

Universitas Kristen Maranatha

Email : hassanain.haykal@gmail.com, demson.tiopan@maranatha.edu, shellyelviraa@gmail.com

Abstract

The development of the digital economy in Indonesia is progressing very fast and rapidly. The advancement of technology makes transaction activities practical, fast, and safe. However, in reality, Elektronik transactions are only partially secure. Many cases of electronic transaction crimes, such as electronic payment system breaches, harm customers, including leaking personal data. The method used in this research is normative juridical research with a statutory, conceptual, and case approach, which aims to produce new arguments, theories, or concepts in solving the problems to be studied. The results of the study concluded that the role and function of the State in supervising and mitigating risks in electronic transaction crimes is needed as a constructive solution in solving cybercrime problems, especially in this case, electronic transaction crimes. The security dimensions of electronic transactions to minimize the occurrence of crime are Authentication, Integrity, Non-Repudiation, Privacy, and Safety. Several methods can be used to meet the security dimensions of electronic transactions, namely: Public Key Infrastructure (PKI), Public Key Algorithm, Digital Signature, Digital Certificate, Secure Socket Layer (SSL), Transport Layer Security (TLS), and Secure Electronic Transaction (SET). Financial Institutions, including Banking, can apply some of these methods in the context of electronic transaction security.

Keywords: Supervision, Risk Mitigation, Electronic Transaction Crimes.

INTRODUCTION

The development of the *digital economy* in Indonesia is progressing very quickly and rapidly. Even Indonesia is predicted to be the largest country that takes advantage of the advancement of the digital economy in the Southeast Asian region. One of the positive impacts arising from the development of the *digital economy* is the way of transactions for the Indonesian people have begun to change from conventional transactions to electronic transactions, which opens wider opportunities for business actors to expand their business with cheaper costs, easier buying and selling processes, and has a wide range of consumers wider.

According to Article 1 Point 2 of Law Number 11 of 2008 concerning Electronic Information and Transactions (from now on referred to as the ITE Law), it is explained that Electronic Transactions are legal acts carried out using computers, computer networks, and/or other electronic media. It can be said that one of the electronic transaction activities is payments made through an electronic system, or known as an electronic payment system (*e-payment system*). The e-payment system has changed people's need for a payment instrument to meet every transaction's speed, accuracy, and security. History proves that the development of payment instruments continues to change in form, ranging from metal forms to conventional banknotes. Until now, payment instruments have undergone an evolution in the form of data that can be placed in a container, or called electronic payment instruments. There are various types of electronic payment instruments, such as credit cards and debit cards, and what has recently developed is *e-money* which is usually in the form of *stored value cards*.

With the advancement of technology, transaction activities become practical, fast, and safe. But in reality, electronic transactions are not necessarily secure. This can be seen in the case of electronic transaction crimes in Banking Financial Institutions in the form of the first breach of the electronic payment system in 2001, which at that time was quite shocking with the emergence of *phishing* sites

www.clickbca.com which were duplicates of www.klikbca.com. Then a break-in case also occurred in early 2010 was a *skimming* problem on several banks' Automated Teller Machines/Automated Teller Machines (ATMs). This resulted in many customer accounts being breached or compromised, including the personal data of the bank account owner. Several risks may occur in the use of electronic payment systems that are broken by criminals, including:¹

1. Financial losses directly resulting from fraud or fraud;
2. Data theft of valuable information;
3. Loss of business profits caused by disruption to services;
4. Unauthorized use of facilities;
5. Loss of trust from consumers; and
6. Costs resulting from uncertainty.

The above not only results in losses to business actors but will ultimately have an impact on consumers/customers who have entrusted the system in the use of their funds. Therefore, in this case the State must quickly and swiftly carry out an effort to supervise and mitigate risks in electronic transaction crimes that are currently rife. The legal basis of government policy in handling electronic transaction crimes is regulated in Article 40 paragraph (1) of the ITE Law states that the Government protects the public interest from all types of disturbances as a result of misuse of Electronic Information and Electronic Transactions that disturb public order, by the provisions of the Laws and Regulations.

Based on the problems mentioned above, the author will discuss more comprehensively about the types of electronic transaction crimes, the Government's efforts in dealing with electronic transaction crimes, and the third formulation related to the role and function of the State in supervising and mitigating risks in electronic transaction crimes.

RESEARCH METHODS

This research is legal research using normative juridical research. The reason researchers use normative legal research is to produce arguments, theories, or new concepts in solving problems about the role and function of the State in supervising and mitigating risks in electronic transaction crimes.

The approach method used is the *statute approach* and conceptual approach, which is carried out by reviewing all related laws and regulations and discussing and analyzing concepts, theories and doctrines that discuss problems. About this approach, the research is carried out through two stages, namely literature studies and field research which are only supportive.

The data analysis used is qualitative juridical analysis, namely the data obtained, both in the form of secondary data and primary data, are analyzed without using statistical formulations. However, it is done through a process of hermeneutical interpretation.

RESULTS OF RESEARCH AND DISCUSSION

A. Types of Electronic Transaction Crimes

The information and communication technology revolution has increased the use of computer systems and networks. The existence of these technological advances has implications for the development of crime. Traditional crimes are now transforming into ²*cybercrime* using the internet and other electronic devices. *Cybercrime* or computer-based crime, is a crime involving computers and networks (*network*). The computer may have been used in the commission of the crime, or it may have been the target.³⁴

¹ Warwick Ford and Michael S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall, New Jersey, 1997, pg.2.

² Alalwan, N., Alzahrani, A., & Sarrab, M. "Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey". ICoFCS 2013, pg.33.

³ R. Moore "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing. 2005.

⁴ Warren G. Kruse, Jay G. Heiser, *Computer forensics: Incident Response Essentials*. Addison-Wesley, 2002, Pg. 392.

Cybercrimes can be defined as: "Offences committed against an individual or group of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm or harm to the victim either directly or indirectly, using modern telecommunications networks such as *the Internet* (networks including but not limited to *Chat rooms, email, notice boards* and groups) and mobile phones (*Bluetooth/SMS/MMS*)".⁵ *Cybercrime* is a person who commits unlawful acts with the intention of guilt or commits crimes in the framework of *cybercrime*.⁶ *Cybercrime* can threaten a person's security, state security, or financial health.⁷

The United States, the United Kingdom, and Singapore, including Indonesia, are countries that have been quite well-established in designing strategies to combat *cybercrime*, especially in the form of legal formulations. In contrast, most countries in the region, including Burkina Faso, Gambia, Ghana, Kenya, Senegal, and Zimbabwe use emergency laws and policies with an *ad hoc* approach to the phenomenon of *cybercrime*. Other countries in the region try to prevent such activities by blocking access to certain websites.⁸

Based on the results of the author's research, it shows that there are at least 9 (nine) types of electronic transaction crimes, including:⁹

1. *Unauthorized Access to Computer System and Service*

Crimes committed by entering/infiltrating a computer network system unlawfully, without permission. Usually, *criminals* (hackers) do it with the intention of sabotage or theft of important information.

2. *Data Forgery*

It is a crime to falsify data on important documents stored as *scriptless documents* over the internet.

3. *Cyber Espionage*

It is a crime that utilizes the internet network to carry out spying activities against other parties, by entering the target party's *computer network system*.

4. *Cyber Sabotage and Extortion*

This crime is committed by interfering, destroying, or destroying a data, computer program or computer network system connected to the internet.

5. *Infringements of Privacy*

This crime is usually directed against a person's personal information stored on a *computerized* personal data form, which if known by others can harm the victim materially or immaterially, such as credit card numbers, ATM PINs, hidden defects or diseases and so on.

6. *Cracking*

Crimes using computer technology committed to undermine the security of a computer computer and usually commit theft, anarchist acts once they gain access. Usually we often misinterpret between a hacker and a cracker, where the hacker himself identik with negative deedsf, even though hackers are people who like to program and believe that information is very valuable and there is something that can be published and confidential.

7. *Carding*

Carding is an online shopping activity using illegally obtained debit or credit card data. Compared to other crimes, *carding* is relatively easy to do because it does not require a physical card and only relies on data from the debit/credit card you want to target. Usually, perpetrators will search and obtain data from debit or credit cards through fake *marketing*, fake merchants, recording sensitive data by unscrupulous individuals at *merchants*, or from lost cards. Once the person gets all the data from the card number, expiration date, validity period, Card Verification Value (CVV), card limit and

⁵ Halder, D., & Jaishankar, K. *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations* Hershey, PA, USA: IGI Global, 2011.

⁶ Poonia, A. S. "Cyber Crime: Challenges and its classification". *International Journal of Emerging Trends & Technology in Computer Science (IJETCS)*, 2014, pg.119.

⁷ Steve Morgan, "Cyber Crime Costs Projected To Reach \$2 Trillion by 2019". *Forbes*. Retrieved September 22, 2016.

⁸ Dejo Olowu, "Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa", *Journal of Information, Law & Technology*, 1, 2009, pg. 8.

⁹ Sadino, Liviana Kartika Dewi, "Internet Crime in Electronic Commerce", *Journal of Al Azhar University Indonesia*, Vol. 1 No. 2 July 2016, p.12.

other information, the perpetrator will use the data to make online shopping transactions and his financial bills will be borne by the victim.

8. *Phishing*

Phishing is asking (baiting) computer users to disclose confidential information by sending false important messages, whether *emails*, *websites*, or other electronic communications with phishing techniques. The data targeted by phishing is personal data (name, age, address), account data (*username* and *password*), and financial data (credit card information, accounts). The official term phishing is *phishing* which comes from English fishing, namely fishing. Phishing activities are intended to lure people to provide personal information voluntarily without realizing it. Though the information shared will be used for criminal purposes. Because the message looks real and is usually accompanied by threats, users are often trapped by sending sensitive personal information such as *user ID*, *password/PIN*, credit card number, expiration, and CVV.

9. *Card Skimming*

Card skimming is the act of stealing ATM/debit card data by illegally copying (reading or storing) information contained in the magnetic stripe using a *card skimmer* placed in a card slot at an ATM/debit machine or even an *Electronic Data Capture* (EDC) machine when you shop using a debit or credit card.

In addition to these actions, the perpetrator will try to get your ATM/debit card PIN by peeking at the button you press when transacting at an ATM/EDC device. You can also install a small camera at a hidden angle at the ATM machine. Suppose the perpetrator has obtained a copy of your information from the magnetic stripe and ATM/debit card PIN. In that case, the perpetrator will create a fake card using the data that has been obtained and transact using the PIN that has also been obtained.

B. **Government Efforts in Dealing with Electronic Transaction Crimes**

In dealing with *cybercrime* including electronic transaction crimes, the Indonesian government has made several efforts as follows:¹⁰

1. **Enacting the ITE Law**

The Government of Indonesia has passed Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) on April 21, 2008. It has now been amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. The ITE Law is the first legal umbrella specifically regulating *cyber law* in Indonesia. The background of the ITE Law aims to ensure legal certainty in the field of information and electronic transactions. This guarantee is important, considering that the development of information technology has resulted in changes in the economic and social fields.

2. **Optimization of OJK's Supervision Function of Banking Financial Institutions**

The provisions of the regulatory and supervisory duties specified in Article 5 of Law Number 21 of 2011 concerning the Financial Services Authority (OJK Law), mean that the regulatory task is combined with the supervisory task, in other words, OJK has the authority of both at once, namely regulating and supervising. The combination of these two duties is further stipulated in Article 6 letter (a) of the OJK Law which stipulates, "OJK carries out regulatory and supervisory duties on financial services activities in the banking sector". Because OJK must carry out these regulations and supervision, OJK is authorized to do so.


Authority is something that is delegated or from power, the right that is possessed to make decisions, attitudes or actions based on assigned responsibilities. The combination of OJK's authority in carrying out regulatory and supervisory duties in the banking sector, can be seen in the provisions of Article 7 of the OJK Law, that to carry out regulatory and supervisory duties in the Banking sector as referred to in Article 6 letter (a), OJK has the authority:^{11,12}

a. **Regulation and supervision regarding bank institutions which include:**

¹⁰ Dicky Efraim Simanungkalit, "Indonesian Government Policy in Dealing with Hackers in Indonesia, 2008-2014", *eJournal of International Relations*, 2018, 6 (3), 1299-1312.

¹¹ M. Marwan & Jimmy P., *Legal Dictionary*, Reality Publisher, Surabaya, 2009, Pp. 648.

¹² Hirsanuddin and Ahmad Solehudin, *Dynamics Settings Supervision Banking in Indonesia* Book Nation, NTB, 2021, pp.122-123.

- 
- 1). Licensing for bank establishment, opening of bank offices, articles of association, work plans, ownership, management and human resources, bank mergers, consolidations and acquisitions, and revocation of bank business licenses.
 - 2). The bank's business activities include sources of funds, provision of funds, hybridized products, and activities in the service sector.
 - b. Regulation and supervision regarding bank health which includes:
 - 1). Liquidity, profitability, solvency, asset quality, minimum capital adequacy ratio, maximum lending limit, loan-to-deposit ratio, and bank reserves.
 - 2). Bank statements related to the health and performance of the bank.
 - 3). Debtor information system.
 - 4). *Credit testing*.
 - 5). Bank accounting standards.
 - c. Regulation and supervision regarding prudential aspects of banks, including:
 - 1). Risk management.
 - 2). Bank governance.
 - 3). Know your customer and anti-money laundering principles.
 - 4). Prevention of terrorism financing and banking crime.
 - 5). Bank checks.

Article 7 of the OJK Law regulates the duties and authorities of OJK in banking regulation and supervision, this can be interpreted as the authority of OJK is the authority in *microprudential* regulation and supervision. Regulation and supervision regarding institutional, health, prudential aspects and bank inspection are the scope of *microprudential* regulation and supervision which is the duty and authority of OJK. The scope of *macroprudential* regulation and supervision, namely regulation and supervision other than those stipulated in this article, is the duty and authority of Bank Indonesia. To regulate and supervise *macroprudential*, OJK assists Bank Indonesia to make *moral appeals* to banks.¹³

Macro-prudential aspects related to monetary and payment system policy, such as reserve requirements, foreign exchange requirements, open market operations, and reports and audits related to the implementation of monetary and payment system duties are the authority of the monetary authority of Bank Indonesia.¹⁴

3. Cooperate with Institutions, Agencies and Organizations

The Indonesian government's efforts in dealing with *cybercrime* including electronic transaction crimes in Indonesia are collaborating with several institutions in Indonesia that also work based on the ITE Law to deal with cybercrime. The government forms some institutions, but individuals or organizations form some.

a. Ministry of Communication and Information

The Ministry of Communication and Information Technology (Kemenkominfo) acts as a regulator, especially the Directorate General of Information Applications which has 6 Directorates, and also has Civil Servant Investigators to handle ITE criminal cases. The Ministry of Communication and Information is tasked with carrying out government affairs in communication and informatics to assist the President in organizing the country's government.

b. OJK

The Financial Services Authority (OJK) is an independent institution free from interference from other parties, which has the functions, duties, and authorities of regulation, supervision, examination, and investigation as referred to in Law Number 21 of 2011 concerning the Financial Services Authority. In carrying out its duties, OJK coordinates with BI in making supervisory regulations in the banking sector. OJK is also authorized to carry out consumer protection by OJK Regulation No. 01/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector.

c. PPATK

¹³ Explanation Article 7 OJK Law.

¹⁴ Mohammed Djumhana, *Law Banking in Indonesia*, Mold V, Citra Aditya Filial piety, Bandung, 2006, Pp. 130.

The rapid development of technology that has penetrated the financial services sector is well realized by the Center for Financial Transaction Reporting and Analysis (PPATK). Moreover, the development of technology can have a negative impact. On that basis, PPATK has a way to anticipate these negative impacts, namely by forming a new desk, namely the Fintech and Cyber Crime Desk, which is in the form of tapping and misuse of information or data in electronic form or transferred electronically, electronic data theft, fraud via the internet, website destruction, and so on.

d. EN-SIRTII/CC

The Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC) has a supporting role in law enforcement, especially against crimes that utilize information technology. Especially in the presentation of electronic evidence, Id-SIRTII/CC has facilities, expertise and procedures to analyze to make the evidence material legally valuable. In an investigation, Id-SIRTII/CC is central in providing information about statistics and patterns of attacks (incidents) in Indonesian internet traffic.¹⁵

e. ID-CERT

Indonesia Computer Emergency Response Team (ID-CERT) was the first CERT team established in Indonesia, in 1998. ID-CERT is a community-based and community-based technical coordination team for independent communities. ID-CERT plays a role in coordinating technical complaints received and is reactive, both domestically and abroad. In its current form, ID-CERT is reactive (not active) to cases entered or reported by other parties. ID-CERT does not have the authority to investigate cases thoroughly, but only to be a trustworthy liaison, especially by those reporting incidents.¹⁶

f. DIT TIPPID EXUS

In the National Police Headquarters, the handling of cybercrime is in the Directorate of Special Economic Crimes (DIT TIPPID EKSUS) in Subdirectorate IV which handles crimes including crimes related to *cybercrime*, information crimes and electronic transactions. The main duties of Sub-Directorate IV/Cybercrime Field are 1) Conducting investigations and investigations of certain crimes in the field of *cybercrime* that occur in the jurisdiction of Polda Metro Jaya; 2) Organizing the filing and completion of case files by the administrative provisions of criminal investigations and investigations; 3) Organizing the implementation of budget management, as well as the management of investigations and investigations of certain crimes, in the field of *cybercrime* that occurs in the jurisdiction of PoldaMetro Jaya; 4) Carry out case analysis, economic issues that stand out/disturb the community and their handling actions, as well as assess the effectiveness of the implementation of the duties of the Cybercrime Sub-Directorate; 5) Organizing the development of functions and techniques of criminal investigation and investigation *cybercrime*; 6) Carry out other duties ordered by the Dir and Wadir of Reskrimsus Polda Metro Jaya.¹⁷

g. PANDI

Indonesian Internet Domain Name Manager (PANDI) is a non-profit organization formed on December 29, 2006 by the Government of the Republic of Indonesia and the Indonesian internet community. PANDI was formed to manage domain.ID name in a professional, accountable, and transparent manner by the legal principles of the Republic of Indonesia. PANDI is a legal entity as an association, consisting of individuals from Indonesian internet *multistakeholders*. PANDI membership reflects the representation of the Government of the Republic of Indonesia, academics, and businesses. The duties of PANDI, namely 1) Formulate policies in the field of management of Indonesian High-Level Domain Names; 2) Prepare, operate, and maintain the required infrastructure and provide an electronic system for the management of Indonesian High Level Domain Names; 3) Organizing the registration of Indonesian High Level Domain Names by the provisions of laws and regulations, propriety applicable in society, and precautionary principles.^{18,19}

4. Conducting socialization to the community


¹⁵ <http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtiicc.html> access March 28, 2023.

¹⁶ <https://www.cert.or.id/tentangkami/id/> accessed March 28, 2023.

¹⁷ <http://www.reskrimsus.metro.polri.go.id/StrukturOrganisasi/StrukturOrganisasi.aspx? Id=6&Menuid=0> access date 28 March 2023.

¹⁸ <https://pandi.id/profil/tentang-pandi/> access date 28 March 2023.

¹⁹ <https://pandi.id/profil/tugaspanidi/akses> date 28 March 2023.



Another effort of the Indonesian government in dealing with cyber crime is to socialize the public, to be more concerned about cybercrime. Since 2008, the Ministry of Communication and Information has organized all agencies' socialization through seminars and technical guidance. This evaluation is not only intended to analyze the feasibility or effectiveness of existing forms of security, but also as a tool to describe the state of readiness of the information security framework to the leaders of the agencies being guided. The approach is carried out through an information security management system and through a careful, accurate, and up to date technological approach to close any holes or loopholes for cyber attacks. In theory, information security aims to ensure information integrity, data confidentiality, information availability, and compliance with regulations and laws.²⁰

5. Cooperation with other countries

Indonesia has cooperated in handling cyber crime cases with countries such as Australia, Hong Kong and China. The agreement with Australia was signed on November 13, 2006, in Mataram, Lombok. Signed by Dr. N. Hassan Wirajuda as Minister of Foreign Affairs of the Republic of Indonesia and Alexander Downer as Minister of Foreign Affairs of Australia. The handling of cyber crime cases is contained in Article 3 concerning the Scope and Form of Cooperation, paragraph (7) concerning Law Enforcement Cooperation, point F concerning Cybercrime Agreement between the Republic of Indonesia and Australia concerning the Framework for Security Cooperation, Mataram, Lombok, 2006. Activities carried out after the MoU by Indonesia and Australia were the establishment of CCISO (*cyber crime investigations satellite office*) on April 29, 2013, which was inaugurated by the Deputy Chief of the Indonesian Police Department, General Nanan Sukarna (representing the Chief of Police Department, General Pol Timur Pradopo) with the Chief of Police *Australian Federal Police Commissioner*, Tony Negus. CCISO has been officially established in Polda Metro Jaya, Mabes Polri, Polda Medan, Polda Bali and Polda NTB. Tony Negus also explained that Australia will assist in equipping equipment and training all members who will work at CCISO Indonesia and Australia will pour approximately Australia \$ 9 million to help build everything.²¹

The next agreement with the country of Hong Kong, signed on November 3, 2014, took place in Monaco. It was signed by Sugeng Priyanto as Inspector General of Police of the Republic of Indonesia and Lo Mung-Hung as *Senior Assistant Commissioner Director of Crime and Security of Hong Kong Police Force*. The handling of cyber crime cases is contained in Article 2 concerning the Purpose and Scope of Cooperation, paragraph (1) concerning the Prevention and Eradication of International Crime, point D concerning Cybercrime Memorandum of Understanding Between the National Police of the Republic of Indonesia and the Hong Kong Police in the Prevention and Prevention of International Crime and Capacity Building, Monaco, 2014.

In 2016, Indonesia and China plan to conduct joint operations including cyber warfare simulation, cyber warfare response and mitigation, cyber *monitoring*, cyber crisis management, and planning for data *center* recovery. Expert Staff of the National Cyber Information Security and Resilience Desk, Muchlis Ahmady, said cooperation is part of knowledge sharing because *cyber* problems cannot be handled alone. Expert Staff of the National Cyber Information Security and Resilience Desk, Muchlis Ahmady, also said that his party and the CAC (*Cyberspace Administration of China*) had held a meeting earlier this week as a pre-MoU (*memorandum of understanding*) related to *capacity building* for *cyberspace* human resources.²²

6. Joint Training in Dealing with Cybercrime

Efforts to combat and prevent cybercrime have begun with a meeting by the National Legal Development Agency (BPHN) with the *Korean Institute of Criminology (KIC)* and the *United Nations Office on Drugs and Crime (UNODC)* held on October 30-31, 2008 in Seoul, South Korea. In the meeting, an ²³ *online* cyber crime prevention and countermeasures training program was held at law enforcement in Indonesia, including the police, prosecutors, judges and cyber crime investigators. The way to overcome this is by introducing an international forum, the *Virtual Forum Against*

²⁰ <https://m.tempo.co/read/news/2013/11/16/072530183/penggunateknologi-diajak-peduli-cyber-crime> access date 28 March 2023.

²¹ <http://www.plimbi.com/news/84972/indonesia-buka-kantor-cybercrime-investigations> access date 28 March 2023.

²² <https://www.antaraneews.com/berita/541577/ri-tiongkok-rintis-kerja-samakeamanan-cyber> access date 28 March 2023.

²³ <http://www.bphn.go.id/news/2008121213332241/Pencegahan-danpenanggulangan-kejahatan-Cyber>, access date March 28, 2023.

Cybercrime. The forum presents various information about cybercrime for researchers, legal practitioners, and the general public and organizes *online* training for law enforcement to tackle and eradicate *cyber crime*.

The training process will be provided in the form of a syllabus and *online* materials prepared by KIC and UNODC and will be translated into local languages. The *online* material includes basic training consisting of 26 lessons, concerning knowledge of Information and Communication Technology and regulation in the field of cybercrime and advanced training consisting of 119 lessons concerning knowledge of *Cybercrime Investigation* (procedures, techniques and digital forensics) as well as various seminars with issues and topics related to *cybercrime*.²⁴

C. The Role and Function of the State in Supervising and Mitigating Risks in Electronic Transaction Crimes

The role of the State is contained in the Preamble of the 1945 Constitution 4th Paragraph, namely protecting the entire Indonesian nation and all Indonesian bloodshed, promoting general welfare, educating the nation's life, and implementing world order based on independence, lasting peace, and social justice. While the functions of the State are defense and security, justice, regulation and order, welfare and prosperity. Based on this thinking, the role and function of the State in carrying out supervision and risk mitigation in electronic transaction crimes will be described as follows:

1. Supervision Aspect

The role and function of the State in carrying out supervision on electronic transaction crimes is carried out in several aspects as follows:²⁵

a. Supervision of Product Standards and Labels

The rise of online commerce or what we call *e-commerce* behind this makes it very easy for people to make transactions in meeting their various needs. The application of *e-commerce* has become commonplace for business actors to adjust to market needs. The development of *e-commerce* globally provides opportunities for small, medium companies to compete better with large companies because market access has become equal. This opportunity can only be utilized by business actors who are competent in using *e-commerce*.

The implementation of *e-commerce* transactions must be balanced with strict supervision in each implementation. In Law Number 7 of 2014 concerning Trade (Trade Law) itself, the supervisory function of *e-commerce* trade has yet to be fully regulated clearly. In Chapter XVI Article 98 regarding supervision it is stated:

(1) The Government and Local Government have the authority to supervise Trade activities.

(2) In carrying out supervision as referred to in paragraph (1), the Government establishes supervision policies in the field of Trade.

The supervisory function mandated by the Trade Law is only limited to trade in general, not to *e-commerce* trade with characteristics different from conventional trade. Negligence to this supervisory function can be a loophole for violations in *e-commerce* transactions. Like the problem of standardization, because it is easy to transact on the internet with the lure of low prices, sometimes many consumers only look at low prices, not at the quality of goods sold. This makes a gap for business actors/rogue importers to get around the entry of goods that should not meet the standards set by the government through the Indonesian National Standard (SNI). Still, through *e-commerce* transactions these non-SNI product goods can freely enter the community.

In the Trade Law, restrictions have been given on what things are the supervisory duties of the mandate of this Trade Law. Article 100 paragraph (3) states:

"The Supervisory Officer as referred to in paragraph (2) in exercising his authority shall at least supervise over:

- a. Licensing in the field of Trade;
- b. Trade in controlled, prohibited and/or regulated Goods;

²⁴ *Ibid.*

²⁵ Deky Pariadi, "Supervision E Commerce Deep Law Trade And Law Protection User", *Journal Law & Development*, Vol. 48 No. 3 (2018): 652-670.



- c. Distribution of Goods and/or Services;
- d. Registration of Domestic Products and Import Origin related to security, safety, health, and the environment;
- e. Mandatory application of SNI, technical requirements, or qualifications;
- f. Warehouse Registration; and
- g. Storage of necessities and/or essential goods."

The Ministry of Trade (Kemendag), as the trade sector supervisor, requires all products or goods traded through *e-commerce* to meet the Indonesian National Standard (SNI). The Ministry of Trade will tighten supervision of *the e-commerce* business, ensuring that all products sold have met these provisions.

The Director General of Standardization and Consumer Protection of the Ministry of Trade revealed that the supervision will be carried out by the Regulation of the Minister of Trade (Permendag) Number 72/M-Dag/Per/9/2015 concerning the Third Amendment to the Minister of Trade Regulation Number 14/M-Dag/Per/3/2007 concerning Standardization of Services in the Field of Trade and Supervision of Mandatory SNI for Goods and Services Traded. In addition, products sold online must also comply with Minister of Trade Regulation Number 73/M-Dag/Per/9/2015 concerning the Obligation to Include Labels in Indonesian on Goods. Article 2 paragraph (1) of Permendag No. 73/M-Dag/Per/9/2015 states, "Business actors who produce or import goods for trade in the domestic market must include labels in the Indonesian." The Minister of Trade also provides a classification of what types of products are required to contain labels in Indonesian, including: electronic goods for household purposes, telecommunications and informatics; building material goods; goods for motor vehicles (spare parts and others); and textile goods and textile products.

b. Supervision of the Legality of Business Actors

Trade through *e-commerce* is also a special concern in the Trade Law. The existence of Chapter VIII concerning Trade Through Electronic Systems Article 65 of the Trade Law will be clearly regulated starting from the identity and legality of business actors, technical requirements for goods and qualifications of services offered, prices and payment methods, to the way of delivery of goods.

Related to data and information on business actors required to be registered in Article 65 of the Trade Law has been regulated in the ITE Law. Article 10 paragraph (1) of the ITE Law affirms that: "Every business actor who organizes Electronic Transactions can be certified by a Reliability Certification Body. Then Article 15 paragraph (1) states, "Every Electronic System operator must operate the Electronic System reliably and securely and is responsible for the proper operation of the electronic system."

Regarding certification, this is reaffirmed in article 41 of Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions which reads: "The implementation of Electronic Transactions in the public or private sphere that uses Electronic Systems for the benefit of public services must use Reliability Certificates and/or Electronic Certificates". The legality and identity of the perpetrators are very important in *the e-commerce* trade regulated in this Trade Law. This sees the many phenomena of still not trusting consumers towards *e-commerce* services in Indonesia.

c. Supervision and Development of Consumer Protection Implementation

In carrying out the function of guidance and supervision and ensuring the implementation of consumer protection for goods traded, Law Number 8 of 1999 concerning Consumer Protection (Consumer Protection Law) through Article 29 regulates this, namely:

- (1) The government is responsible for fostering the implementation of consumer protection that guarantees the obtaining of consumer and business rights and the implementation of consumer and business obligations.
- (2) Guidance by the government on the implementation of consumer protection as referred to in paragraph (1) is carried out by the Minister and/or the relevant technical minister.
- (3) The Minister as referred to in paragraph (2) coordinates the implementation of consumer protection.

(4) Guidance on the implementation of consumer protection as referred to in paragraph (2) includes efforts to:

- a. the creation of a business climate and the growth of healthy relationships between business actors and consumers;
- b. the development of non-governmental consumer protection agencies;
- c. Improving the quality of human resources and increasing research and development activities in consumer protection.

(5) Government Regulations regulate further provisions regarding the guidance of consumer protection implementation.

In connection with the provisions of Article 29 of the Consumer Protection Law, the main factor that becomes a weakness of consumers is the level of understanding and awareness of their rights which still needs to be improved and correlates with low consumer education factors. Based on this, Article 29 of the Consumer Protection Law states that a government is responsible for fostering the implementation of consumer protection to empower consumers in obtaining their rights. Consumer empowerment, by the principles of fairness and balance, must not harm the interests of business actors, but on the contrary through consumer protection is expected to encourage a healthy business climate and the birth of a resilient company in facing competition through the provision of quality goods and/or services. Efforts to foster consumer protection organized by the government as mandated by law are to obtain consumer and business actors' rights and implement their obligations by the principle of justice.

d. Supervision of Banking Financial Institutions

About electronic transactions in the banking sector, the establishment of laws and regulations must also apply to business actors or issuers, and there is consistency with regulations and their implementation. These rules must be announced and formulated clearly and understandably by customers as the object of the arrangement, this is because the electronic transaction system is a transaction with electronic evidence. Legal problems in the electronic system will occur if the electronic payment system used to carry out electronic transactions (payments) fails and results in losses, or even the existence of an electronic transaction crime.²⁶²⁷

OJK has authorities, one of which is the authority to supervise banking. This authority to supervise (*right to control*) has 2 (two) supervisory techniques, namely:

- 1). *On-site supervision* consists of general and special examinations to obtain an overview of the bank's financial condition and to monitor the level of bank compliance with applicable regulations, as well as to find out whether there are unhealthy practices that endanger the continuity of the bank's business;
- 2). *Off-site supervision* is supervision through monitoring tools such as periodic reports submitted by banks, reports on inspection results and other information.²⁸

The role of OJK in providing consumer protection according to the provisions of Article 28 to Article 31 of the OJK Law can be taken preventive and eradication measures. According to Article 28 of the UUOJK, OJK is authorized to take measures to prevent consumer and public losses in the context of consumer and public protection. In this case, OJK is authorized to take steps to prevent customer losses. Other actions in protecting consumers are efforts to accommodate customers' aspirations. OJK conducts consumer complaint services by preparing adequate tools for the service of complaints of consumers who are harmed by banks, including creating a complaint mechanism for aggrieved consumers.

2. Risk Mitigation of Electronic Transaction Crime

Risk mitigation is an effort to reduce/stop negative impacts (losses) that have occurred. The relationship between risk management and internal control. The main meeting point is the importance of taking *preventive action* or building an effective *early warning system or alert system*,

²⁶ Niniek Suparni, *Cyberspace Peoblematics and Anticipation Setting*, Light Graphics, Jakarta, 2009, Pp. 110-111.

²⁷ Ni Nyoman Anita Candrawati, "Protection Law Towards Holder Cards E-Money As Tool Payment Deep Transaction Commercial", *Journal Master of Laws Udayana*, Vol. 3 No. 1, 2014, Pp. 7.

²⁸ Zulfi Diane Zaini, *Independence Bank Indonesia and Settlement Bank Problematic*, Keni Media, Bandung, 2012, p.150.



where various risks that may occur and their impacts can be identified, measured, and minimized as little as possible (*controllable risk*).

In mitigating the risk of electronic transaction work, 2 (two) main things must be considered, namely 1) what things are needed to create security for electronic transactions; and 2) the method used to create such security.

In principle, the security dimension of electronic transactions to minimize the occurrence of crime, among others:

1. The authentication, buyers, sellers, and payment institutions involved must be identified as parties entitled to enter into the transaction;²⁹
2. Integrity, assurance that data and information transferred to e-commerce remain intact and unchanged;
3. Non-Repudiation, the customer needs protection against denial from the seller that the goods have been delivered or payment has not been made. Information is needed to ascertain who the sender and recipient are;
4. Privacy, customers want their identities to be secure. They don't want others to know what they're buying;
5. Safety, customers want assurance that providing credit card number information on the internet is safe.

In addition, some several methods and mechanisms can be used to meet the security dimension of electronic transactions, namely:³⁰

1. *Public Key Infrastructure (PKI)*

Allowing users not inherently secure in public networks such as the internet, the PKI would feel safe and privately exchange money and data through public use.³¹

2. *Public Key Algorithm*

Also called an *asymmetric algorithm (asymmetric algorithm)* is an algorithm that uses different keys when encrypting and doing descriptions.

3. *Digital Signature*

Digital signature is a signature made electronically, with more guarantees for data security and data authenticity, both guarantees about the identity of the sender and the correctness of the data or data packet.

4. *Certificate Digital*

The Certificate Authority is a trusted third party (*Trust Thrid Party/TTP*). Certificate Authority that will associate the key with its owner. This TTP will issue a certificate containing the person's identity and the person's private key.

5. *Secure Socket Layer (SSL)*

A protocol that creates a protective pipe between the *cardholder's browser* and the *merchant*, so that hijackers or attackers cannot intercept or hijack the information flowing in the pipe. In its use, SSL is used in conjunction with other protocols, such as HTTP (*Hyper Text Transfer Protocol*), and *Certification Authority*.

6. *Transport Layer Security (TLS)*

It is a cryptographic protocol that provides security for communications on the Internet such as e-mail, faxing, and other data transfers.

7. *Secure Electronic Transaction (SET)*

Is a *combination of public/private key technology with digital signatures*. In encryption, the public key uses 56 bit encryption up to 1024 bits, so the level of encryption combination is very high. In the transaction, the CA creates a digital certificate containing identity information, the cardholder's

²⁹ Bendovschi, "A. Cyber Attacks Trends, Patterns And Security Countermeasures". *Procedia Economics And Finance*, 28, (2015). PG.29.

³⁰ Andre M. R. Wajong and Carolina Rizki Daughter, "Security Deep Electronic Commerce" *ComTech* Vol.1 No.2 December 2010, 867-874.

³¹ E. Casey, "Error, Uncertainty, And Loss In Digital Evidence," *International Journal of Digital Evidence*, Vol. 1, No. 2, 2002.

public key, and credit card number information that is 'hidden', so the cardholder is like having a digital "KTP". Developing SET infrastructure is relatively expensive, so this is one of the disadvantages.

CONCLUSION

Electronic transaction crime is part of *cybercrime*, classified as a crime category that harms financial aspects. There are several types of electronic transaction crimes that criminals, such as Unauthorized Access to Computer System and Service, Data Forgery, Cyber Espionage, Cyber Sabotage and Extortion, Infringements of Privacy, Cracking, Carding, Phishing, and Skimming often commit.

The Indonesian government has made several efforts to deal with electronic transaction crime cases, such as: 1) Enacting the ITE Law; 2) Optimization of OJK's supervisory function towards the Banking Finance Lembaga; 3) Cooperate with several institutions, agencies or organizations in Indonesia; 4) Conduct socialization to the community; 5) Work the same as other countries; and 6) conduct joint training in dealing with *cyber law*.

The role and function of the State in supervising and mitigating risks in electronic transaction crimes is needed as a constructive solution in solving *cybercrime* problems, especially in this case electronic transaction crimes. Supervision activities are carried out on several aspects such as 1) Supervision of Standardization and Product Labels; 2) Supervision of the legality of business actors; 3) Supervision and Development of Consumer Protection Implementation; and 4) Supervision of Banking Financial Institutions. In addition to supervision, the State needs to carry out risk mitigation activities regarding the health of electronic transactions. In principle, 2 (two) main things must be considered in carrying out risk mitigation activities, namely 1) what things are needed to create security for electronic transactions; and 2) the method used to create such security. The security dimensions of electronic transactions to minimize the occurrence of crime are Authentication, Integrity, Non-Repudiation, Privacy, and Safety. In addition, some several methods and mechanisms can be used to meet the security dimensions of electronic transactions, namely: Public Key Infrastructure (PKI), *Public Key Algorithm*, *Digital Signature*, *Digital Certificate*, *Secure Socket Layer (SSL)*, *Transport Layer Security (TLS)*, and *Secure Electronic Transaction (SET)*.

BIBLIOGRAPHY

Book:

- [1] Halder, D., & Jaishankar, K. *Cyber Crime And The Victimization of Women: Laws, Rights, and Regulations* Hershey, PA, USA: IGI Global, 2011.
- [2] Hirsanuddin dan Ahmad Solehudin, *Dinamika Pengaturan Pengawasan Perbankan di Indonesia*, Pustaka Bangsa, NTB, 2021.
- [3] M. Marwan & Jimmy P., *Kamus Hukum*, Reality Publisher, Surabaya, 2009.
- [4] Muhamad Djumhana, *Hukum Perbankan di Indonesia*, Cetakan V, Citra Aditya Bakti, Bandung, 2006.
- [5] Niniek Suparni, *Cyberspace Peoblematika dan Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009.
- [6] R. Moore, *Cyber crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2005.
- [7] Warren G. Kruse, Jay G. Heiser, *Computer forensics: Incident Response Essentials*, Addison-Wesley, 2002.
- [8] Warwick Ford dan Michael S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall, New Jersey, 1997.
- [9] Zulfi Diane Zaini, *Independensi Bank Indonesia dan Penyelesaian Bank Bermasalah*, Keni Media, Bandung, 2012.

Journals, Papers:

- [1] Alalwan, N., Alzahrani, A., & Sarrab, M. "Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey". *ICoFCS*, 2013.
- [2] Andre M. R. Wajong dan Carolina Rizki Putri, "Keamanan Dalam Electronic Commerce" *ComTech* Vol.1 No.2 Desember 2010.
- [3] Bendovschi, "A. Cyber Attacks Trends, Patterns And Security Countermeasures". *Procedia Economics And Finance*, 28, (2015).
- [4] Dejo Olowu, "Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa", *Journal of Information, Law & Technology*, 1, 2009.



- [5] Dedy Pariadi, "Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen", *Jurnal Hukum & Pembangunan*, Vol. 48 No. 3 (2018).
- [6] Dicky Efraim Simanungkalit, "Kebijakan Pemerintah Indonesia Dalam Menangani Hacker Di Indonesiatahun 2008-2014", *eJournal Ilmu Hubungan Internasional*, 2018, 6 (3).
- D. Casey, "Error, Uncertainty, And Loss In Digital Evidence," *International Journal of Digital Evidence*, Vol. 1, No. 2, 2002.
- [7] Ni Nyoman Anita Candrawati, "Perlindungan Hukum Terhadap Pemegang Kartu E-Money Sebagai Alat Pembayaran Dalam Transaksi Komersial", *Jurnal Magister Hukum Udayana*, Vol. 3 No. 1, 2014.
- [8] Nugraha, Y. (2021). Covid-19 in Italy: Impact of Lockdown in Italy on Socio-Economic Situation. *Journal of Social Science*, 2(2), 223-227.
- [9] Poonia, A. S. "Cyber Crime: Challenges and its classification". *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 2014.
- [10] Rahayu, W. K., Purwanti, A., Astuti, R. S., & Lituhayu, D. (2023). Enhancing Women's Resilience in Disaster Condition in Padang City West Sumatra Province. *International Journal of Social Service and Research*, 3(3), 775-779.
- [11] Steve Morgan, "Cyber Crime Costs Projected To Reach \$2 Trillion by 2019", *Forbes*, Retrieved September 22, 2016.

Laws and Regulations:

- [1] Undang-Undang Dasar Tahun 1945 Amandemen Ke-4;
- [2] Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen;
- [3] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
- [4] Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan;
- [5] Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan;
- [6] Peraturan OJK No. 01/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan;
- [7] Peraturan Menteri Perdagangan (Permendag) Nomor 72/M-Dag/Per/9/2015 tentang Perubahan Ketiga atas Permendag Nomor 14/M-Dag/Per/3/2007 tentang Standarisasi Jasa Bidang Perdagangan dan Pengawasan SNI Wajib Terhadap Barang dan Jasa yang Diperdagangkan;
- [8] Permendag Nomor 73/M-Dag/Per/9/2015 tentang Kewajiban Pencantuman Label Dalam Bahasa Indonesia Pada Barang

Internet:

- [1] <http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtiicc.html> [28-03-2023].
- [2] <http://www.bphn.go.id/news/2008121213332241/Pencegahan-danpenanggulangan-kejahatan-Cyber>, [28-03-2023].
- [3] <http://www.plimbi.com/news/84972/indonesia-buka-kantor-cybercrime-investigations> [28-03-2023].
- [4] <http://www.reskrimsus.metro.polri.go.id/StrukturOrganisasi/StrukturOrganisasi.aspx?id=6&Menuid=0> [28-03-2023].
- [5] <https://m.tempo.co/read/news/2013/11/16/072530183/penggunateknologi-diajak-peduli-cyber-crime> [28-03-2023].
- [6] <https://pandi.id/profil/tentang-pandi/> [28-03-2023].
- [7] <https://pandi.id/profil/tugaspandi/> [28-03-2023].
- [8] <https://www.antaraneews.com/berita/541577/ri-tiongkok-rintis-kerja-samakeamanan-cyber> [28-03-2023].
- [9] <https://www.cert.or.id/tentangkami/id/> [28-03-2023].