LAW
RESEARCH
REVIEW
QUARTERLY

published by
FACULTY *of* LAW
UNIVERSITAS NEGERI SEMARANG
K Building 1st Floor, Sekaran Campus, Gunungpati
Semarang, Central Java, Indonesia, 50229
Email: lawquarterly.journal@mail.unnes.ac.id

ISSN 2716-3415

LAW RESEARCH REVIEW QUARTERLY VOL. 7(1) FEBRUARY 2021

ISSN 2716-3415

LAW RESEARCH REVIEW QUARTERLY

VOLUME 7 ISSUE 1
FEBRUARY 2021

Published quarterly by
UNNES
FACULTY *of* LAW
UNIVERSITAS NEGERI SEMARANG
INDONESIA

ISSN 2716-3415

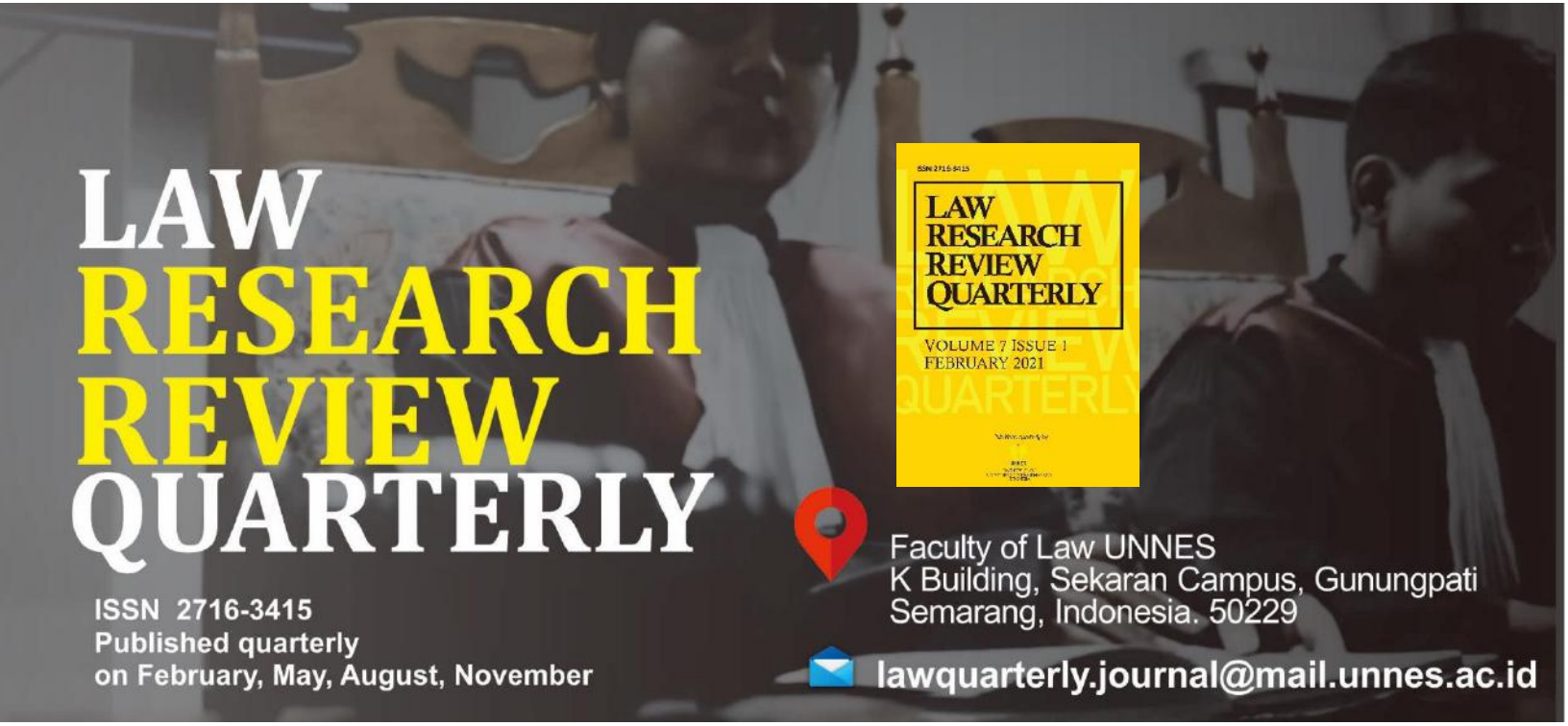
LAW RESEARCH REVIEW QUARTERLY

VOLUME 7 ISSUE 1
FEBRUARY 2021

Published quarterly by

UNNES
UNIVERSITAS NEGERI SEMARANG

FACULTY *of* LAW
UNIVERSITAS NEGERI SEMARANG
INDONESIA



EDITORIAL TEAM

FOCUS AND SCOPE

Law Research Review Quarterly is ***a double blind peer-reviewed journal*** published by Faculty of Law, Universitas Negeri Semarang, Indonesia, and the journal has been implemented the full system of open journal system (OJS). The Law Research Review Quarterly initially published research articles that had been disseminated in the National Seminar on Law at the Semarang State University and published in Bahasa In donesia since 2015. Then, since 2020 starting from Volume 6 Number 1, *Seminar Nasional Hukum Universitas Negeri Semaran*g changed to Law Research Review Quarterly and published four times in one year (every February, May, August, and November) and exclusively publishes in English. The Law Research Review Quarterly aims to be a forum for law activists, legal practitioners, academics, law fighters, law enforcement officials, and students in developing scientific fields of law in various researches, both normative and empirical research (Research Article and Review Article). Law Research Review Quarterly publishes articles related to the law (but not limited to): Criminal Law, Civil Law, International Law, Procedural Law, State administration law, Constitutional Law, Business Law, Law and Society, Islamic law, Customary Law, Environmental Law, Law and Human Rights, aw of technology, Health Law, Law of the Sea, Diplomatic and consular law, Humanitarian Law, International Organizational Law, Comparative Law, Tax Law, International Economic and Trade Law, Law and Public Policy, Anti-Corruption Law, Anti-terrorism law, Law of Intellectual Property Rights, Land Law, Legal Reform, Insurance Law, Legal Aid, Law Justice and Crime, and others relating to the study of law and its various aspects (including political, economic, social and cultural).

JOURNAL HISTORY

The Law Research Review Quarterly was originally called the 'Semarang State University Law National Seminar' Journal, which was published in 2015. As a form of development towards an internationally reputable Journal, starting in 2020 the name Law Research Review Quarterly was used using the new ISSN code (starting Volume 6 Number 1). Since its publication in 2015, this journal uses the Open Journal System (OJS) in full and can be accessed free of charge. Starting in 2017, this journal has also involved various reviewers from various institutions from within the country and starting in 2020 this journal will involve several partners from abroad, such as Malaysia, Brunei Darussalam, Japan, Australia, United States, Thailand, Nigeria, India, Bangladesh, Vietnam, the People's Republic of Tiongkok, and Russia. This journal has also collaborated with various parties, one of them with the Journal Management Association in Indonesia (APJHI).

LAW RESEARCH REVIEW QUARTERLY

VOLUME 7 ISSUE 1, FEBRUARY 2021

CONTENTS

RESEARCH ARTICLE

RESEARCH ARTICLE

The Urgency of Redefinition of Offense Formulation of Corruption in The Law on The Eradication of Corruption

Sholahuddin Al-Fatih
Faculty of Law, Universitas Muhammadiyah Malang, Indonesia
Jl. Raya Tlogomas No. 246 Malang, East Java, Indonesia
✉ sholahuddin.alfath@gmail.com

OPEN ACCESS

Citation: Al-Fatih, S. (2021). The Urgency of Redefinition of Offense Formulation of Corruption in The Law on The Eradication of Corruption. *Law Research Review Quarterly, 7*(1), 1-18. https://doi.org/10.15294/lrrq.v7i1.43897.

Submitted : January 9, 2021
Revised : January 30, 2021
Accepted : February 3, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

This research aims to analyse corruption law in Indonesia, especially in the form of offense formulation of corruption in the law on the eradication of corruption. This study used mixed legal method, namely descriptive qualitative and normative juridical method. This research found that corruption in Indonesia still doing as business as usual. Moreover, in the offense formulation of corruption eradication, there are quite several ambiguous and multi-interpretative norms, that can be interpreted widely by the judge. This condition is very horrible and terrible. In connection with the above conclusions, then there are some things that can be suggested by the authors and are expected to be used as material for consideration for parties related to this research, the government should provide clear and certain offense formulation of corruption and the judges may not interpret the formulation of corruption offenses with the aim of reducing or alleviating the punishment of corruptors.

Keywords: *Redefinition; offense; formulation; corruption; law*

1. INTRODUCTION

Corruption and catch-hand operation (well known in Indonesia as OTT or *Operasi Tangkap Tangan*) cases of recent officials have again made *headlines in print* and online newspapers. In recent months, KPK conducted OTT to two advanced Indonesian Cabinet ministers, namely Juliari

Batubara (Minister of Social Affairs) and Edhy Prabowo (Minister of Marine Affairs and Fisheries).

Although KPK has routinely conducted OTT and strict crackdown on corruptors, the fact that corruption cases persist today, like mushrooms in the rainy season. Corruption is nothing new in this country. Even corruption has gone viral since the beginning of this country's founding. Kartono in the 80s has put limits on the definition of corruption as the conduct of individuals who use their authority and position to extract personal gain, harming the public interest and the state (Kartono, 2012). There are discussions and scientific studies on corruption in the early era of independence as well as evidence that corruption is not new and prevention and eradication efforts have begun since time immemorial.

Referring to the notes submitted by Denny Indrayana, efforts to prevent and eradicate corruption have been started since 1957 through an institution named the Coordinating Board of Property Reviewers (Indrayana, 2016). Furthermore, the government at that time commonly known as the Old Order Era re-established anti-corruption institutions in a few years continuously, such as the birth of the State Apparatus Activities Supervisory Agency/Bapekan (1959-1962), The Committee for Retooling State Apparatus/ Paran 1 (1960-1963), Paran 2/Operation Budi (1963-1967), Command Retooling Apparatus Revolution/ Kotrar (1964-1967) (Indrayana, 2016). The New Order era was also no less ferocious in blocking the pace of corruption. It is recorded that there are 4 anti-corruption institutions born in the New Order Era, namely; Corruption Eradication Team 1 (1967), Commission 4 (1970), Operation Control (1977-1981) and Corruption Eradication Team 2 (1982) (Indrayana, 2016).

The commitment to fight corruption is also a key point of the post-reform government. Noted, the Reform Era gave birth to 3 anti-corruption institutions, namely the Joint Team for the Eradication of Corruption Crimes (TGTPK), the Corruption Eradication Commission (KPK) and the Coordination Team for the Eradication of Corruption (*TimTasKorupsi*) (Indrayana, 2016). Until now, the one who still exists and gets the authority to prevent and eradicate corruption, collution and nepotism (well known in Indonesia as *Korupsi, Kolusi, Nepotisme,* KKN) in this country is KPK. Although it has involved many institutions with

various dynamics in it, the KKN case, especially corruption seems to be still running as usual.

Corruption cases in Indonesia do not continue to decrease, but instead continue to take root and run like busines as usual (Lubis, 2011). This is evidenced by a report from Transparency International (TI), on the Corruption Perception Index (CPI) or commonly referred to as the *Indeks Persepsi Korupsi* (IPK). Indonesia as one of the countries surveyed by TI, in the last survey in 2016, Indonesia pocketed a score of 37 points. Indonesia is ranked 90th out of 176 countries surveyed worldwide. At the Southeast Asian level, Indonesia lost to Singapore (CPI score of 85), Brunei Darussalam (58), Malaysia (49). Indonesia has only better rankings and points compared to Thailand (35), Philippines (35), Vietnam (33), Myanmar (28) and Cambodia (21). CPI takes a range of values from 0 to 100, where 0 is perceived to be very corrupt, while 100 is very clean (Al-Fatih, 2018).

The data then improved in 2019. Transparency International Indonesia (TII) released data on Indonesia's corruption perception index (CPI) in 2019 at number 40 with the highest score of 100. The corruption perception index refers to 13 expert surveys and assessments to measure public sector corruption in 180 countries and territories. CPI value is based on a score of 0 for very corrupt and a score of 100 is very clean. Based on rankings, Indonesia is ranked 85th out of 180 countries. Indonesia's corruption perception index score has increased by two levels from 2018. In 2018, Indonesia had a score of 38 out of 100 with an 89th place out of 180 countries (Mashabi, 2020). However, with the OTT of two ministers and several regional heads in 2020, Indonesia's CPI score may fall again.

In the Florentin Saga, Machiavelli looked at several reasons that made corruption rampant. *First*, the state is enslaved by another country. Every year, the government seeks foreign loans of up to tens of trillions of rupiah to close the budget deficit. The source could be from multilateral institutions such as the IMF, World Bank or ADB. In addition, there is also bilateral and commercial debt by issuing global bonds that are usually denominated in U.S. Dollars, and most recently Yuan. As a result, Indonesia seems to be a slave to the countries or financial institutions of the debt guarantor. Governments in making policies often

get interference from outside parties for their benefit. As a result, it is very difficult for the government to make regulations for its own internal affairs.

The *second,* cause of corruption is the lust of hoarding among the rulers. The drive to commit corruption not only comes from within, but also comes from the environment. The envy and spite of co-worker's wealth as well as the encouragement of families to buy new homes, jewelry, and cars could also trigger authorities to commit acts of corruption. Through his financial puns, the ruler traded idealism and public morals pragmatically. Third, a high-end lifestyle. Undoubtedly, the lifestyle of the upper class is always in the luxury. They live off popularity, on high incomes with little work.

With high cases of corruption in a region, it will have an impact on the damage to the system order and social dynamics. Some of the consequences that arise as a result of the actions of the corrupters are (Revida, 2003):

1) Economic system, such as the run of capital abroad, disruption to companies, disruption of investment.
2) Socio-cultural system, such as social revolution, high crime rate, demoralization, and social inequality.
3) The political system, such as the takeover of power, the loss of authority of the government, political instability, the destruction of democracy.
4) Administrative system, such as lack of administrative ability, loss of expertise, loss of state resources, limitations of government discretion, taking repressive measures.

If observed specifically, the symptoms are clearly already occurring in Indonesia. So, to avoid more harmful impacts, it is necessary for the government, NGOs, communities, and all relevant stakeholders to join hands, shoulder to shoulder and join hands to fight corruption. This research focuses on answering the question of the formulation of deliberative corruption crimes whether it is in accordance with the development of corruption cases in Indonesia or not. Through this research, hopefully the input related to the redefinition of offense corruption crimes can be changed in the next revision of the Anti-Corruption Law, which is expected to help law enforcement in preventing and eradicating corruption in Indonesia (Lubis, 2018).

This research examines and analyzes two main point, *first* concerning the effort by the government to eradicate corruption in Indonesia, and *second* the best model of offense formulation of corruption crime.

2. METHOD

A. Research Types and Approaches

This study used mixed legal method, namely descriptive qualitative method (Soekanto, 2018) and normative juridical method (Marzuki, 2017). Where the object of this research is offense formulation of corruption crime and the Focus Group Discussion under the topic "*Telaah Konsep Perumusan Tindak Pidana Korupsi Dalam Upaya Pembaharuan Undang-Undang Pemberantasan Tindak Pidana Korupsi*," Saturday, 1 September 2018, in Orchid Room, Hotel Sahid Montana II, Malang to strengthen this research. This research is an empirical (holistic/combined) normative legal research, namely the study of legal materials, both primary and secondary legal materials and assessing the legal consequences/impacts.

B. Data Sources

The source of data in this study is to use secondary data is data from library research where in the secondary data consists of 3 (three) legal materials, namely primary secondary and tertiary legal sources as follows:

1) Primary Legal Sources is legal material that is binding in the form of applicable laws and regulations and is related to the issues discussed, consists of:
   a) Criminal Code by R. Soesilo.
   b) TAP MPR No. XI/MPR/1998 on the Implementation of a Clean State from Corruption, Collusion and Nepotism.
   c) Law No. 28 of 1999 on the Implementation of a Clean State from Corruption, Collusion and Nepotism.
   d) Law No. 31 of 1999 jo Law Number 20 Year 2001 Law No. 30 of 2002 on the Corruption Eradication Commission (KPK).
   e) Law No. 46/2009 on The Corruption Criminal Court.
   f) Law No. 15 of 2002 jo Law No. 25 of 2003 on Money Laundering Crimes.

g) Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes.

2) Secondary Legal Source is legal material that explains the primary legal entity, where secondary legal material in the form of literature books, websites, and the work of scholars, consists of:
   a) Books:
      i. Introduction to Legal Research by Soerjono Soekanto.
      ii. Legal Research by Peter Mahmud Marzuki.
      iii. Criminology by Topo Santoso.
      iv. Pathology Social by Kartono Kartini.
      v. Special Crime by Aziz Syamsuddin.
      vi. Books on Legal Research.
      vii. Books on Normative Legal Research.
      viii. Book - Legal Research Method.
      ix. Documents in the Police.
   b) Journal articles include:
      i. Tinuk Dwi Cahyani and Sholahuddin Al-Fatih, "Peran Muhammadiyah dalam Pencegahan dan Pemberantasan Korupsi di Kota Batu," (*Justitia Jurnal Hukum*, Volume 4, No. 2, 2020).
      ii. Sholahuddin Al-Fatih, "Darus as an Anti-Corruption Education," (*Asia Pacific Fraud Journal*, Volume 3, No. 1, 2018).
3) Tertiary Legal Source is legal material as a complement to the two previous legal materials, namely the legal dictionary and the results of interviews or empirical observations as a support to provide a comprehensive picture both normatively and sociologically or empirically.

C. Data Collection Method

The technique used in collecting this data is taken from legal materials as normative studies, mostly obtained through legal documents, including legislation, law books, and law journals.

D. Data Processing Method

Data analysis is a process that is never finished. The data analysis process is actually a work to find themes and formulate hypotheses, even though there is actually no

definite formula to be used to formulate hypotheses. It is just that the analysis of data themes and hypotheses are further enriched and deepened by combining them with existing data sources. The data processing and analysing by prescriptive method (Marzuki, 2014) to get new formula of offense formulation of corruption crime.

E. Research Location

The location of research conducted by the author to obtain data sources, namely: Focus Group Discussion under the topic "*Telaah Konsep Perumusan Tindak Pidana Korupsi Dalam Upaya Pembaharuan Undang-Undang Pemberantasan Tindak Pidana Korupsi*," Saturday, 1 September 2018, in Orchid Room, Hotel Sahid Montana II, Malang.

3. RESULT AND DISCUSSION

A. Efforts to Eradicate Corruption

Corruption is not new in this country, and its eradication efforts are almost the age of independence itself. As mentioned in previous discussions, every government in Indonesia has sought to eradicate corruption (Lubis, 2011). The effort started from the Corruption Eradication Team in 1967 until the establishment of the KPK in 2003 (Ma'ruf, Santoso, & Mufifah, 2019; Suryani, 2015; Saifullah, 2017). KPK is an Independent institution established by the government and responsible for efforts to eradicate corruption in Indonesia. There are several efforts that can be taken in eradicating corruption in Indonesia both preventive and repressive efforts (Ma'ruf, Santoso, & Mufifah, 2019; Suryani, 2015; Saifullah, 2017).

Prevention efforts are carried out using non-penal lines, while suppression efforts are carried out through penal lines. However, the crackdown provides several points of weakness (Ma'ruf, Santoso, & Mufifah, 2019; Suryani, 2015; Saifullah, 2017), including: criminal sanctions are *ultimum remidium* (the last resort) (Erdianti & Al-Fatih, 2019), require high costs, criminal law is *kurieren am symptom* (cure symptoms) and is only a symptomatic treatment not causative because the causes of such crimes are complex and are beyond the reach of criminal law and prison is the best area for perpetrators of crimes to learn and imitate crimes from other perpetrators (Santoso & Zulfa, 2005). Thus, using

penal routes to eradicate corruption is considered less effective (Cahyani & Al-Fatih, 2020).

In view of this fact, KPK seeks to present a non-penal line that focuses on education efforts for the community through ACCH (Anti-Corruption Clearing House) (ACCH, 2016). The socialization of education encouraged by KPK in ACCH provides some content and domain to eradicate corruption for the younger generation. The content can be accessed through the internet and there are also printed forms such as picture books, journals, articles, and pocketbooks. To support this step, KPK tries to actively involve several elements of society such as students (from elementary to college level), teachers, NGOs and related officials (Haris & Al-Fatih, 2020).

In addition to efforts and direct actions through the KPK, the government has also prepared a juridical basis for the eradication of corruption crimes, for example: TAP MPR No. XI/MPR/1998 on the Implementation of a Clean State from Corruption, Collusion and Nepotism, Law No. 28 of 1999 on the Implementation of a Clean State from Corruption, Collusion and Nepotism, Law No. 31 of 1999 jo Law Number 20 of 2001 Law No. 30 of 2002 on the Corruption Eradication Commission (KPK), Law No. 46 of 2009 on The Corruption Criminal Court and Law No. 15 of 2002 *jo* Law No. 25 of 2003 on Money Laundering Crimes, which was later changed to Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes (Ismaidar & Yudi, 2019).

Although efforts through the ratification of the juridical basis for the eradication of corruption crimes are also accompanied by the establishment of anti-corruption institutions such as the KPK, with a complete tool, so that the KPK can conduct legal efforts, ranging from investigations, investigations to prosecutions, the fact that corruption cases are still found and infected the country's celebrities, moreover, lately emerged efforts to weaken the KPK institutionally and authorities. The entry of deliberative formulation of corruption in the RKUHP, is also strongly suspected as an attempt to weaken the KPK. Not to mention the interpretation of the definition of corruption that has changed after being interpreted differently by the Constitutional Court. This dynamic, seems to be a double-

edged hot ball for efforts to eradicate corruption in the country.

B. Offense Formulation of Corruption Crimes

Based on the provisions in Law No. 31 of 1999 jo. Law No. 20 of 2001, corruption crimes can be grouped into several deliberative formulations as follows (Syamsuddin, 2011):

1) Offense corruption group that can harm the country's finances/economy (Article 2 and 3 of Law No. 31 of 1999)
2) Bribery deliberation group both active and passive (Article 5, 6, 11, 12 and 12B of Law No. 20 of 2001)
3) Deliberative group corruption of embezzlement (Articles 8, 9 and 10 of Law No. 20 of 2001
4) Group offense corruption of extortion in office (Article 12e and f Law No. 20 of 2001)
5) Deliberative group related to cheating (Article 7 of Law No. 20 of 2001)
6) Conflict of interest in Procurement (Article 12 letter I of Law No. 21 of 2001)
7) Gratification (Article 12 b of Law No. 20 of 2001)

The seven types of offense formulation experienced an expansion of offense formulation (criminal acts). The expansion is in the formulation in the interpretation of the meaning against the law of Law No. 31 of 1999 *jo*. Law No. 20 of 2001 states corruption as a formal deliberation, but the understanding against the law in a corruption crime as a formal and material deliberation (Syamsuddin, 2011).

As a formal deliberation, an act can be declared as a criminal act if the act has fulfilled the deliberative formulation in the law without having to cause adverse consequences. So, although the act has not yet caused financial losses to the state, but if the act has been "able" categorized will cause state losses, the perpetrator is already punishable. Similarly, if the results of the corruption crimes have been returned to the state, but does not scorch the unlawful nature of the act (Syamsuddin, 2011). While the notion of the nature of the contrary to formal and material law refers to an act not only contrary to the prevailing laws and regulations, but also a despicable act and contrary to the sense of community justice (Syamsuddin, 2011).

The unlawful nature of formal and material law is contained in Law No. 31 of 1999 *jo*. Law No. 20 of 2001, as

formulated in the general explanation in the law. Consideration of the list of formal and material understanding in Law No. 31 of 1999 *jo*. Law. No. 20 of 2001, as follows:

1) Given that corruption occurs systematically and widely, it not only harms the country's finances and economy, but is a violation of the social and economic rights of society at large (classed as extra ordinary crime), so its eradication must be carried out in an extraordinary way.
2) Given the impact of corruption so far in addition to harming the state's finances, it also inhibits the growth and continuity of national development that demands high efficiency.
3) To respond to the development of legal needs in society, in order to make it easier to prove, to reach various modus operandi of financial irregularities or the country's economy is increasingly sophisticated and complicated.

Interpreting an offense of corruption to be a formal or material deliberation, and legal experts of corruption often dissent. There are always pros and cons that end up causing problems. Some problems related to the formulation of corruption offense in the Law on the Eradication of Corruption include: First, the involvement of the Constitutional Court in interpreting the formulation of corruption offense. Through the Decision of the Constitutional Court No. 25/PUU-XIV/2016, in the decision of the Constitutional Court revealed, "Declaring the word *'can'* in Article 2 paragraph (1) and Article 3 of the Anti-Corruption Law is contrary to the 1945 Constitution and has no binding legal force.

Reject the applicant's application for other than and the rest. Although 4 of the 9 Constitutional Judges who decided the case gave a different view or dissenting opinion, but overall, the Decision of the Constitutional Court removed the phrase "*can*" in the Law on the Eradication of Corruption. The Court (Constitutional Court) provides juridical arguments related to the matter, including (Syamsuddin, 2011):

1) The phrase word "*can*" be interpreted as an estimate or estimate. The element of harming the state's finances is no longer understood as an estimate (potential loss), but it must be understood that it has happened or real loss

in the corruption. Thus, the phrase "*can*" must be omitted, because it causes the impact of obscurity and uncertainty in suspecting a case.

2) The phrase "*can*" can be used as a tool for policy criminalization. Related to the criminalization of policies that may arise due to the principle of discretion to conduct a policy that is urgent and important to do. So, when forced the phrase "*can*" as one of the deliberative formulations of corruption, then it can result in a lot of policy makers who should be suspected of committing corruption.
3) The phrase "*can*" make corruption offense as a formal deliberation. So, this is feared to cause fear and concern in public officials. As a result, they are careful in making policies, budget absorption is minimal, work programs do not run optimally, development is stagnant, people's welfare cannot be improved. This is a domino effect of the formal deliberative formulation in the corruption.
4) The phrase "*can*" in Article 2 paragraph (1) and Article 3 of the Law on the Eradication of Corruption creates legal uncertainty and is manifestly contrary to the guarantee that everyone is entitled to a sense of security and protection from the threat of fear in Article 28G paragraph (1) of the 1945 Constitution. Feared by formal deliberations, public officials are wary, especially those who are referred to as PPK.
5) The phrase "*can*" be contrary to the principle of formulation of criminal acts that must meet the legal principles must be written *(lex scripta),* must be interpreted as read *(lex stricta),* and not multi-interpreted *(lex certa).* Because, in fact the phrase "can" is often unable to be measured, giving rise to ambiguous meanings.

In practice, Article 2 paragraph (1) and Article 3 of the Law on the Eradication of Corruption often cause problems. For example, a) regarding the law, b) elements against the law that are often ambiguous and jumbled between the concept of criminal law *(wederrechttelijk) or* civil law *(onrechtmatigedaad),* c) elements of enriching themselves, others or corporations and d) harming the state's finances. So, it is necessary to decide with a broad but strict interpretation*(strict)*and clear (*clear*). According to thrifty writers, it is still necessary to maintain the phrase word "*can*"

in the Law on the Eradication of Corruption. This is because the phrase "*can*" can be proven by several other elements, including:

1) The loss of the phrase "*can*" fundamentally change the qualifications of formal deliberations of corruption crimes into material deliberations. Consequently, if the prohibited consequences of "*harming the state's finances or the state economy*" have not or have not occurred even though the element of "*unlawfully*" and the element of "enriching yourself or others or a corporation" has been fulfilled, then it means that there has not been a crime of corruption.
2) Concerns that the phrase "*could*" potentially make a government official punishable without any wrongdoing in the form of state losses are unwarranted. Because, the Law on Government Administration has provided protection to government officials who are suspected of abusing authority that harms the state's finances through a testing mechanism to PTUN. Whereas there is or is no abuse of authority that is suspected of causing state losses will be decided based on the results of the supervision of the government's internal apparatus or inspectorate
3) By re-entering the phrase "*can*" in the amendment of the Law on the Eradication of Corruption, the formulation of corruption offense can be more widespread but strict and clear. Because in fact, the phrase "*can*" have been preceded by two other elements of the corruption, namely the element "*unlawfully*" and the element *"enrich yourself or others or a corporation*." Thus, when the element of "may harm the state's finances" has not been met, then there has been other preliminary evidence through the element of "*unlawfully*" and the element of "*enriching one's own or others or a corporation*." This is also evidence that there is no need to worry that officials arrested on charges of causing financial losses to the state or criminalizing the policy, because those who are examined by the KPK and then designated as suspects usually have fulfilled the existing corruption element.

In addition to interpreting and canceling the meaning of the phrase "*can*" in Article 2 paragraph (1) and Article 3 of the Law on the Eradication of Corruption, the Constitutional Court is also recorded to have intervened in

interpreting the formulation of corruption offense. On July 24, 2006, the Constitutional Court through Decree No. 003/PUU-IV/2006 stated the norm of Explanation of Article 22 Paragraph (1) of the Corruption Act contrary to the constitution so that it becomes a formal norm (Kompas, 2017).

Consideration of the Constitutional Judge in the first amendment related to the norm of the formulation of the phrase "*unlawfully*" is an act that is only contrary to written law, while the law is no longer written in it. This is because unwritten law creates uncertainty due to the different conditions and understandings of society and changes over time so that it will always vary and places (Kompas, 2017).

In fact, Article 15 of the Law on the Eradication of Corruption in the phrase "*evil drafting*" was also interpreted by the Constitutional Court in a case filed by Setya Novanto some time ago. The interpretation model carried out by the Constitutional Court is considered to limit the wiggle room of investigators, prosecutors, and judges in eradicating corruption in Indonesia. Moreover, we must understand the position of the Constitutional Court, which should not be a positive legislator through the interpretation they make.

In addition to the problem of interference of the Constitutional Court in interpreting the formulation of corruption offense, other problems arising from the material contained in the Law on the Eradication of Corruption itself. The second problem, related to multi-interpretation and ambiguity of the definition of corruption offense formulation, including:

1) Related to the deliberative arrangements that are regulated twice, for example Article 5 paragraph (2) and Article 11C of Law No. 31 of 1999 jo. Law No. 20 of 2001 which equally regulates civil servants who receive bribes.
2) There are contradictory articles on the issue of criminal threats, namely Article 6 paragraph (2) and Article 12 letter C of Law No. 20 of 2001.
3) There is ambiguity in Article 21 of Law No. 20 of 2001 which regulates efforts or actions to prevent, obstruct or thwart directly or indirectly against suspects with alleged corruption.

4) Blunt provisions related to the evidence are reversed in Articles 12 B, 37, 37 A and 38 B in Law No. 20 of 2001. The provision is considered barren, ambiguous, multi-interpretive and applies narrowly. With this error, the formulation that should be made to set the burden of proof is reversed, but in its implementation becomes the usual evidentiary process.

Looking at the various definitions in the Law on the Eradication of Corruption that are multi-interpreted, confusing, and interesting to be tested to the Constitutional Court, it is necessary for the government to immediately make revisions or amendments to the Law on the Eradication of Corruption. The above notes, related to some of the problems considered problematic, need to be re-formulated immediately, to provide legal certainty for law enforcement and the public of course.

The government does not need to take tactical and exclusive steps by inserting the formulation of corruption offense into the RKUHP (Penal Code Draft), because it will only weaken the KPK and efforts to eradicate corruption in Indonesia. Given the importance and urgency of redefinition of the formulation of corruption offense, then the government should immediately form a special team, which contains experts from criminal law, government law, anti-corruption NGOs as well as community representatives or organizations to make a better formulation of corruption offense.

4. CONCLUSION

This research concluded and highlighted that the background of the corruption is caused by several factors, such as lifestyles factors, environmental factors, and social environmental factors. Some of the consequences that arise as a result of the actions of the corrupters are economic system, socio-cultural system, political system, and administrative system, such as lack of administrative ability, loss of expertise, loss of state resources, limitations of government discretion, taking repressive measures. Efforts to prevent and eradicate corruption in Indonesia have been started since 1957 through an institution named the Coordinating Board of Property Reviewers. Furthermore, the government at that time commonly known as the Old Order Era re-established anti-corruption institutions in a

few years continuously, such as the birth of the State Apparatus Activities Supervisory Agency/Bapekan (1959-1962), The Committee for Retooling State Apparatus/Paran 1 (1960-1963), Paran 2/ Operation Budi (1963-1967), Command Retooling Apparatus Revolution/ Kotrar (1964-1967). The New Order era was also no less ferocious in blocking the pace of corruption. It is recorded that there are 4 anti-corruption institutions born in the New Order Era, namely: Corruption Eradication Team 1 (1967), Commission 4 (1970), Operation Control (1977-1981) and Corruption Eradication Team 2 (1982). The commitment to fight corruption is also a key point of the post-reform government. Noted, the Reform Era gave birth to 3 anti-corruption institutions, namely the Joint Team for the Eradication of Corruption Crimes (TGTPK), the Corruption Eradication Commission (KPK) and the Coordination Team for the Eradication of Corruption. Until now, the one who still exists and gets the authority to prevent and eradicate corruption, collution and nepotism (well known in Indonesia as KKN) in this country is KPK. However, corruption in Indonesia still doing as business as usual. Moreover, in the offense formulation of corruption eradication, there are quite several ambiguous and multi-interpretative norms, that can be interpreted widely by the judge. This condition is very horrible and terrible. In connection with the above conclusions, then there are some things that can be suggested by the authors and are expected to be used as material for consideration for parties related to this research, *first* the Government should provide clear and certain offense formulation of corruption, and *second*, the judges may not interpret the formulation of corruption offenses with the aim of reducing or alleviating the punishment of corruptors.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

6. ACKNOWLEDGEMENT

None

7. REFERENCES

ACCH. (2016). "Tindak Pidana Korupsi". Retrieved February 24, 2020, from KPK website: https://acch.kpk.go.id/id/statistik/tindak-pidana-korupsi

Al-Fatih, S. (2018). Darus as an Anti-Corruption Education. *Asia Pacific Fraud Journal*, *3*(1), 117–123. https://doi.org/10.21532/apfj.001.18.03.01.14

Cahyani, T. D., & Al-Fatih, S. (2020). Peran Muhammadiyah dalam Pencegahan dan Pemberantasan Tindak Pidana Korupsi di Kota Batu. *Justitia Jurnal Hukum*, *4*(2), 117–123. https://doi.org/10.21532/apfj.001.18.03.01.14.Volume

Erdianti, R. N., & Al-Fatih, S. (2019). Fostering as an Alternative Sanction for Juveniles in the Perspective of Child Protection in Indonesia. *JILS (Journal of Indonesian Legal Studies)*, *4*(1), 119–128. https://doi.org/10.15294/JILS.V4I01.29315

Haris, & Al-Fatih, S. (2020). School of Intuition as An Education for Child to Prevent Corruption in Indonesia. *TEST Engineering & Management*, *83*, 11884–11892.

Indrayana, D. (2016). *Jangan Bunuh KPK*. Malang: Intrans Publishing.

Ismaidar, I., & Yudi, P. (2019). Kajian Hukum dalam Penerapan Undang-Undang Tentang Pencucian Uang dalam Rangka Pemberantasan Tindak Pidana Korupsi di Indonesia Berbasis Nilai Keadilan. *JURNAL JUSTIQA*, *1*(1), 17-28.

Kartono, K. (2012). *Patologi Sosial*. Jakarta: Raja Grafindo Persada.

Kompas. (2017). "Putusan MK dalam Penegakan Hukum Korupsi". Retrieved August 31, 2018, from Kompas website: https://nasional.kompas.com/read/2017/02/02/20153701/putusan.mk.dalam.penegakan.hukum.korupsi

Lubis, E. Z. (2018). Dampak Melawan Hukum Dalam Tindak Pidana Korupsi. *Jurnal Administrasi Publik: Public Administration Journal, 7*(2), 107-116. https://doi.org/10.31289/jap.v7i2.1332

Lubis, T. M. (2011). *Melawan Korupsi dengan Pembatasan Transaksi Tunai*. Malang: Fakultas Hukum Universitas Brawijaya.

Ma'ruf, M. A., Santoso, G. A., & Mufidah, A. M. (2019). Peran Mahasiswa dalam Gerakan Anti Korupsi. *UNES Law Review, 2*(2), 205-215.

Marzuki, P. M. (2014). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana Prenada Media Group.

Mashabi, S. (2020). "Indeks Persepsi Korupsi Indonesia pada 2019 Naik Jadi 40". Retrieved January 9, 2021, from Kompas website: https://nasional.kompas.com/read/2020/01/23/16565951/indeks-persepsi-korupsi-indonesia-pada-2019-naik-jadi-40?page=all.

Revida, E. (2003). *Korupsi di Indonesia: Masalah dan Solusinya*. Medan: FISIP USU.

Saifulloh, P. P. (2017). Peran Perguruan Tinggi dalam Menumbuhkan Budaya Anti Korupsi di Indonesia. *Jurnal Hukum & Pembangunan, 47*(4), 459-476.

Santoso, T., & Zulfa, E. A. (2005). *Kriminologi*. Bandung: Raja Grafindo Persada.

Soekanto, S. (2018). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Press.

Suryani, I. (2015). Penanaman Nilai-Nilai Anti Korupsi di Lembaga Pendidikan Perguruan Tinggi Sebagai Upaya Preventif Pencegahan Korupsi. *Jurnal Visi Komunikasi, 14*(2), 285-301.

Syamsuddin, A. (2011). *Tindak Pidana Khusus*. Jakarta: Sinar Grafika.

Trust is that there should be no difference between what you do and say and what you think.

Umar ibn Khattab, *The Caliph*

ABOUT AUTHORS

Sholahuddin Al Fatih, S.H., M.H., is a lecturer at Faculty of Law, University of Muhammadiyah Malang, Indonesia. His main area of research is Constitutional Law, Electoral Law, and Human Rights. The author also serving as Editor in Chief *Legality Jurnal Hukum* at Faculty of Law, Universitas Muhammadiyah Malang Indonesia. He obtained his Bachelor of Law degree from Universitas Brawijaya and Master of Law degree from Universitas Airlangga. Currently, the author is pursuing a doctoral education at the Doctoral Program Faculty of Law Universitas Brawijaya, Malang, Indonesia.

RESEARCH ARTICLE

US Right of Veto Against UN Resolution on Terrorism of ISIS Foreign Militias

Annisa Farras Tsabitah[1]✉, **Khoirur Rizal Luthfi**[2]
[1,2] Faculty of Law, UPN Veteran, Jakarta, Indonesia
Jl. Rs Fatmawati, Pd. Labu, Kec. Cinere, Jakarta 12345, Indonesia
✉ annisafarrast@upnvj.ac.id

Abstract

This paper analyzes how the US proposes the right of veto in the UN-issued resolution concerning anti-terrorism, namely Persecution, Reintegration, and Rehabilitation system of foreign ISIS militants who are stranded in Syrian camps. How the veto of United States position on ISIS foreign prisoners has the potential to violate the veto provisions based on the UDHR, International Humanitarian Law, as well as the 1949 Geneva Convention and its Additional Protocols I and II 1997. This study was conducted to determine the effect of the US veto on the fate of ISIS foreign militias and the efforts and steps that could be taken to resolve the ISIS Foreign Militia problem from the perspective of international law. The research method employed in this study was juridical normative. A study found that the PRR resolution on ISIS foreign militias was canceled with the issuance of a veto by the United States. Several efforts can be made in dealing with this including maintaining the role of the PRR on foreign ISI militants detained in Syria holding camps, focusing on handling foreign ISIS militias, and countering terrorism through related conventions, such as the Universal Declaration of Human Rights (UDHR), The 1949 Geneva Convention, and Additional Protocols I and II of 1977, as well as continuing to urge all member states and all parties that all action taken against terrorism are required to meet obligations under international law, including humanitarian law, international human rights law, and international refugee law by still considering the impact of those actions.

Keywords: *UN; Right of Veto; US; Terrorism*

OPEN ACCESS

Citation: Tsabitah, A. F., & Luthfi, K. R. (2021). US Rights of Veto Against UN Resolution on Terrorism of ISIS Foreign Militias. *Law Research Review Quarterly, 7*(1), 19-42. https://doi.org/10.15294/lrrq.v7i1.44464/10.15294/lrrq.v7i1.43897.

Submitted : December 19, 2020
Revised : January 15, 2021
Accepted : February 13, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

1. INTRODUCTION

The organ of the United Nation that functions in resolving conflicts are the Security Council. The UN Security Council is one of the 6 main organs of the United Nations (UN). The UN Charter leaves the mandate to the Security Council to protect international peace and security (Wikipedia, 'Dewan Keamanan PBB', 2020), the UN Charter delegates powers to the Security Council in:

1) Investigating a situation that is dangerous to world peace.
2) Recommending procedures for peaceful dispute resolution.
3) Directing all states parties to the United Nation in terminating economic, sea, air, mail, radio communication, and diplomatic relations.
4) Carrying out the decisions of the Security Council militarily, or in other ways.

Besides its powers and functions, in carrying out its duties, the Security Council is given a right called the right of veto. The right of veto is familiar for it is the right to cancel decisions, decrees, draft regulations, and laws or resolutions. Initially, this veto power was intended to protect the interests of the founders of the UN, the countries that won World War II. Historically, the veto power has been assigned to the five permanent members of the UN Security Council including the United States, Russia, England, France, and the People's Republic of China, since they were the winner of World War II.

By law, the powers of permanent members of the UN Security Council are a given privilege. However, they also have the same obligations and responsibilities legally as other UN member states. The Charter only defines primary responsibilities for international peace and security on the side of the Security Council (Suwardi & Kurnia, 2019: 291). Article 27 paragraph 1 of the UN Charter explained that each member of the Security Council has one vote. However, where there is connection between the provisions of Article 27 paragraph 1 and paragraph 3, there are procedural and non-procedural differences in voting rights between permanent members of the Security Council and non-permanent members of the Security Council.

The United States as one of the founders of the United Nations that is also part of the UN Security Council, in its

journey, is a country that has quite often issued its privileges to draft resolutions submitted by the United Nations after Russia. Currently, data shows the US has issued 82 veto rights. One of the recent vetoes issued by the US was concerning the draft resolution proposed by Indonesia as President of the UN Security Council for the 2019-2020 period. In the four resolutions submitted, the resolutions that were not accepted were related to the anti-terrorism movement. One of the targets to be achieved is related to countering terrorism, particularly issues of persecution, rehabilitation, and reintegration (PRR) as well as women's peace. Indonesia intends to encourage a comprehensive approach to dealing with terrorism. Thus, the UN Security Council is expected not only to focus on the aspect of law enforcement but also efforts to rehabilitate and reintegrate terrorists into society (CNN, 13 October 2020). However, the US argues this resolution is still inaccurate since it does not prioritize the 'repatriation' of standard foreign militants. According to the US, the repatriation of foreign militants to their home countries is the right step, because thousands of foreign ISIS militias among them are detained in Syria and Iraq. They have to undergo integration into society after serving prison terms, and the government of the home country is asked to provide support for their families. Repatriation and accountability for crimes committed by ISIS militants are very important to prevent them from being the next generation of ISIS (Republika, 13 October 2020). Furthermore, there is the issue of the execution by Kurdish forces detaining captured ISIS prisoners.

The statement made by the Ministry of Foreign Affairs can be inferred that Indonesia views the need for consideration of the international community in eliminating the right of veto. Moreover, Indonesia also supports restrictions on the use of the right of veto, such as using veto for situations that are truly dangerous, for example, human crimes and humanitarian situations. Therefore, Indonesia supports the proposal of the Accountability, Coherence, and Transparency (ACT) group in the formulation of a Code of Conduct regarding restrictions on the use of the veto.

The basis for granting the right of veto tends to be of political interest rather than legal considerations. Thus, this makes the 5 veto-holding countries have higher sovereignty than other UN member countries. However, it does not rule

out that the veto is proposed for the sake of good and a more mature design in the future. However, the anti-terrorism movement has to be voiced and emphasized to all member countries, and efforts to overcome it need to be given special attention to achieve the welfare of the entire nation. This is because the failure of the Council to adopt a draft resolution is an important matter. It not only stifles collective efforts in dealing with the threat of terrorism but also sends a bad image signal to the Council which is not united in the fight against the specter of terrorism.

The crime of terrorism is a crime against humanity that poses a serious threat to the integrity and sovereignty of a nation. Terrorism can be a threat to national security and sovereignty as well as world peace. One of the main causes of the crime of terrorism is radicalization. Currently, there has been no clarity in formulating the term terrorism, including the United Nations. Generally, the term terrorism is divided into State Terrorism and Non-State Terrorism. However, non-state terrorism often happens in the 21st century (Riza, 2006: 47-46).

One of the main factors that cause terrorism is radicalism and religious fundamentalism as well as social injustice. This is felt by a certain group who want to realize a religious, political, or ideological goal. Thus, acts of terror become a tool used in achieving this goal by targeting civilian and state targets due to resistance to capitalism in Western countries. Several elements are categorized as terrorism. Some of the doctrines of scholars as a source of law in the classification of acts of terrorism, namely:

a) Actions of taking away human rights that are non-derogable rights.
b) Actions accompanied by violence with non-selective, random, and indiscriminate targets.
c) Actions accompanied by careful or organized planning.
d) Actions cause real fear and great unrest in society.

International regulations on terrorism are more specifically contained in article 2 paragraph 1 of the International Convention for the Suppression of Terrorist Bombings, which stated that "*Any person commits an offense within the meaning of this Convention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal devices in, into or against a place of public use, a State or government facility, a public transportation system*

or an infrastructure facility:(a) With the intent to cause death or serious bodily injury; or (b) With the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or are likely to result in major economic loss".

In solving the terrorism issues, the role of international institutions is needed, with all the tasks and authorities that have been determined, since the United Nations as an organization aims to carry out world peace. Furthermore, the role of each member and all parties is necessary to ensure that all measures are taken to combat terrorism meet obligations under international law, including humanitarian law, international human rights law, and international refugee law by taking into account the potential effects of counterterrorism act exclusively.

Previous studies related to this research article, referring to several journals, discussed the effects of the use of veto power by the United States on cases of Israeli aggression in Gaza, where the influence of the veto proposed by the United States created a never-ending conflict in the Gaza since after a resolution is given a veto, the resolution turns into a draft resolution and cannot take effect (Hardianti, Widagdo, & Nurdin, 2015). This illustrates that every decision taken by the Board will produce a significant effect. Furthermore, the discussion regarding the granting of veto rights proposed by Russia (Widagdo, Kusumaningrum, & Prasetyo, 2019; Hardianti, Widagdo, & Nurdin, 2015) in the armed conflict in Syria. This situation made several conflicts that occurred not resolved quickly due to the issuance of the veto. This is because the substance of the use of the veto and the regulations contained in article 27 paragraph 1 and 3 of the UN Charter has not found a correlation. Permanent member countries do have privileges apart from voting rights in general. However, this requires further explanation. Thus, further alternative solutions can be sought for conflicts that have arisen and have not received resolution. As the article compiled by the researchers, concerning the veto that was proposed by the United States on the resolution of terrorism by ISIS foreign militias, America needs to express its opinion and reasons for the veto issued.

A study conducted by Buana & Adwani (2018) also discussed the juridical review of the use of the United States'

veto power as the UN Security Council, as well as the function of the Security Council in general, namely maintaining international peace and security. The peace referred to as stipulated in Chapter VI and Chapter VIII of the UN Charter is the peaceful settlement of disputes and steps that can be taken if there is a threat to the peace, violation, or an act of aggression. Moreover, if there is a conflict between the obligations of UN members (under the UN Charter) and their obligations under international agreements, it is their obligations under the UN Charter that take precedence. The research conducted by Soemitro (2015) regarding the Phenomenon of ISIS Radicalism Movement in International Law concluded that ISIS as the perpetrator of terror acts continues to claim lives and triggers the fear of the international community both individually (individually and in government). However, this cannot be used as a reference in categorizing a radical movement group as a subject of international law. Supporting elements are needed to finally determine the appropriate category and then become the basis for fighting terrorism. A similar study was also carried out by Aryani (2017) regarding Russia's attack on ISIS in Syrian territory according to the National Humanitarian Law. The armed conflict that at that time was carried out by ISIS in Syria made the Syrian Government allow Russia to carry out airstrikes on its territory to attack the anti-terrorism coalition. However, this action creates a responsibility that is required to be resolved, since it raises an element of a violation of international law in human rights law.

Based on this background of the study, the authors formulated the following problems: How does the US veto influence the fate of ISIS foreign militias and the efforts and steps that can be taken to resolve the ISIS Foreign Militia problem from the perspective of International Law.

2. METHOD

A. Type and Approaches of the Research

This study is a normative juridical study, which uses the main legal material, namely examining theories, concepts, and principles, and laws related to this study (Yudiono, 2013). The approach used in this study was a qualitative approach, where the researchers investigate, find, describe, and explain social influences that cannot be explained by a

quantitative approach. Furthermore, a statutory approach was also used, which is an approach carried out by examining all laws and regulations that are related to the legal issues being handled (Marzuki, 2010: 93).

B. Data Sources

The data in this study were obtained in the form of secondary data, namely data from library research. Secondary data consists of 3 (three) legal materials, namely primary legal materials, secondary legal materials, and tertiary legal materials as follows:

1) Primary Legal Sources are binding legal materials in the form of applicable laws and regulations related to the issues being discussed. In this study, primary legal materials consist of:
   a) International Humanitarian Law.
   b) Universal Declaration of Human Rights.
   c) Article 27 paragraph 2 of the UN Charter.
   d) The 1949 Geneva Convention.
   e) The 1977 Additional Protocol I to the Geneva Conventions on the protection of victims of international armed conflict.
   f) The 1977 Additional Protocol II to the Geneva Conventions on the Protection of non-international armed conflicts.
2) Secondary Legal Sources are materials that provide an explanation of secondary legal materials, such as books, theses, published or unpublished articles, journals, newspapers, the internet, research findings, expert opinions, or law graduates who can support in solving the problems studied in this study (Soekanto, 2007: 52).
3) Tertiary Legal Sources are legal materials as a complement to the two previous legal materials, namely the legal dictionary and the results of interviews or empirical observations as a support to provide a complete picture either normatively, sociologically, or empirically.

C. Data Collection Method

The data collection technique was taken from normative study legal materials, mostly obtained through legal documents, including statutory regulations, legal books, and legal journals.

D. Data Processing Method

The data generated in this study in the form of a case study. A case study is generated to develop understanding by describing cases under the research subject. The research findings were presented in the Analytical Descriptive form. Descriptive is an explanation of the findings of research conducted to obtain a comprehensive and systematic picture. Then, analytic is a picture obtained from research based on careful analysis to obtain evidence of the formulated problem that is the background of this study.

3. RESULT AND DISCUSSION

The development of Human Rights to this day is still quite worrying. The world after the World War, expected to bring about a more peaceful situation, still shows the ongoing bloodshed nowadays. One of them is the emergence of Islamic State militant groups in Iraq and Syria. They call themselves the ISIS (Islamic State of Iraq and Syria). Its ideology follows a radical, hardline Islamic ideology that plans to establish an Islamic state in the form of a Caliphate like the time of the Prophet. ISIS did not hesitate to behead detainees themselves, one of which was the beheading of US journalist James Foley. This illustrates how humanitarian principles are still being violated, and shows an insult to human dignity (Soejipto, 2015: 1).

According to Wahid, Abdul (Sunardi & Sidik, 2004: 24-29), ISIS (Islamic State of Iraq and Syria) is a *jihadi* militant group whose existence and all its activities have developed and are known by the entire international community. All of its activities are dominated by acts of violence that disturb the international community because they are considered to disturb world security and peace. ISIS is a group that was initiated by Al Qaeda which always attempts to make large-scale expansion in its political struggle. The Sunni Wahabi-based ISIS in the Middle East region has declared its country's status as an Islamic (caliph) state which rules over all Muslims around the world. After the fall of Saddam Hussein's regime in Iraq, there have been prepared people who might create chaos and as soon as possible build an Islamic caliphate.

As a group associated with al-Qaeda, ISIS follows the Islamic Fundamentalist trend. Furthermore, as an Islamic militant group, ISIS adheres to a political and radical form

of Islam, namely thinking that Islam is a comprehensive and exclusive solution to all the world's political, economic, and social problems. Furthermore, it should be noted that ISIS is not a nationalist group operating under a religious label, but a *jihad* group committed to liberating Muslims around the world. ISIS aims to build an Islamic caliphate that covers the entire territory of Iraq, Levant, Lebanon, Syria, and others. Thus, Islam is interpreted as an ideology in politics, not a purely theological one. Therefore, the ISIS struggle was taken from outside the realm of religion which had historically been placed in secular politics. ISIS has the goal of establishing an Islamic caliphate in the country or territory they struggle with and once this local caliphate is established, the global caliphate will be pursued (El Renova, 2016).

Judging from the general description of ISIS, ISIS can be classified as a terrorist organization. According to the facts, ISIS is based on elements contained in the characteristics of terrorists, such as actions carried out individually or in groups, causing fear (terror), and the existence of certain motives. Since the defeat of ISIS by Kurdish forces under Abu Bakr Al Baghdadi in 2018, more than 9,000 family members of ISIS fighters are reportedly still in the Al-Hol camp, Northeast Syria, of which 6,500 are children (CNN, 26 March 2019).

In this regard, Syrian President Bashar al-Assad plans to indict foreign ISIS militants in his country, especially those imprisoned in Kurdish-controlled North Syria camps. Assad argued that this condition could be used as a way to reunite a divided Syria. Besides that, some of the local ISIS militants have been tried in court by Kurdish forces, but not by foreign militants since Kurds have asked the Syrian government to take responsibility for them. However, some Western countries from the International Coalition refuse to repatriate their nationals from Syria for security reasons. Then, Amnesty International stated the possibility that detainees might not reach trial, as tens of thousands of prisoners have disappeared in prison since the start of the war in 2011. Meanwhile, thousands more have been executed without trial, when others have been tortured to death. Therefore, the Security Council is trying to re-submit a resolution related to fighting against world security threats, hoping that if this resolution can be adopted, this

might become the main instrument for the Council and all member states of the United Nations, as well as the United Nations system, to build a comprehensive strategy and long term in countering terrorist acts and violent extremism that are conducive to terrorism and preventing the recurrence of terrorist acts (Liputan 6, 28 November 2019).

Under international law, foreign militants stranded in Syrian holding camps deserve to be handled by their respective countries. However, those who stated that they left their country were threatened with statelessness and several countries refused to accept them again on the grounds of threats to national security. The anticipation of former terrorism returning home but at risk of attack in the country, by making new and invisible alliances. According to UNHCR, a stateless person is a person who is stateless in any country. In the 1954 Convention Relating to the Status of Stateless Person, it was stated how everyone still provides legal protection for Stateless Person and proper treatment as a human being. The rights contained in this Convention shall be granted and shall not be discriminated against based on religion, race, or country of origin. The 1954 Convention relating to the Stateless Person stipulates that the country of residence of stateless persons is obliged to protect human rights to citizens or foreign nationals who legally reside in the territory of the state's sovereignty. However, this condition still has not found a midpoint with the actual situation (Salim, 2017: 141-155).

The Universal Declaration of Human Rights (UDHR) and regulatory instruments and conventions govern international human rights that have existed since 1948. These instruments are still being developed to this day because almost everyday reports from around the world against violations of humanitarian law continue to emerge. The classic approach to human rights is suggested by David Forstyle and Jack Donnelly. This approach explains how the evolution and development status of human rights after World War II. One of the human rights politics shows several characteristics, including:

1) The contestation between classical norms of state sovereignty with new norms of domestic standards that apply in each country.
2) Contestation between human rights formulations in the political, economic, and social fields.

3) A statement that basic human rights are different (not universal).

This principle encourages the development of Positivistic thinking, namely the idea that the regulation of rights must be carried out by state and political authorities. In positivistic thinking, sources of law have to be listed in the law and accompanied by sanctions for violations of the law. The state is a means for the protection of basic human rights. The positivistic approach becomes the basis for the concept of state sovereignty which is widely adopted by IR theory. In article 5 of the UDHR, Article 7 of the ICCPR, it is stated: "*no one shall be subjected to torture or to cruel inhuman or degrading treatment or punishment.*" In a democratic society, this idea is being seriously enforced and structures regional and national human rights frameworks and legislation that ensure that these values can be extended equally to all citizens (Soejipto, 2015: 9-13).

Terrorism according to the perspective of international law is not a simple problem, because terrorism issues can contain many aspects such as politics, economy, ethnicity, ideology, and so on. Acts of terrorism have recently had a serious impact on causalities among the civilian population. Acts of terrorism are a problem that cannot be resolved partially by each country. However, global acts of violence have to be resolved jointly by the international community in a comprehensive manner (Soejipto, 2015: 213).

Chadwick (1996), "*Self-determination, Terrorism and The International Humanitarian Law*" stated that International Humanitarian Law (IHL) can be used as a legal guide in cases of terrorism since IHL regulates the tools/weapons, the methods used, the protection of prisoners of war, as well as objects that can be protected in armed conflict. Some of the regulations in IHL include a strict prohibition on all acts aimed at spreading terror among civilians, and the Ministry of Health, as well as international affairs also prohibiting acts that are considered terrorist acts. Besides, IHL contains several regulations governing the obligation to follow up on violations of these prohibitions, as well as many regulations related to the enforcement mechanism of these obligations.

ISIS status in international law is not as a state, but as a non-state actor (Nasution, 2017). ISIS does not fight against colonial domination and foreign occupation, nor does it seek

self-determination against racist governments. Therefore, the war against ISIS in IHL does not refer to article 2 of the Geneva Convention and does not include an international armed conflict since it does not meet the criteria as an international armed conflict based on the Geneva Conventions of 1949 and Additional Protocol I of 1977.

However, under the research raised, related to foreign ISIS militants who in this case act as people who are not or are no longer bound to war and their status as hostages being held in holding camps in Syria, acts of terror along with the stipulating provisions will be explained as in the IHL, the Geneva Convention of 1949 and Additional Protocols I and II of 1977 (Kusumaatmadja, 1963: 82-83).

1) The taking of hostages is provided for in article 75 of Protocol I Article 3 of the Geneva Convention, and Article 4 paragraph (2)(b) of Protocol II.

   Article 3:

   "In the case of an armed conflict that is not of an international nature taking place within the territory of one of the participating parties. Each party to the conflict will be obliged to carry out at least the following provisions:

   (1) Individuals who do not participate actively in the conflict, including members of the war who have put down their weapons and those who are no longer participating (host de combat) due to illness, injuries, detention, or any other cause, are under, however, it is required to be treated with humanity, without any adverse distinction based on race, color, religion or creed, gender, ancestry, or any other criterion.

   For this purpose, the following actions are prohibited and will still be prohibited from being carried out against these individuals at any time and place:

   a. Violence on body and soul, especially every kind of murder, bullying, cruel treatment, and persecution;
   b. Taking hostages;
   c. Destruction of personal honor, especially humiliating and degrading treatment;
   d. Convicting and carrying out the death penalty without the precedence of a decision handed down by a court that is established regularly, which provides all judicial guarantees recognized as a necessity by civilized nations.

   (2) The wounded and the sick should be collected and cared for.

   An impartial humanitarian body, such as the International Committee of the Red Cross, can offer its

services to the parties to a conflict.
The parties to the conflict shall further endeavor to enforce by way of special agreement all or part of the other provisions of this Convention."

The implementation of the above provisions will not affect the legal position of the parties in dispute.

2) The killing of persons who are not or are no longer bound in warfare is regulated in article 75 of Protocol I, Article 3 of the Geneva Convention, and article 4 paragraph (2a) of protocol II, which reads *"against the persons referred to in paragraph I are and shall remain prohibited at any time and in any place whatsoever; Violence to the life, health, and physical or mental well-being of persons in particular murder as well as cruel treatment such as torture, mutilation, or any form of corporal punishment."*

Furthermore, Article 27 states that "protected persons under all circumstances, have the right to respect for themselves, family rights, religious beliefs, and practices, as well as their customs and habits. They have to always be treated with humanity and have to be protected against all acts of violence or threats of violence and humiliation. They also cannot be used as objects for the public."

Closely related to article 27, which requires the parties to the convention to protect and respect protected people, the provision in article 31 "prohibit coercion, both physical and spiritual, to obtain information from them. Any act causing bodily suffering or the extermination of a protected person is prohibited by the Convention." This prohibition does not only cover murder, maltreatment, and other acts which are also mentioned in article 12 Protocol I and Protocol II of Geneva Convention but also covers any other acts of violence such as using civilian or military state equipment. Therefore, it is necessary to pay more attention and appropriate steps to the fate of foreign militias if they are positioned as people who have been protected due to defeat in war and in eradicating terrorism.

One of the agenda for the UN Security Council discussion regarding "*Threats to international peace and security caused by terrorist acts*" was held on August 31, 2020, with draft resolution number S/2020/852 (UN, 2020) was not reached. The draft includes:

1) Emphasizing its decision in resolution 1373 (2001) that all Member States are obliged to ensure that everyone

who participates in the financing, planning, preparation, or act of terrorism or support of terrorist acts is brought to justice.

2) Keeping in mind its decision that all Member States should ensure that their domestic laws and regulations establish sufficient, serious criminal offenses to provide the ability to prosecute and punish the activities described in paragraph 6 of resolution 2178 (2014), and paragraph 5 of resolution 2462 (2019) in a way that reflects the seriousness of the offense.
3) Calling on the Member States to assess and investigate suspected individuals who they believe to be terrorists, including FTF suspects and their accompanying family members, entering member states of the territory, to develop and implement comprehensive risk assessments for their individuals, and to take appropriate action, including taking into account appropriate prosecution, rehabilitation, and reintegration measures, as well as emphasizing that the Member States have to ensure that they take all such actions following international law, especially international human rights law, international humanitarian law, and international refugee law.
4) Reaffirming that those who are responsible for committing or otherwise responsible for terrorist acts, and violations of law or international humanitarian or human rights violations in this context, must be held accountable.
5) Summoning on the Member States to analyze the application of national criminal charges related to terrorism, to consider whether it results in the application of criminal penalties which should reflect the gravity of the offense, when treating terrorism convicts act humanely and respect their human rights, and provide for the rehabilitation and reintegration of prisoners into a community where possible to reduce recidivism and encouraging the Member States to share relevant experiences on the application of criminal penalties for criminal offenses, rehabilitation of persons convicted of criminal offenses, rehabilitation of persons convicted of criminal acts of terrorism and measures that have to be taken to reintegrate individuals into society, including the conditions that suit of a court-

supervised exemption.

However, the American representative, Kelly Craft, at that time said that the draft resolution did not prioritize the reparation of ISIS foreign militia detainees, which was deemed inappropriate and bad enough. The following are some of the reasons America has denied the draft (UN, 2020):

1) America believes that this draft resolution is intended to address the prosecution, rehabilitation, and reintegration of terrorists, including foreign terrorist fighters and their family members. Yet, it even fails to include a reference to an important first step – repatriation to the country of origin or nationality.
2) America strongly regrets that the Security Council could be satisfied with a draft resolution that lacks the security ramifications of leaving international terrorist fighters to plan their escape from custody and leave their family members without any escape, opportunity, or hope.
3) America believes that persecution and reintegration are breeding grounds for the generation of ISIS fighters.
4) America argues that terrorist fighters and their families are easily overlooked if they are an unrelated problem.

The statement shows that America is not cooperating with the other fourteen councils in eradicating the conditions of foreign militias being held in Syria. America considers that the benefits of rehabilitation and reintegration programs are still varied, ranging from risks and needs, including psychosocial, educational, and family.

One of the statements in another UN resolutions, namely Resolution 2483 (UN, 2019), regarding the threat of terrorism, it is stated that "Recognizing that prisons can be a potential incubator for radicalization for terrorism and terrorist recruitment, and the proper assessment and monitoring of people convicted of terrorist offenses is essential to reducing terrorists' chances of attracting recruits, and also recognizing that Member States may need to continue to engage with offenders upon release from prison to avoid recidivism, following relevant international law and taking into account, where appropriate, the UN Standard Minimum Rules for the Treatment of Prisoners, or the "*Nelson Mandela Rules*." It also states that "*Given the importance of the Counter-Terrorism Executive Directorate (CTED) to include in CTED country assessments, where*

appropriate, information on Member State efforts to address the issue of trafficking in persons and its relationship to sexual violence in conflict and post-conflict situations perpetrated by terrorist groups as part of their strategic and ideological objectives, and used as a tactic by certain parties for armed conflict, including non-state armed groups designated as terrorist groups."

The ISIS group is considered to have violated international human rights law since it has carried out attacks without any principle of discrimination between the civilian population and the military. It also has exploited children and women. Thus, ISIS can be tried by national courts as long as the country is deemed "*capable and willing*:" to prosecute them. However, if the national state is deemed unable and willing to prosecute international human rights violators, the International Criminal Court (ICC) has the competence to prosecute perpetrators of international human rights violations in the Iraq and Syria conflicts.

Therefore, in facing this situation, the Security Council seeks to increase the role of PRR, namely Persecution, Rehabilitation, and Reintegration of ISIS foreign militant prisoners who cannot return to their country. The conviction of the perpetrators of terrorism is an important step in maintaining security stability in the future. The pattern of punishment might be different, that is, all measures are taken to maintain a safe and humane environment in the prison. The means that help to counter radicalization and the recruitment of terrorists will be developed. The pattern of correctionalization is carried out to prevent further terrorist radicalization in prisons and is expected to be able to foster and educate detainees better. However, the implementation of the concept of social rehabilitation and reintegration has not yet shown optimal results. One of the reasons is that at the stage of coaching terrorist convicts, many recidivists have repeated their actions.

There are three main points of thought about the goals to be achieved from a punishment, namely:

1) Correcting the criminal's personality.
2) Making people deterred from committing crimes.
3) Making certain criminals incapable of committing other crimes, that is criminals who have otherwise been irreparable.

The terrorist convict coaching aims to eliminate radical

elements in terrorist teachings. Due to its formation through recruitment and formation in several places, the teachings given are quite firmly entrenched. Eradicating the criminal act of terrorism does not mean eliminating the life of the perpetrator of the crime, but rather eliminating the causative factors of terrorists in their actions. Thus, a way to eliminate these causative factors is to carry out coaching in a correctional institution.

The terrorist convict coaching is also a demand for international interests since juridically, this crime also threatens the security of the world. In several points in Resolution 2490 on Threats to World Security and Peace, the United Nations welcomes the great efforts of the Iraqi Government to defeat ISIL and calls for assistance from the international community to ensure that ISIL members are held accountable for their crimes in Iraq and Syria, as well as wherever these crimes against humanity occur.

In dealing with acts of terrorism, the UN has also made several efforts. The General Assembly has held actions and international cooperation to prepare agreements and actions through the Security Council. The result is the issuance of 12 conventions on terrorism which have been approved by 185 countries as follows:

1) Convention on Offences and certain Other acts Committed on Board Aircraft ("*Tokyo Convention*", 1963-Safety of Aviation).
2) Convention for the Suppression Unlawful Seizure of Aircraft ("*Hague Convention*", 1970 – Aircraft Hijacking).
3) Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation ("*Montreal Convention*", 1971 – applies to acts of Aviation sabotage such as bombings aboard aircraft in flight)
4) Convention on the Prevention and Punishment of Crime Against Internationally Protected Persons (1973 – outlaw attacks on senior government officials and diplomats).
5) International Convention Against the Taking of Hostages ("*Hostages Convention*", 1979)/
6) Convention on the Physical Protection of Nuclear Material ("*Nuclear Materials Convention*", 1980 – combats unlawful taking and use of nuclear material)/
7) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil

Aviation, supplementary to the Convention for the Suppression of Unlawful Acts Against the Safety of Civil aviation (Extends and Supplement the Montreal Convention on Air Safety, 1980).

8) Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, (1988 – applies to terrorist (1988 – applies to terrorist activities on ships).
9) Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelve (1988 – applies to terrorist activities on fixed offshore platforms).
10) Convention on the Marking of Plastic Explosives for Detection (1991 – provides for chemical marking to facilitate detection of plastic explosives, e.g., to combat aircraft sabotage).
11) International Convention for the Suppression of Terrorist Bombing,1997; UN General Assembly Resolution.
12) International Convention for the Suppression of the Financing of Terrorism, 1999.

Besides those 12 conventions, the United Nations has also established the United Counter-Terrorism Implementation Task Force (CTITF) in July 2005 to ensure all coordination and coherence in the effort to fight against terrorism. Supports were provided by member countries. Furthermore, after the meeting, 23 CTITF members joined to collaborate.

Apart from the aforementioned efforts, other efforts made by the United Nations include paving the way for cooperation between the authorities with financial matters or world financial institutions to supervise funds obtained by terrorists to carry out their actions, as well as countries or parties that provide assistance funds to commit terrorism crimes. Therefore, the UN General Assembly established the *International Covenant for the Suppression of the Financing of Terrorism* which was put into effect in early 2002 (Islami, 2017: 183-186).

The United Nations is the holding of all growing international organizations. Several bodies are formed under it such as The General Assembly, The Security Council, The Economic and Social Council, The Trusteeship, The International Court of Justice, and The UN Secretariat.

Article 103 of the Charter of the United Nations explains that in the event of a conflict or conflict between the obligations of UN members (according to the UN Charter) and their obligations under international agreements, then their obligations under the UN Charter take precedence. The supremacy also applies to international treaties that were concluded after the entry into force of the UN Charter. Meanwhile, international treaties that were issued before the UN Charter cannot apply. Besides that, in international law, there are alternatives used to keep working on the fate of the foreign ISIS militias. In Resolution 2474, it was stated that "*each state party to the 1949 Geneva Convention to respect and ensure respect for the convention in all situations*." Thus, related to the eradication of terrorism, referring to the Geneva Convention of 1949 and Additional Protocols I and II of 1977 can be an alternative (Islami, 2017: 174-175).

Eradicating terrorism requires multilateral cooperation and a strong national defense system. Thus, crimes on humanity can be classified as state and non-state actors. As in the draft UN resolution that cannot be implemented, all member states continue to supervise and guard against terrorism and pay attention to the fate of their citizens who are detained in holding camps in Syria by Kurdish forces. Article 49 of 1949 Geneva Convention I, it is stated that "each member state is obliged to establish regulations related to armed conflict, seek and follow up people who commit violations, and ensure fair action to the violators who have been found." This regulation requires member states to play an active role in upholding the principles of international law by upholding human values. Therefore, under any circumstances, including dangerous conditions, all will adhere to human values.

4. CONCLUSION

This research concluded and emphasized that the influence of the US veto on the fate of foreign ISIS militias and the efforts and steps that can be taken to resolve the issue of ISIS Foreign Militias from the perspective of International Law. The influence of the US veto on the fate of ISIS foreign militias is that the ISIS foreign militants detained by Kurdish forces are still in holding camps on Syrian territory without any further handling. International Amnesty maintains the possibility that detainees may not reach trial, as tens of

thousands of detainees have disappeared in prison since the beginning of the war in 2011, thousands more have been executed without trial, while others have been tortured to death. However, the need for conducive handling in preventing radicalization into terrorism, recruitment of members, financial support for terrorists, forms of promotion carried out through politics, and religion, et cetera cannot be tolerated. To put an end to and resolve these armed conflicts, gender participation and equality, facilities for investigation, prosecution, reintegration, and rehabilitation are required. Efforts and actions that can be carried out on ISIS foreign militias from the perspective of international law include as follows: *First,* prioritizing the role of the PRR on ISIS foreign militants detained in Syrian holding camps. The conviction of the perpetrators of terrorism is an important measure in maintaining security stability in the future; *Second,* enacting alternatives used to keep working on the fate of the ISIS foreign militias. Resolution 2474 stated that "each state party to the 1949 Geneva Convention has to respect and ensure respect for the convention in all situations." Thus, referring to the Geneva Convention of 1949 and Additional Protocols I and II of 1977 can be an alternative to the eradication of terrorism. Foreign prisoners have no right to be tortured or treated cruelly and inhumanly or to be humiliated. Besides the efforts and measures taken from an international legal perspective, there are also several steps that the UN can pay attention to in handling ISIS foreign militia prisoners, including the following: First, United Nations can continue to carry out surveillance and monitoring, in particular, the United Nations Office for Counter Terrorism (UNOCT) and UNODC, as well as other Global Compact entities. They can continue to provide technical assistance and capacity building to the Member States to support them in strengthening their responses to the linkages between international terrorism and organized crime, whether domestic or transnational, including by developing instruments that can help tackle the radicalization of terrorism in prisons and assess the risk of terrorist recruitment, being consistent with international law, and encouraging the Counter-Terrorism Committee (CTC). With CTED support, they can continue cooperating in facilitating technical assistance and capacity building, including by

sharing information, with relevant bilateral and multilateral technical assistance providers; Second, the Security Council in carrying out its function of maintaining world peace and security continues to encourage all member states and all parties, that all actions are taken to eradicate terrorism have to meet the obligations under international law, including humanitarian law, international human rights law, and international refugee law by considering the impact of the action.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Adi, D. W. S. (2018). Penggunaan Hak Veto oleh Rusia dalam Konflik Bersenjata di Suriah. *Doctoral Dissertation*, Universitas Brawijaya.

Aryani, V. (2017). Serangan Rusia Terhadap Islamic State of Iraq And Syria (ISIS) Di Wilayah Suriah Menurut Hukum Humaniter Internasional. *Kumpulan Jurnal Mahasiswa Fakultas Hukum*, 1-15. http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/2266

Buana, T. Z. S., & Adwani, A. (2018). Tinjauan Yuridis Terhadap Penggunaan Hak Veto Amerika Serikat Sebagai Anggota Tetap Dewan Keamanan Perserikatan Bangsa-Bangsa. *Jurnal Ilmiah Mahasiswa Bidang Hukum Kenegaraan*, *2*(3), 677-688. http://www.jim.unsyiah.ac.id/kenegaraan/article/view/13576

Chadwick, E. (1996). *Self-determination, terrorism and the international humanitarian law of armed conflict*. Leiden: Brill Nijhoff.

Diantha, I. M. P., & Mahartayasa, M. (2016). Hak Veto Dewan Keamanan Perserikatan Bangsa-Bangsa dalam Kaitan dengan Prinsip Persamaan Kedaulatan. *Kertha*

Negara: Journal Ilmu Hukum, *4*(3), 1-7. https://ocs.unud.ac.id/index.php/Kerthanegara/article/view/20791

El Renova, E. S. (2016). *Kedudukan Islamic State of Iraq and Syria (ISIS) dalam Hukum Internasional*. Lampung: Universitas Lampung.

Hardianti, S. D., Widagdo, S., & Nurdin, N. (2015). Akibat Penggunaan Hak Veto oleh Amerika Serikat terhadap Kasus Agresi Israel di Gaza. *Jurnal Hukum Universitas Brawijaya*, 1-20. http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/985/974

Hasibuan, H., Sudarsono, S., Nurjaya, I. N., & Sugiri, B. (2017). Radicalization in the Teaching Religion and Its Relations with Criminal Acts of Terrorism. *Brawijaya Law Journal*, *4*(2), 161-174.

Islami, M. N. (2017). *Terorisme Sebuah Upaya Perlawanan*. Yogyakarta: Pustaka Pelajar.

Kusumaatmadja, M. (1963). *Konvensi Djenewa Tahun 1949 mengenai Pelindungan Korban Perang*. Bandung: Dhiwantara.

Marzuki, M. P. (2010). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group

Nasution, A. R. (2017). Penegakan Hukum Terhadap Kejahatan Terorisme Sebagai 'Extraordinary Crime' dalam Perspektif Hukum Internasional dan Nasional. *Deliberatif*, *1*(1), 1-23. https://ojs.uscnd.ac.id/index.php/deliberatif/article/view/7

Riza, S. (2006). *Dimensi Internasional Terorisme*. Jakarta: Penerbit Spektrum.

Salim, H. R. (2017). Perlindungan Hukum Terhadap Stateless Person di Indonesia. *Novum: Jurnal Hukum*, 4(1), 141-155. https://doi.org/10.2674/novum.v4i1.20919

Soejipto, A. W. (Ed.). (2015). *HAM dan Politik Internasional: Sebuah Pengantar*. Jakarta: Yayasan Pustaka Obor Indonesia.

Soekanto, S. (2006). *Pengantar Penelitian Hukum*. Jakarta: UI Press.

Soemitro, D. P. (2015). Fenomena Gerakan Radikalisme ISIS dalam Hukum Internasional. *Jurnal Hukum dan Bisnis (Selisik)*, *1*(2), 129-141. https://doi.org/10.35814/selisik.v1i2.635

Soeprapto, S. (1995). *Hubungan Internasional, Sistem, Interaksi dan Perilaku*. Jakarta: PT. Raja Grafindo Persada.

Suwardi, S. S., & Kurnia, I. (2019). *Hukum Perjanjian Internasional*. Jakarta: PT. Sinar Grafika.

Wahid, A., & Sidik, M. I. (2004). *Kejahatan Terorisme: Perspektif Agama, HAM, dan Hukum*. Bandung: Refika Aditama.

Widagdo, S., Kusumaningrum, A., & Prasetyo, D. A. (2019). *Pengantar Hukum Perjanjian Internasional*. Malang: Universitas Brawijaya Press.

Yudiono, S. (2013). *Metode Penelitian*. Lampung: Universitas Lampung.

Laws and Regulations

International Humanitarian Law.

The 1949 Geneva Convention.

The 1977 Additional Protocol I to the Geneva Convention on the protection of victims of international armed conflict.

The 1977 Additional Protocol II to the Geneva Convention on the Protection of non-international armed conflicts.

The UN Charter.

Universal Declaration of Human Rights.

Other Sources

Allen, Elizabeth F. Civil Liberty Woes When Dealing with Uncivil Foes: The Effect of Civil Liberties and Human Right on Counterterrorism Operations. Naval War College Newport RI Joint Military Operations Dept, 2014. Accessed on 16 December 2020 at 11.33 WIB.

AS Veto Resolusi PBB Milisi Asing ISIS. https://www.cnnindonesia.com/internasional/20200901183417-134-s541699/as-veto-resolusi-pbb-pemulangan-milisi-asing-isis. Accessed 13 October 2020 at 13.12 WIB

Dewan Keamanan Perserikatan Bangsa-Bangsa. https://id.wikipedia.org/wiki/Dewan_Keamanan_Perserikatan_Bangsa-Bangsa#:~:text=Dewan%20Keamanan%20PBB%20adalah%20salah,menjaga%20perdamaian%20dan%20keamanan%20internasional.&text=4.%20melaksanakan%20keputusan%20Dewan%20Keamanan,atau%20dengan%20cara%2Dcara%20lainnya. Accessed on 28 October 2020 at 00.53 WIB.

Draft Resolution UN Council S/2020/852

https://undocs.org/en/S/2020/852. Accessed on January 25, 2021, at 12.52 WIB.

Kemlu, https://kemlu.go.id/portal/id . Accessed on October 13, 2020, at 23.16 WIB.

Resolusition 2490, Ancaman terhadap perdamaian dan keamanan internasional https://undocs.org/en/S/RES/2490(2019) Accessed on 6 December 2020 at 11.00 WIB

Resolution 2482, Ancaman terhadap perdamaian dan keamanan internasional https://undocs.org/S/RES/2482(2019) Accessed on December 6, 2020 at 13.25 WIB

US Veto Indonesia's Resolution in the UN Security Council, https://republika.co.id/berita/qfypti459/as-veto-resolusi-indonesia-di-dewan-keamanan-pbb. Accessed 13 October 2020 at 12.51 WIB.

Written Record UN Council S/2020/870 https://undocs.org/en/S/2020/870. Accessed on January 25, 2021, at 12.54 WIB.

ABOUT AUTHORS

Annisa Farras Tsabitah is student of the Faculty of Law Universitas Pembangunan Nasional Veteran Jakarta, Author is a final year student with a concentration majoring in International Law. She actively participates in volunteer activities outside or on campus, one of them by following the Global Volunteer in Thailand, became a teacher for approximately 6 weeks and she currently a volunteer for officer units Covid-19.

Khoirur Rizal Lutfi, S.H., M.H., currently active as a lecturer of international law at the Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta. Some of the research and community service activities he has undertaken, "P*rospects of Implementing Mutual Legal Assistance Against Transnational Tax Crimes (Study of Reciprocal Agreements between Indonesia-Switzerland)*", 2020, "*Optimalisasi Peran Bantuan Hukum Timbal Balik dalam Pengembalian Aset Hasil Tindak Pidana Korupsi*", (2020), "*Legitimasi Kebijakan Indonesia dalam Penindakan Illegal, Unreported dan Unregulated Fishing menurut Perspektif Hukum Internasional*", 2017, "*Teori Hukum Alam dan Kepatuhan Negara Terhadap Hukum Internasional*", 2012, and "*Peningkatan Pemahaman Aspek-Aspek Hukum Transnasional bagi Masyarakat di Kota Depok*", 2020.

RESEARCH ARTICLE

Law Enforcement in the Aspects of Natural Resources and Environmental

Hery Prasetyo[1], Ayon Diniyanto[2]
[1] Universitas 17 Agustus 1945 Semarang (UNTAG), Indonesia
Jl. Pemuda No.70, Pandansari, Semarang, Indonesia
[2] IAIN Pekalongan, Indonesia
Jl. Kusuma Bangsa No.9, Panjang Baru, Pekalongan, Indonesia
ayondiniyanto24@gmail.com

Abstract

Development in humans and a country is a must. However, in development must apply a balance with nature and the environment. This is important because so far, development often has the potential to contribute to damage to natural resources and the environment. In Indonesia, there are several developments that provide evidence of damage to natural resources and the environment, even though Indonesia already has legal instruments to prevent and enforce violations of environmental damage. This phenomenon actually illustrates that the policies for protecting natural resources and the environment are still not optimal for the flow of development. This research examines the relevance between development and damage to natural resources and the environment. This research also analyzes law enforcement in the aspects of damage to natural resources and the environment.

Keywords: *Law Enforcement; Development; Environment*

OPEN ACCESS

Citation: Prasetyo, H., & Diniyanto, A. (2021). Law Enforcement in the Aspects of Natural Resources and Environmental Damage. *Law Research Review Quarterly, 7*(1), 43-52. https://doi.org/10.15294/lrrq.v7i1.44244

Submitted : December 19, 2020
Revised : January 20, 2021
Accepted : February 11, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

1. INTRODUCTION

Development is a necessity for mankind in this world. Development can be said to know no time. From the past until now onwards, the world will be filled with development. Every individual or human group will tend to do physical or non-physical development. Even the state is not timid in its development agenda, especially those related to physical development. Almost all countries in the world are doing development. Developed countries carry

out massive development. Industry, mining, technology cannot be separated from the object of development. The world that is currently in the heart is a construction of development.

In Indonesia, the development phenomenon is almost the same as in other countries. Almost, every time doing physical and non-physical development. Since Indonesia's independence, it has continued into the old order era, the new order, and currently in the reform era. Development is often the country's main agenda in order to advance Indonesian people or society. Development can also be used as a pretext for realizing a large and developed country. It is not surprising if we see Indonesia's current condition which is decorated with developments, especially physical or infrastructure development. Roads, bridges, reservoirs, airports, public facilities, large buildings are increasingly mushrooming. That is part of development (Fauzie, 2019).

In fact, such a development has various obstacles. Not all development in Indonesia goes hand in hand with sustainable environmental protection. In some places, even development runs linearly with the damage to natural resources and the environment. This condition is certainly sad and also dangerous. On the other hand, development is a necessity that must be done. But on the other hand, development also has the potential to destroy natural resources and the environment, a dilemma. According to him, this is still being done even though development can destroy natural resources and the environment.

Many countries have exploited natural resources for economic or development reasons. As a result, there is damage to the ecosystem, lost forests, environmental pollution (water and air) and many more. This condition actually explains that development participates in damaging natural resources and the environment. Development which also destroys natural resources and the environment is development carried out without prioritizing environmental aspects. This is certainly very dangerous for the future of the nation's generation. Natural resources and the environment that should be preserved so that our children and grandchildren can enjoy it, the fact is that currently it has started to be reduced due to development that is not friendly to natural resources and the environment. There is a need for prevention and action to

overcome damage to natural resources and the environment (Firmansyah & Gunawan, 2007: 105-107).

Indonesia as a constitutional state in accordance with Article a paragraph (3) of the 1945 Constitution of the Republic of Indonesia must be present to resolve problems related to development due to damage to natural resources and the environment. The state through its instruments, namely law, must be present to solve this problem. The goal is for development to continue but not to damage natural resources and the environment, so that future generations can enjoy the natural resources and environment in Indonesia.

In addition, protecting and protecting natural resources and the environment from being damaged is part of realizing a sustainable life. This paper examines the extent of the relevance between development and damage to natural resources and the environment. This paper also examines the connection with law enforcement in the aspect of damage to natural resources and the environment.

2. METHOD

A. Research Types and Approaches

This research uses non-doctrinal legal research. This type of non-doctrinal legal research consists of juridical empirical legal research and sociological juridical legal research. Non-doctrinal legal research does not only examine legal aspects normatively. Studies in non-doctrinal research are examining those related to legal aspects and other things that occur in the field or in community conditions (sociology). This research uses empirical juridical research. This means that apart from examining legal aspects in this case Law Number 32 of 2009 concerning Environmental Protection and Management, researchers will also study empirical facts in the field related to damage to natural resources and the environment supported by evidence (Sonata, 2014: 27-30).

The approach in research consists of qualitative, quantitative, and mixed approaches (qualitative and quantitative). Research conducted by researchers used a qualitative approach. A qualitative approach is a research approach carried out by capturing phenomena in society. This phenomenon in society is then studied and described

in narrative form supported by arguments and analysis (Hardani, et, al, 2020: 277-278).

B. Data Sources

Sources of data in this study use primary data sources and secondary data sources. Primary data sources are the main data sources in research. Secondary data sources are sources of supporting data for primary data. The primary data sources of this research are:

1) The 1945 Constitution of the Republic of Indonesia.
2) Law Number 32 of 2009 concerning Environmental Protection and Management.

Secondary data sources in this study consisted of journals related to research themes and internet sources.

C. Data Collection Method

Data collection methods in this study were carried out by observation and document study. Observations were made by observing the symptoms related to the research theme based on data sources. Document studies were conducted to obtain data from data sources in the form of statutory regulations, journals, and data sources on the internet.

3. RESULT AND DISCUSSION

A. Relevance between Development and Damage to Natural Resources and the Environment

As mentioned earlier, development with damage to natural resources and the environment has a direct relevance. The impact of unfriendly development and not synergizing with nature can cause damage to nature and the environment. Empirical facts have proven the amount of damage to natural resources and the environment due to development (Firmansyah & Gunawan, 2007: 105-107). These empirical facts need to be proven and re-analyzed so that they can conclude that development that is not friendly to nature will cause damage to natural resources and the environment. This proof becomes a point or conclusion that development has relevance to natural and environmental damage. This evidence can be seen as follows.

First, the change in land use makes development potentially damaging to natural resources and the environment. Development, which requires land as a

medium for development, is likely to result in a land conversion. Land that was previously used as forest or green land has to be converted into dry land due to development. The conversion of land functions like this clearly damages natural ecosystems, especially green lands. It is therefore clear that land development that requires land conversion will cause damage to natural resources and the environment. The conversion of land functions should be harmonized with reforestation. Ecosystems that have been damaged due to land use change must be replaced with new ecosystems. But these solutions are very difficult to implement and only minimize the damage to natural resources and the environment (Lisdiyono, 2015: 81-82; Lisdiyono, 2007: 149-150).

Second namely the exploitation of natural resources which destroy natural resources and the environment. Exploitation of natural resources is part of development, because the impact of natural resource exploitation is for development. However, no matter how good controlling the environmental impact on the exploitation of natural resources, it will still damage the natural resources itself and the surrounding environment. The continuous exploitation of natural resources, the longer it will damage and even destroy the natural resources themselves. Even the ecosystems that exist above natural resources will be damaged due to exploitation. There has been no effective way of saying that exploitation of natural resources will be friendly to natural resources and the environment itself, but there is the opposite. The longer and more continuously exploited natural resources, the damage to natural resources and the environment will inevitably occur. The real impact is that natural ecosystems that are on the surface or in natural resources will definitely be damaged when exploitation is carried out (Lisdiyono, 2011: 14).

Third is industrial waste pollution. Industry is part of the country's development. Not surprisingly, if a country that increasingly makes industry as a main commodity, the country will be said to be more advanced. Developed countries can be seen as examples. Making industry the main sector of the economy and development. But the impact of the industry is waste. Industrial waste in the form of liquids, smoke, etc. is a problem for the sustainability of natural resources and the environment. The failure of

industrial waste management has clearly had an impact on the destruction of natural resources and the environment. No wonder the global condition is getting hotter due to pollution from motor vehicles and industrial waste. Earth's climate has become damaged due to industrial waste. Waters can also be polluted due to industrial waste, let alone deadly waste clearly damaging the water ecosystem (Lisdiyono, 2011: 14-15).

The three examples have become evidence that development has relevance to damage to natural resources and the environment. Land conversion, exploitation of natural resources and industrial waste are development activities that can destroy natural resources and the environment.

B. Law Enforcement in the Aspects of Natural Resources and Environmental Damage

Damage to natural resources and the environment must have a cause. One of the causes is the low environmental impact control. It is true that environmental impact control has not been able to fully overcome the damage to natural resources and the environment. The existence of environmental impact control can at least minimize damage to natural resources and the environment. In addition, environmental control is also a win-win solution for the stagnation of handling damage to natural resources and the environment. Without development in a world life is also a difficult thing. Therefore, it is necessary to control the environmental impact so that development can proceed with minimal damage to natural resources and the environment. This can be said as sustainable development.

The question is, why does environmental damage continue to occur on a large scale? Are environmental impact controls not implemented? Indonesia actually already has Law Number 32 of 2009 regarding Environmental Protection and Management. Article 4 states that the scope of environmental protection and management consists of (a) planning; (b) utilization; (c) control; (d) maintenance; (e) supervision; and (f) law enforcement. This means that the provisions in Law Number 32 of 2009 concerning Environmental Protection and Management can be said to be comprehensive. Moreover, there are materials related to law enforcement. Law enforcement is part of

guarding and enforcing aspects of planning, utilization, control, and maintenance.

The question is why the damage to natural resources and the environment is still happening under construction? Even though there are already regulations governing the protection and management of the environment. If there are regulations that regulate, the damage to natural resources and the environment should not occur on a large scale due to development. The statement concludes that the law enforcement of Law Number 32 of 2009 concerning Environmental Protection and Management has not been optimal. The law has not yet become a guide in carrying out sustainable development or development that is friendly to natural resources and the environment (Lisdiyono, 2014: 73-75).

Supposedly, law enforcement against development that damages natural resources and the environment can be optimal. Law Number 32 of 2009 concerning Environmental Protection and Management as a legal instrument to protect natural resources and the environment must be strictly enforced so that damage to natural resources and the environment does not occur on a large scale due to development. In fact, it can be said that the law enforcement of Law Number 32 of 2009 concerning Environmental Protection and Management has not been maximized, so that there is still visible damage to the environment and natural resources due to development.

4. CONCLUSION

This paper concluded that the relevance of development to damage to natural resources and the environment lies in the evidence. The evidence referred to is that development can potentially damage the environment. There are at least three evidence that can conclude that development can destroy natural resources and the environment if development is not carried out in an environmentally friendly manner. The three evidence are land use change, exploitation of natural resources, and industrial waste pollution. The existence of development that damages natural resources and the environment also proves that law enforcement has not been maximized. The legal instruments of Law Number 32 of 2009 concerning Environmental Protection and Management which should be able to prevent and minimize

damage to natural resources and the environment have not been optimally enforced. Therefore, Indonesia, which already has legal instruments, should protect and manage the environment including natural resources and the environment so that it is not damaged by development.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Fauzie, Y. Y. (2019). Beda Pembangunan Infrastruktur Era Soeharto Hingga Jokowi. Retrieved from: https://www.cnnindonesia.com/ekonomi/20190108205316-532-359404/beda-pembangunan-infrastruktur-era-soeharto-hingga-jokowi.

Firmansyah, M & Gunawan, D. S. (2007). Antara Pembangunan Ekonomi dan Degradasi Lingkungan. Eko-Regional. 2(2), 105-112. Retrieved from: https://media.neliti.com/media/publications/266519-antara-pembangunan-ekonomi-dan-degradasi-287bbe4e.pdf.

Hardani, et, al. (2020). Metode Penelitian Kualitatif & Kuantitatif. Yogyakarta: Pustaka Ilmu.

Lisdiyono, E. (2007). Pergeseran Substansi Kebijakan Tata Ruang Nasional dalam Regulasi Daerah (Studi Empirik di Kota Semarang). *Hukum dan Dinamika Masyarakat*, 4(2), 149-161. Retrieved from: http://203.89.29.50/index.php/hdm/article/viewFile/368/421.

Lisdiyono, E. (2011). Pengadaan Tanah untuk Kepentingan Umum Implikasinya dengan Alih Fungsi Lahan dan Penataan Ruang. Hukum Dan Dinamika Masyarakat, 9(1), 12-20. Retrieved from: http://203.89.29.50/index.php/hdm/article/viewFile/400/451.

Lisdiyono, E. (2014). Penyelesaian Sengketa Lingkungan Hidup Haruskah Berdasarkan Tanggung Jawab Mutlak atau Unsur Kesalahan. *Jurnal Spektrum Hukum, 11*(2), 67-76. Retrieved from: http://203.89.29.50/index.php/SH/article/viewFile/620/587.

Lisdiyono, E. (2015). Kebijakan Pemerintah Kota Semarang dalam Pemberian IMB (Izin Mendirikan Bangunan) Terhadap Kawasan Lindung Di Kota Semarang. *Jurnal Law Pro Justitia, 1*(1), 80-103. Retrieved from: https://ejournal.medan.uph.edu/index.php/lpj/article/view/230/97.

Republic of Indonesia. (1945). *The 1945 Constitution of the Republic of Indonesia.*

Republic of Indonesia. (2009). *Law Number 32 of 2009 concerning Protection and Environmental Management*.

Sonata, D. L. (2014). Metode Penelitian Hukum Normatif dan Empiris: Karakteristik Khas dari Metode Meneliti Hukum. *Fiat Justisia Jurnal Ilmu Hukum, 8*(1), 15-35. Retrieved from: https://jurnal.fh.unila.ac.id/index.php/fiat/article/view/283/349.

The nation behaves well if it treats the natural resources as assets which it must turn over to the next generation increased; and not impaired in value.

Theodore Roosevelt

ABOUT AUTHORS

Hery Prasetyo is a Master of Law Student at Universitas 17 Agustus 1945 Semarang (UNTAG).

Ayon Diniyanto, S.H., M.H., is a lecturer at the Department of Constitutional Law, IAIN Pekalongan. He obtained his Bachelor's and Master's degree from the Faculty of Law Universitas Negeri Semarang, Indonesia. Besides as a lecturer, he also serving as a professional researcher at Insfre Indonesia and Legal Advocacy Studies Center. He also one of the supervisors at Pesantren Riset Al Muhtada (RPM) Kota Semarang.

RESEARCH ARTICLE

Online Buying and Selling Fraud in Indonesia and Its Criminal Law Enforcement

Asif Lutfiyana
Data Privacy Research Center, Indonesia
✉ asiflutfiyana97@gmail.com

OPEN ACCESS

Citation: Lutfiyana, A. (2021). Online Buying and Selling Fraud in Indonesia and Its Criminal Law Enforcement. *Law Research Review Quarterly, 7*(1), 53-68. https://doi.org/10.15294/lrrq.v7i1.43192

Submitted : September 7, 2020
Revised : January 15, 2021
Accepted : February 2, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

The development of technology and information is quite fast, especially on the internet. Through the internet, everyone can access and find all information around the world quickly and easily. The internet spurs the emergence of creativity in all fields, especially in business. So that there emerged online businesses that provided various kinds of human needs, ranging from food, clothing, property, and other needs. Online business is very useful to reduce costs and time during the buying and selling process. In contrast to conventional business, which requires producers and consumers to meet in person, so it requires a lot of money and time. This research aims to analyse and examine the fraud case of online transactions in Indonesia and its law enforcement. The research emphasized and found that in every facility that is offered by an online business, there is always an opening for crime to emerge. Therefore, the government established a regulation, namely Law Number 11 of 2008 concerning Electronic Information and Transactions as the legal umbrella for cybercrime. However, this regulation still needs to be reviewed because it still has weaknesses in ensnaring cybercrime. Where the development of technology and information is increasingly complex. So, it requires flexible regulations on technological developments.

Keywords: *Online Transactions; Fraud; Criminal Law*

1. INTRODUCTION

The rapid development of information and communication technology needs to be considered. Even though it makes it easy for the community, sometimes that convenience can be misused as a tool to commit crimes. Crime in the field of technology itself is often referred to as cyber crime or cyber crime or in foreign languages it is known as cybercrime. Pornography, embezzlement, data theft, illegal access to a system (hacking), bank account burglary, internet system tampering (cracking), theft of credit card numbers (carding), provision of misleading information, illegal transactions of goods, are some of the frequent examples of cybercrime. happened and harmed many parties (Suyanto, 2005: 48; Fitri, Syukur, & Justisa, 2019).

The United Nations as an institution that has one of the main objectives of maintaining world peace and security, has issued a resolution No. 55/63 on December 4, 2001, in which it was agreed that all countries must work together to anticipate and fight crimes that misuse information technology.

The technology offered by computers, especially the internet, is very supportive in all fields. Especially for those who are innovative and have a business spirit, of course they will benefit greatly from the internet. With the internet network, they can open a shop without spending money, only need to create an attractive buying and selling website plus some promos and quality goods.

Online business trends or what is often known as online shops are now mushrooming, almost all types of necessities are in the online shop. any need can be fulfilled by simply clicking on the picture and transferring money. But as consumers we need to be careful, if we are easily lulled by advertisements that place products at low prices, don't be easily tempted because there are so many irresponsible people out there under the guise of a business creating fake

accounts to deceive consumers. When consumers transfer money to the seller's account, but in the end the goods ordered are not received by the buyer, even if the bad accounts are sometimes untraceable.

Humans are social creatures who cannot live alone, requiring the role of others in fulfilling their needs (Waluyo & Feryanto, 2008: 73). Human needs are getting more and more complex every day, various methods are used to fulfill them. Law was created as something related to the minimum provisions needed to bring about public order through government stipulations (Rosidawati & Santoso, 2013: 35; Prabowo, 2012; Setiawan & Achyar, 2013). The rise of cybercrima encourages the government to move quickly in dealing with the response. However, in Indonesia, cybercrime has only been regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions. Indonesia needs a legal umbrella in fighting cybercrime. Because we know that now technology is growing rapidly and there are also many humans who are not wise in managing it.

2. METHOD

The research method is used as a tool to help and answer problems in the main research through procedures and techniques using research steps, using normative research methods, by describing the science of law in the dogmatic layer of law. The type of method used in this paper is normative legal research methods, from secondary legal materials, existing literature, as well as writings in the form of theses and articles, also taking from primary legal material, namely related laws, and the Criminal Code.

3. RESULT AND DISCUSSION

A. Cybercrime: The Capture of Indonesia

The problem of cyber crime that is carried out through the internet media often occurs in Indonesia. By law, this crime is not a simple crime as it is generally,

because the tools used are computers and the internet. An informal data indicates that Indonesia is the third largest "*hacker*" country in the world. Meanwhile, for Indonesia, the "*hacker*" city was first occupied by Semaranng, then Yogyakarta (Ariyadi, 2008; Amelia, 2016).

Cyber crime is known by two terms, namely "*cybercrime*" and "*computer related crime*" which are contained in two UN conference documents regarding The Treatment of Offender in Havana, Cuba in 1990 and in Vienna, Austria in 2000. The term cyber crime itself divided into 2, namely first cybercrime in a narrow sense called a computer crime. Second, ciber crime in a broad sense is called computer related crime.

The term cyber crime in the UN X / 2000 conference in Vienna, Austria includes crimes committed:

1) By using the means of a computer system or network (by means of a computer system or network)
2) In a computer system or network (in a computer system or network) and
3) Against a computer system or network (ageinst a computer system or network)

From the above explanation, it can be concluded that the narrow meaning of cyber crime is aimed at a computer system or network. Meanwhile, in a broad sense, cyber crime includes all new forms of crime shown to computers, computer networks and their use as well as traditional forms of crime which are now being committed using or with the help of computer devices (computer related crimes) (Tianotak, 2011: 2; Karo & Sebastian, 2019).

The problems faced in the law of information and telecommunications, especially the problem of cyber crime, are very broad, because they are no longer limited by the territory of a country and can be accessed anytime and anywhere. Actually, if we look again, cyber crime is similar to crime in general, namely as a

crime and a motivation to harm others with different tactics through computers and the internet.

To better understand cyber crime, here are some forms of action, as explained by Juju & Sulianta (2010: 75), as follows:

1) Carding
   Carding is shopping using someone else's credit card, usually by stealing data on the Internet, the perpetrator is the carder.
2) Hacking
   Hacking is the activity of breaking into other people's computer programs, including on a website. There are two types of hackers, first black hackers (crackers) and there are so-called white hackers. What black hackers do is usually damage and steal from other people's web or systems. While white hackers usually tell the admin or website account owner that their website has a security hole that can be broken into.
3) Cracking
   Cracking is a hacking activity with malicious motives. Another name is the black hat hacker. If hackers only peek at security holes, here crackers are more daring to destroy the security of other people's computers and focus on enjoying the results.
4) Defacing
   Defacing is the activity of destroying website pages with an improper appearance. What is being done is solely seeking personal satisfaction, fun, revenge, political elements, and other crimes
5) Spamming
   Spamming is the act of sending e-mail that the recipient does not want, it can also be through the comment box or guest book of a site. Spamming is also often referred to as bulk email or junk e-mail, aka junk, while the sender is referred to as a spammer. An example of the event most frequently experienced by the community is the lucky draw

message sent via email and SMS (Short Message Service), although many people have been deceived.

6) Phishing
   Phishing is an activity to lure internet users to want to provide personal data information and passwords on a fake website. Usually occurs in online banking users.
7) Malware
   Malware is a "*malicious*" program in the form of viruses, worms, trojans, horses, adware, browsers, hijackers, and many more which are infected into an application, so that when someone runs the program it can damage the infected software or operating system.
8) Hijacking
   Hijacking or in Indonesian can be interpreted as piracy which is defined as one of the crimes of piracy of other people's work. The most common crime is software piracy (Saragih & Siahaan, 2016: 23).

B. E-Commerce: Potential Fraud

With the existence of information and communication science, especially the internet, the marketing and sales process can be carried out at any time without being bound by space and time. The power of e-commerce allows geophysical barriers to disappear (Pradana, 2015: 36). The ability of the internet to be able to transmit data in various forms such as text, video, animated images, sound, and others, many business people take advantage of this technology by creating websites to promote their business. All levels of society who are familiar with internet technology are already familiar with this online buying and selling activity.

The activity of buying and selling online in English is called electronic commerce (e-commerce). Can be defined as the application and application of e-business

(e-business) related to commercial transactions, such as: electronic funds transfer, SCM (supply chain management), e-marketing (emarketing), or online marketing (online marketing), online transaction processing, electronic data interchange (EDI), product promotion and others (Jauhari, 2010: 159).

The global definition of e-Commerce is all forms of trading transactions of goods or services that are carried out electronically (Jauhari, 2010: 159). In general, e-Commerce is a package in the form of technology, applications and business processes that connect companies, consumers and communities through electronic transactions and trade in goods, services and information that are carried out electronically. Another definition of E-commerce is the process of buying, selling, transferring, or exchanging products, services, or information through computer networks via the internet (Kozinets, et.al, 2010: 71). Compared to conventional business principles, e-commerce is certainly more efficient. All processes are carried out electronically, starting from suppliers, distributors, partners, consumers, can be done faster, more intensively, and can be more cost effective in transportation.

C. E-Commerce Scams

The types of cybercrime are quite diverse, as previously discussed. What often happens when buying and selling online is usually fraud. The modes range from email phishing, scam investment websites, money games, online buying and selling and many more.

In online buying and selling scams, scammers can disguise themselves as sellers and buyers. When playing the role of a buyer, scammers will ask for their goods to be shipped first, but recently this rarely happens. If the fraudster plays the role of a seller, he will usually offer goods at a lower price than the original price. Then, if the buyer has started transferring

money to the seller's account, a few moments later the seller will run away and block the buyer's account so that he cannot hold him accountable. There is another possibility, namely that the seller still sends the ordered item, but it is different or not in accordance with what was ordered.

The risk of online shopping is very high, so this can reduce consumer confidence in shopping online. The risks that are quite worried about are credit card fraud, unsuitable goods, quality of goods, delivery of goods and consumer personal data. different from conventional trading where sellers and buyers meet directly in carrying out transactions.

In order to avoid online buying and selling scams, you should be more careful and do not be tempted by cheap prices. In addition, we also need to know the mode of this type of fraud. Krisianto (2014) highlighted are some tips for avoiding online crimes, as follows:

1) Be selective in receiving information
   Even though the internet is a repository of information. However, not all the information we get from the internet is not always true.
2) Be selective in providing information
   Do not be easy to believe with people who are first known on the internet. And avoid disseminating information that you yourself have doubts about its correctness.
3) Consult with more experienced people
   Can ask the cyber crime expert or join discussions in online forums.
4) Up to date anti Virus
   Make sure your computer has an antivirus that is up to date. In order to prevent the spread of computer viruses that are accidentally installed.

D. Legal Arrangements against Cybercrime in Indonesia

The development of information technology, including the internet, presents challenges for policy

makers. The law is required to adapt to social changes that occur. The rapid development of internet use invites crime to occur.

It is easy for someone to create a fake identity to surf the internet, carry out electronic transactions anywhere, making it difficult for legal officials to determine the true identity and location of the perpetrator. No matter how strong the e-commerce system is, there is a risk of crime in the form of fraud, credit card hijacking (carding), illegal transfer of funds from certain accounts (Liddy & Sturgeon, 1988: 21).

Prior to the enactment of the ITE Law as a form of active government role. Law enforcement officers use the Criminal Code in ensnaring cyber crime cases. The provisions contained in the Criminal Code concerning cyber crime are still global. Teguh Arifiady categorized several things specifically regulated in the Criminal Code and arranged according to the level of intensity of the case (Sumenge, 2011: 105), namely:

1) The provisions relating to the theft offense in Article 362 of the Criminal Code
2) Provisions relating to the destruction / destruction of goods are contained in Article 406 of the Criminal Code
3) Offenses regarding pornography are contained in Article 282 of the Criminal Code
4) The offense regarding fraud is contained in Article 378 of the Criminal Code
5) Provisions relating to the act of entering or crossing another person's territory,
6) Crimes regarding embezzlement are contained in Article 372 of the Criminal Code & 374 of the Criminal Code
7) Crimes against public order are contained in Article 154 of the Criminal Code
8) Offenses regarding insult are contained in Article 311 of the Criminal Code.
9) The offense regarding letter forgery is contained in Article 263 of the Criminal Code

10) Provisions regarding secret leakage are contained in Article 112 of the Criminal Code, Article 113 of the Criminal Code, & Article 114 of the Criminal Code
11) Offenses regarding gambling are contained in Article 303 of the Criminal Code

Criminal acts regulated in the ITE Law are regulated in CHAPTER VII concerning prohibited acts which can be categorized into several groups, namely:

1) Criminal acts related to illegal activities.
2) Criminal acts related to interference.
3) Criminal acts facilitate acts prohibited by Article 34 of the ITE Law.
4) The criminal act of falsifying information or electronic documents is contained in Article 34 of the ITE Law.
5) Additional criminal acts are contained in Article 36 of the ITE Law.
6) Emphasis on criminal threats in Article 52 of the ITE Law.

Regarding the crime of fraud, the ITE Law regulates the crime of illegal access (Article 30), and interference to computer systems (Article 32). As well as regulating additional criminal acts in Article 36 which states that *"... intentionally and without rights or against the law commits an act as referred to in Article 27 to Article 34 which results in losses to other people*".

Previously also regulated in Article 378 of the Criminal Code which reads: "*Anyone who with the intention of benefiting himself or another person unlawfully, by using a false name or fake dignity, with trickery, or a series of lies, moves others to hand over something to him , or in order to give a debt or write off a credit, he will be punished for fraud with a maximum imprisonment of four years*".

However, the Criminal Code is still regulated in general, which is intended for conventional crimes. Meanwhile, fraud in the ITE Law has a narrower scope.

However, Law Number 11 of 2008 concerning Electronic Information and Transactions or which is

often abbreviated as the ITE Law, still has weaknesses, including:

1) The General Provisions Chapter does not clearly describe the explanation of crimes using computers.
2) The ITE Law still uses a pragmatic-political approach, instead of using a public policy approach that involves more groups, so it is not surprising that the ITE Law only regulates the use of technology that has been so widely used in various aspects of human life (Sugiswati, 2011: 62).
3) Provisions concerning the implementation of evil acts or punishable actions such as negligence and mistakes have not been included in the ITE Law, such as the matters regulated in book I of the Criminal Code are not in the ITE Law.
4) The ITE Law also does not regulate the expiration of the crime of hacking. All these criminal activities are regulated in the Chapter concerning what actions are prohibited.

The birth of the ITE Law has not been accompanied by regulations governing its formal law. The existing legal instruments in Indonesia are inadequate to ensnare cybercrime in general and hacking crimes in particular (Sugiswati, 2011: 163; Karo & Sebastian, 2019). As an effort to combat cyber crime, the following steps need to be taken (Sobri, Emigawaty, & Damayanti, 2017: 230), among others:

1) Modernizing the national criminal law and its procedural law.
2) Improve the national computer network security system according to international standards.
3) Increase the understanding and expertise of law enforcement officials regarding efforts to prevent, investigate, and prosecute cases related to cyber crime.
4) Increase citizen awareness about the problem of cyber crime and the importance of preventing these crimes from occurring.

5) Increasing cooperation between countries, be it bilateral, regional and multilateral, in efforts to deal with cybercrime.

E. Factors for the Emergence of Cybercrime

The emergence of cases of law violation through the internet media can be motivated by several factors, including:

1) The economic condition of the community, the level of community needs is increasing while the employment opportunities are also decreasing. This encourages the crime rate to increase. Crime is a portrait of the concrete relation of the development of community life which directly or indirectly has sued the condition of society (Ismail, 2009: 243).
2) The interests of business, politics, culture, religion and so on can become motives, reasons and arguments that make a person and a group of people fall for cyber crime.
3) The Indonesian legal system still provides loopholes and weaknesses in the supervision system for these crimes. So that many criminal acts cannot be ensnared by law.

4. CONCLUSION

Finally, this research highlighted and concluded that cybercrime is not a simple crime as it is in general, because the media used are computers and the internet. However, it can also be said to be similar to conventional crimes, namely both crimes and harming others. The internet makes it easier for businesses, especially online businesses (e-commerce), because it removes geophysical barriers. Various online fraud modes range from e-mail phishing, scam investment websites, money games, online buying and selling and many more. Furthermore, concerning protection against cyber crime is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions and several articles in the Criminal Code.

Especially the criminal act of fraud can be charged under Article 36 of the ITE Law and Article 378 of the Criminal Code.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Amelia, T. N. (2016). Fraud in online transaction: case of Instagram. *Journal of Advanced Management Science Vol*, *4*(4), 347-350. doi: 10.12720/joams.4.4.347-350.

Fitri, F. A., Syukur, M., & Justisa, G. (2019). Do The Fraud Triangle Components Motivate Fraud In Indonesia?. *Australasian Accounting, Business and Finance Journal*, *13*(4), 63-72. http://dx.doi.org/10.14453/aabfj.v13i4.5.

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(3), 242-247. https://ejurnal.ung.ac.id/index.php/JIN/article/view/815.

Jauhari, J. (2010). Upaya pengembangan usaha kecil dan menengah (UKM) dengan memanfaatkan e-commerce. *Jurnal Sistem Informasi*, *2*(1), 1-12.

Juju, D., & Sulianta, F. (2013). *Hitam Putih Facebook*. Jakarta: Elex Media Komputindo.

Karo, R. K., & Sebastian, A. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. *Lentera Hukum*, *6*(1), 1-14. https://doi.org/10.19184/ejlh.v6i1.9567.

Kozinets, R. V., De Valck, K., Wojnicki, A. C., & Wilner, S. J. (2010). Networked narratives: Understanding word-of-mouth marketing in online

communities. *Journal of marketing*, *74*(2), 71-89. https://doi.org/10.1509/jm.74.2.71

Krisianto, A. (2011). *Internet Untuk Pemuda: Panduan Menggunakan Internet Secara Produktif*. Jakarta: Elex Media Komputindo.

Liddy, C., & Sturgeon, A. (1998). Seamless secured transactions. *Information Management & Computer Security*, *6*(1), 21-27. https://doi.org/10.1108/09685229810207416.

Prabowo, H. Y. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal of Money Laundering Control*, *15*(3), 267-293. https://doi.org/10.1108/13685201211238034.

Pradana, M. (2015). Klasifikasi jenis-jenis bisnis e-commerce di Indonesia. *Neo-Bis*, *9*(2), 32-40. https://doi.org/10.21107/nbs.v9i2.1271.

Rosidawati, I., & Santoso, E. (2017). Pelanggaran Internet Marketing Pada Kegiatan E-Commerce Dikaitkan dengan Etika Bisnis. *Jurnal Hukum & Pembangunan*, *43*(1), 27-53. http://dx.doi.org/10.21143/jhp.vol43.no1.1507.

Saragih, Y. M., & Siahaan, A. P. U. (2016). Cyber Crime Prevention Strategy in Indonesia. *SSRG Int. J. Humanit. Soc. Sci*, *3*(6), 22-26.

Setiawan, R., & Achyar, A. (2013). Effects of Perceived Trust and Perceived Price on Customers' Intention to Buy in Online Store in Indonesia. *ASEAN Marketing Journal*, *4*(1), 26-36. https://doi/org/10.21002/amj.v4i1.2029.

Sobri, M., & Damayanti, N. R. (2017). *Pengantar Teknologi Informasi-Konsep dan Teori*. Yogyakarta: Penerbit Andi.

Sugiswati, B. (2011). Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi di Era Informasi. *Perspektif*, *16*(1), 59-72. http://dx.doi.org/10.30742/perspektif.v16i1.70.

Sumenge, M. (2013). Penipuan Menggunakan Media Internet Berupa Jual-Beli Online. *Lex Crimen*, *2*(4), 102-112.

https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/3093/2637.

Suyanto, M. (2003). *Multimedia Alat untuk Meningkatkan Keunggulan Bersaing*. Yogyakarta: Penerbit Andi.

Tianotak, N. (2011). Urgensi Cyberlaw di Indonesia dalam Rangka Penanganan Cybercrime di Sektor Perbankan. *Jurnal Sasi*, *17*(4), 20-21.

Waluyo, S., Feryanto, A., & Haryanto, T. (1977). *Ilmu Pengetahuan Sosial*. Jakarta: Grasindo.

Humans are startlingly bad at detecting fraud. Even when we're on the lookout for signs of deception, studies show, our accuracy is hardly better than chance.

Maria Konnikova

ABOUT AUTHORS

Asif Lutfiyana SH is an independent researcher at Data Privacy Research Center, Semarang Indonesia. She obtained a Bachelor of Law degree from Universitas Negeri Semarang. Since a student, she has been active in various student activities, one of which is in the student journalism unit (LEGIST Student Press Institute).

RESEARCH ARTICLE

Cybersecurity Policy and Its Implementation in Indonesia

Anggoro Yulianto
Information and Communication Technology Awareness Community Movement (*Gerakan Masyarakat Sadar Teknologi Informasi dan Komunikasi*, GEMASTIK)
✉ puttroanggoro@gmail.com

OPEN ACCESS

Citation: Yulianto, A. (2021). Cybersecurity Policy and Its Implementation in Indonesia. *Law Research Review Quarterly, 7*(1), 69-82. https://doi.org/10.15294/lrrq.v7i1.43191

Submitted : September 3, 2020
Revised : November 3, 2020
Accepted : January 10, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

The aim of national defense is to protect and save the integrity of the Unitary State of the Republic of Indonesia, the sovereignty of the state, and its security from all kinds of threats, both military and non-military. One of the non-military threats that could potentially threaten the sovereignty and security of the nation-state is the misuse of technology and information in cyberspace. This paper is intended to analyze the cybersecurity policy in Indonesian and its challenges. This paper highlighted that the threat of irresponsible cyber attacks can be initiated by state and non-state actors. The actor may be an individual, a group of people, a faction, an organization, or even a country. Therefore, the government needs to anticipate cyber threats by formulating a cyber security strategy and determining comprehensive steps to defend against cyber attacks; type and scale of retaliation, and drafting the rule of law.

Keywords: *Cybersecurity; Cybercrime; Law Enforcement; Policy*

1. INTRODUCTION

In the era of globalization, cyberspace has become the staple of human life, and connects people regardless of distance. Cyberspace is a new world brought by the internet (Mahzar, 1999: 9). Paul Wagner (2010) argues that cyberspace is outside every computer system that is connected by wire. Cyberspace also includes:

1) isolated networks (private, military companies);
2) laptops and other personal PCs connected several times (wireless, modem);
3) industrial control machines, including programmable logic controllers (PLCs);

4) industrial robots (connected to a PLC or directly to a computer);
5) home control equipment (household appliances and control units);
6) mobile devices (smartphones, PDAs); and
7) USB and other storage devices.

The virtual world displays reality, even though it is not the real one. This is a virtual world, virtual reality, a world without borders. This is what is meant by a world without borders in a way that cyberspace does not recognize national boundaries, and it removes the dimensions of space, time, and place (Purbo, 2000: 50; Islami, 2018). It enables its citizens to connect with anyone anywhere as Bruce Sterling (1992) argues: *While not exactly "real," "cyberspace" is a real place.* Everything that happens there has very genuine consequences. This "place" is not "real," but it is serious, earnest. Tens of thousands of people have dedicated their lives to it, to the public service of wire and electronic communications.

The concept of cybernation sparked hopes to bring people endless comfort, happiness, and opportunities. However, it comes with a price. Cyber security is a real and urgent need because its impact has the potential to damage or disrupt the lives of people, countries, and even the whole world (Piliang, 1999: 14-15).

The urgency of cybersecurity is all the more pressing because the internet has a certain dark side, for example it is widely perceived to provide access almost exclusively to pornography. A recently published survey showed that more than 80% of the images on the internet are pornographic. Although the survey results themselves turn out to be completely false, the observation that the internet can and does contain illegal, inappropriate or completely illegal material is perfectly legitimate. It also supports fraudulent traffickers, terrorist information exchanges, software pirates, computer hackers, and more (Barrett, 1997: 21; Rizal & Yani, 2016; Jurriëns & Tapsell, 2017).

The world has long been worried about cybercrime. In fact, one of the topics discussed at the 10th UN Congress on the Prevention of Crime and the Treatment of Offenders in Vienna, Austria, 2000 was Crime Related to Computer Networks. However, not every country has cybercrime laws, and not all of them are very worried about this

problem (only developed countries and some developing countries). This depends on how well the country develops laws and how much to do with technological advances. This was revealed at the UN Congress in Vienna:

Reasons for the lack of attention to cybercrime may include relatively low participation rates in international electronic communications, low levels of law enforcement experience and low estimates of expected public harm from e-crime (United Nations Office on Drugs and Crime, 2000).

As a developing country, Indonesia is a little behind in following the development of information technology (Nur, 1998: 34; Chasanah & Candiwan, 2020; Setyawan & Sumari, 2016), as a result of an inappropriate technology development strategy that ignores scientific and technological research. As a result, the transfer of technology from advanced industrial countries was not followed by the mastery of technology itself which turned Indonesia into a non-technology-based country. As an alternative, as Nur (1998: 5-6) said, Indonesia is a new pseudo-industrialized country.

2. METHOD

The fact that Indonesia is still lagging behind in information technology raises questions about the conditions for implementing cyber security policies in Indonesia. Therefore, this study seeks to address this issue. The object of this research is cyber security in the context of law and national defence. Aspects of this discussion include law, national defence, and an international relations perspective. We will use the theory of realism as an analytical knife to see how Indonesia reacts to this international phenomenon. Realism is a school of thought in which states compete for power in international. The study of relationships, power is one of the most widely used concepts (the main concept) as well as the most controversial and difficult to define (Perwita & Yani, 2006: 13).

3. RESULT AND DISCUSSION

A. Cyber Threat Forms and Attack

Cybercrime is a cross-border crime. Because it crosses borders and involves many countries, cybercrime is considered an extraordinary crime. As such, it is important to have multilateral agreements to address them, both at the

regional and international levels. The use of military force should be a last resort. This is because a country cannot simply use military force to carry out attacks or initiate battles. There are many things to consider such as costs and budget. The country must build cyber defence based on digital technology immediately. Some forms of cyber threats today are as follows (Ministry of Defence of the Republic of Indonesia, 2013: 25):

1) Advanced persistent threats (APT), denial-of-service (DoS), and distributed denial-of-service (DDoS) attacks are typically carried out by straining system capacity and preventing authorized users from accessing and using targeted systems or resources. These attacks represent dangerous threats to organizations that rely almost entirely on the ability of the Internet to carry out their activities;
2) The vandalism attack is carried out by replacing the victim's web page with a fake page, where the type of content depends on the criminal motive (it can be pornographic or political);
3) A malware attack is a malicious program or code that can be used to interfere with the normal operation of a computer system. Typically, malware programs are designed for financial gain or other benefits;
4) Cyber infiltration can attack a system through identification.

Authorized user and connection parameters such as password. These attacks are carried out by exploiting vulnerabilities that exist in the system. The main methods used to gain access to the system are:

1) Guess very clear passwords, such as a person's username, the name of someone's spouse or child, date of birth or anything important and related to someone or their family, so that they are easy to guess and find out;
2) Take advantage of an unprotected account. Users can also make mistakes, by not entering their password or giving their password to someone else;
3) Fraud and social engineering. For example, the perpetrator could claim and act as administrator and ask for a password for several technical reasons;

4) Listening to data communication traffic. An eavesdropper will listen to unencrypted data sent over the network via a communication protocol;
5) Trojan horses, certain spying programs and spyware are very dangerous. It can secretly record the parameters used to connect to a remote system.
6) Testing all possible permutations that can be the key to cracking a password, if a cracker knows the cipher algorithm; and
7) Espionage, this is done by recording their connection parameters using software, spyware, or multimedia devices, such as video cameras and microphones, to capture confidential information, such as passwords for accessing protected systems.

Apart from the cyber threats above, there are other types of cyberattacks. These cyberattacks can be categorized into (Carr, 2009):

1) Hardware threat, this threat is caused by the installation of certain equipment that functions to perform certain activities in a system. Therefore, the equipment is a disruption to network systems and other hardware. For example, jamming and network disruption.
2) Software threats, this threat is caused by software whose function is to steal information, to destroy information / systems, manipulate information (Corruption Information) in a system, and others.
3) Data/information threats, this threat is caused by the dissemination of certain data / information for certain motives. What is done in information warfare is considered propaganda.

B. The Role of Cyber Security in National Security

Weak cyber defences can create tensions between countries and destabilize security, create social, economic, and environmental impacts, and disrupt relations between countries (Ghernaouti-Hélie, 2009: 24; Nugraha & Putri, 2016). Cyber security has two keywords: cyber and security. Talking about cyber means talking about information, connections (telecommunications, networks), gateways (computers, devices, users), space, or space, and it is about engaging, using, or relating to computers, networks, and the internet. Meanwhile, security is usually related to assets and asset protection. Security protects assets, protects

computers, networks, programs, and data from unwanted or unauthorized access, alteration or destruction,

Computer security, cyber security, or IT security is information security applied to a computer or network. Computer security aims to help users prevent fraud or detect any fraudulent attempts in information-based systems. Information itself is non-physical. Cyber security is an effort to protect information from cyberattacks. Cyberattack in information operations means any deliberate act to compromise the confidentiality, integrity, and availability of information. This action can be in the form of physical disruption or disruption of the logical flow of the information system. Cyberattacks are attempts to disrupt information that focuses on the logical flow of information systems. National Cyber Security is a term used for cyber security related to the assets / resources of a country (Boisot, 1998: 18; Saputra, et.al, 2019; Arianto & Anggraini, 2019).

The purpose of national cyber security is the protection, domination and control of data and information. National cyber security is closely related to information operations, which involve various parties such as the military, government, state-owned companies, academics, the private sector, individuals, and the international world (Siagian, Budiarto, & Simatupang, 2018). The continuity of information operation does not only depend on cyber security itself, it also depends on physical security, which is related to all physical elements such as data center buildings, disaster recovery systems, and transmission media.

C. Cyber Security Policy in Indonesia

In terms of cyber security, Indonesia already has cyber security systems and strategies implemented by government agencies as well as official communities. Cyber security policy is coordinated by the Ministry of Communication and Information (MCI). There are three government organizations involved in cyber security in Indonesia, which are the Information Security Coordination Team, the Directorate of Information Security, and the Indonesian Security Incident Response Team on the Internet Infrastructure (ID-SIRTII) (Nugroho, Abdullah, Wulandari, & Hanafi, 2019; Saudi, 2018; Zaleski, 1999).

The Information Security Coordinating Team was formed in April 2010 to coordinate cyber security, with a focus on expertise and practice in the information and technology fields. The Information Security Directorate has the task of policy formulation and implementation, training, monitoring, evaluation and reporting in the field of information security governance. Finally, ID-SIRTII was established by the government based on the Government Regulation of the Minister of Communication and Information Technology No. 8 of 2012 to deal with security in internet infrastructure.

Meanwhile, there are two community organizations involved in cyber security in Indonesia. Acting as a support agency, the Indonesian Communications Emergency Response Team (ID-CERT) is an organization that works with the government on special cases to support the development of cyber security in Indonesia. In addition, ID-CERT also functions as a support institution for government organizations (Setiadi, Sucahyo, & Hasibuan, 2012: 111; Perwita & Yani, 2006; Slouka, 1999), such as ID-SIRTII. Another community organization is the Indonesian Academic Computer Security Incident Response Team (ID-ACAD-CSIRT), an organization for universities wishing to focus on developing security in Indonesia. ID-ACAD-CSIRT currently has 40 academic CSIRT university members.

D. Laws and Regulations Related to World Security in Indonesia

The Indonesian government has made a policy regarding the application of cyber security in its law based on Law no. 11 of 2008 concerning Information and Electronic Transactions (ITE). There are several other laws that are indirectly related to policy, but are related to this information, such as Law No. 36 of 1999 concerning Telecommunications, and Law No. 14 of 2008 concerning Freedom of Information.

In addition, the following are laws that support the implementation of cyber security:

1) Law Number 8 of 1999 concerning Consumer Protection,
2) Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia,
3) Law Number 3 of 2002 concerning State Defence,

4) Law Number 15 of 2003 concerning the Enforcement of Government Regulations in lieu of Law Number 1 of 2002 concerning Terrorism and the Eradication of Crime as Law,
5) Law Number 34 of 2004, concerning the Indonesian National Army, and
6) Law Number 25 of 2009 concerning Public Services.

Until now, government regulations as law enforcers, which support the implementation of the national information security policy, are still being processed by MCI. However, several presidential regulations have become a reference in implementing national information security policies. Some of the rules are:

1) Presidential Instruction Number 3 of 2003 concerning National Policy for E-Government Development,
2) Presidential Regulation No. 20 of 2006 concerning the National Agency for Information and Communication Technology (ICT), and
3) Presidential Regulation No. 41 of 2010 concerning the General Policy on National Defence in 2010 - 2014.

Meanwhile, MCI as an ICT regulator has released several regulations as implementation guidelines, such as:

1) Regulation of the Minister of Communication and Information Technology No. 29 of 2006 concerning Certification of Authority Implementation Guidelines,
2) Regulation of the Minister of Communication and Information Technology No. 28 of 2006 concerning the Use of the go.id Domain Name for All Central and Local Government Officials on the Website,
3) Regulation of the Minister of Communication and Information Technology No. 30 of 2006 concerning the Supervisory Committee of the Certification Authority,
4) Regulation of the Minister of Communication and Information Technology No. 41 of 2007 concerning General Guidelines for National ICT Governance,
5) Decree of the Minister of Communication and Information Technology No. 57 of 2003 concerning Guidelines for Making the Institution's E-Government Development Master Plan.

To optimize implementation efforts, the regulations issued require additional material and elaboration on implementation strategies, cooperation models, and organizations. In addition, the implementation of national

cyber defence requires coordination between institutions (Ministry of Defence of the Republic of Indonesia, 2013: 35).

E. Current Cyber Security Policies in Indonesia

Indonesia's cyber security policy began in 2007, after the issuance of the Minister of Communication and Information Technology Regulation No. 26 PER/M.Kominfo/5/2007 concerning Security of Use of Internet Protocol-Based Telecommunication Networks, which was later replaced by Ministerial Regulation of Communication and Information Technology No. 16 /PER/M.Kominfo/10/2010. This was later updated with Ministerial Regulation of Communication and Information Technology NO.29/PER/M.Kominfo/12/2010. An important aspect in regulation is the establishment of ID-SIRTII. The Minister of Communication and Information Technology has assigned a team to help control the security of internet protocol-based telecommunications networks.

The function and task of ID-SIRTII is to monitor and detect early and warn when there is interference on the network. The team also coordinates with relevant parties at home and abroad when it is necessary to secure the network. The team also provides information when threats and disturbances arise. Finally, ID-SIRTII is also working to compile a work plan (Article 9 of the Minister of Communication and Informatics Regulation No. 29/PER/ M.Kominfo/12/2010). According to Hasyim Gautama, the cybersecurity legal framework in Indonesia is based on Law No. 11 of 2008 concerning Information and Electronic Transactions, Government Regulation No. 82 of 2012 concerning the Application of Electronic Systems and Transactions, as well as ministerial circulation letters and ministerial regulations (Ardiyanti, 2014).

Apart from the initiation of laws related to cyber security, to ensure legal certainty in the development of cyber security, the government enforces a national cyber security framework. However, the legal framework for dealing with cybercrime is still weak. Although there are laws that prohibit any form of attack or tampering with electronic systems, no law that specifically regulates and contains cybercrime is available. Meanwhile, cybercrime is evolving and progressing rapidly, making it difficult for law enforcement to handle it (Sterling, 1992; Sudarsono, 1992).

F. Implementation of Cyber Security in Indonesia

The way of handling cyber security in the framework of state defence is still sectoral, not well coordinated or not yet integrated. As stated by the Secretary General of the Ministry of National Education Eris Herryanto (2011), the cyber defence concept applied by the MoD and the Indonesian National Army is still sectoral, not comprehensive as a unit (Herryanto, 2012; Adrdiyanti, 2016).

Therefore, the Ministry of Defence formed a cyber defence operations center team to deal with cybercrime as well as to secure and protect countries in cyberspace. The establishment of the Cyber Defence Operations Center in the national cyber security policy is intended to build a universal defence system, which involves all citizens, territories, and other national resources, and to uphold state sovereignty, as well as to protect the territory. integrity and security of the entire nation from cyber threats.

One of the alternative policies is to place cyber security in the context of defence. Several policies that have been implemented are also in the context of defence. The Cyber Defence Operations Center, as described above, is one of them. The center has a working team formed in 2010 that draws up plans to form an information security incident management team (Alwajih, 2014; Nur, 1998).

4. CONCLUSION

Indonesia already has several policies that regulate cyber security; however, the nature of the policy is general in nature (*lex generalis*, and therefore not specific (*lex specialis*). As a result, the implementation of cyber security has not been effective. To be effective, the government needs to make it specific. and, together with all stakeholders, continue to socialize it. Therefore, the government needs to take the implementation of cyber security more seriously to anticipate cyberattacks Singapore and Malaysia, among ASEAN members, already have specific cyber security policies, and this is in line with the potential threats. Indonesia, on the other hand, does not have a special agency with full authority to manage and handle cyber security, yet. However, even without a special institution, the government must still be able to establish one of its structures or institutions to become the leading sector. This

shows us that the implementation of cyber security is diffuse and that the role of government in cyber defence is small. There are individuals who try to violate norms and laws, break rules and regulations, or take control of the security of information and physical assets for material or non-material benefits. Therefore, the government needs to make some serious efforts to anticipate cyber threats and attacks and save Indonesia's cyber defence from being targeted by irresponsible parties.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Alwajih, A. (2014). Dilema E-Democracy di Indonesia: Menganalisis Relasi Internet, Negara, dan Masyarakat. *Jurnal Komunikasi*, *8*(2), 139-152.

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *5*(1), 95-110. https://doi.org/10.22212/jp.v5i1.336.

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13-30. http://dx.doi.org/10.33172/jpbh.v9i1.497.

Chasanah, B. R., & Candiwan, C. (2020). Analysis of College Students' Cybersecurity Awareness in Indonesia. *SISFORMA*, *7*(2), 49-57. https://doi.org/10.24167/sisforma.v7i2.2706.

Islami, M. J. (2018). Tantangan dalam implementasi strategi keamanan siber nasional indonesia ditinjau dari penilaian global cybersecurity index. *Masyarakat*

Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi, *8*(2), 137-144. http://dx.doi.org/10.17933/mti.v8i2.108.

Jacob, T. (1993). *Manusia, Ilmu dan Teknolog.* Yogyakarta: PT Tiara Wacana.

Jurriëns, E., & Tapsell, R. (Eds.). (2017). *Digital Indonesia: Connectivity and Divergence*. Singapore: ISEAS-Yusof Ishak Institute.

Nugraha, L. K., & Putri, D. A. (2016). *Mapping the Cyber Policy Landscape: Indonesia*. London: Global Partners Digital.

Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi, H. (2019). Keamanan Big Data di Era Digital di Indonesia. *Jurnal Informa*, *5*(1), 28-34. https://doi.org/10.46808/informa.v5i1.65.

Nur, M. (1998, August). Dilema Pengembangan Infrastruktur Informasi Indonesia. *Info Komputer*, *XII* (8), 27-39.

Perwita, A.A., & Yani, Y. M. (2006). *Pengantar Ilmu Hubungan Internasional.* Bandung: PT Remaja Rosdakarya.

Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61-78.

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). *Central European Journal of International & Security Studies*, *13*(4), 104-120.

Saudi, A. (2018). Kejahatan Siber Transnasional dan Strategi Pertahanan Siber Indonesia. *Jurnal Demokrasi dan Otonomi Daerah*, *16*(3). 165-256.

Setyawan, D. P., & Sumari, A. D. W. (2016). Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives. *Jurnal Penelitian Politik*, *13*(1), 1-20. https://doi.org/10.14203/jpp.v13i1.250.

Siagian, L., Budiarto, A., & Simatupang, S. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Peperangan Asimetrik*, *4*(3), 1-18.

Slouka, M. (1999). *Ruang yang Hilang: Pandangan Humanis tentang Budaya Cyberspace yang Merisaukan.* Bandung: Mizan.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books.

Sudarsono, J. (1992). *Ilmu, Teknologi, dan Etika Berprofesi: Pandangan Sosial Politik.* Jakarta: Masyarakat Jurnal Sosiologi, FISIP UI-Gramedia.

Zaleski, J. (1999). *Spiritualitas Cyberspace: Bagaimana Teknologi Komputer Mempengaruhi Kehidupan Keberagamaan Manusia*. Bandung: Mizan.

I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image.

Stephen Hawking

ABOUT AUTHORS

Anggoro Yulianto is an activist and community empowerment activist. Currently, his activities assist the community by increasing public awareness of information technology and its impacts. Anggoro is actively advocating for various cases related to data privacy, cybersecurity, and technology.

RESEARCH ARTICLE

Misuse of Credit Cards or Carding in Indonesia: How is the Law Enforced?

Adib Nor Fuad
Indonesian Technology Law Society Movement
✉ adibnorfuad@gmail.com

OPEN ACCESS

Citation: Fuad, A. N. (2021). Misuse of Credit Cards or Carding in Indonesia: How is the Law Enforced?. Law Research Review Quarterly, 7(1), 83-96. https://doi.org/10.15294/lrrq.v7i1.43165

Submitted : October 13, 2020
Revised : December 23, 2020
Accepted : January 15, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

Misuse of credit cards or cards is a negative impact of the times, the advancement of the internet, and the increasingly sophisticated information technology that has resulted in e-commerce activities in countries around the world including Indonesia. Several carding crime cases in Indonesia have troubled many credit card users. This research aims to analyze and examine the criminal law enforcement on misuse of credit cards in Indonesia. This paper highlighted and found that in overcoming crimes in cyberspace, the government issues special regulations for crimes in which the action uses electronic devices and internet networks, namely the Republic of Indonesia Law No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 1 of 2008 which regulates Information and Electronic Transactions or ITE. This regulation aims to suppress carding crimes that are increasingly happening in Indonesia.

Keywords: *Cybercrime; Misuse of Card; Criminal Law*

1. INTRODUCTION

Changes in times and technological developments are two things that are basically inseparable and are directly proportional to each other. Therefore, the more advanced an era is, the more technology used in that era will be developed, because it is based on the human mindset who always wants to create new things to facilitate every human job itself. The presence of the progress of the times has a major influence on various aspects of human life, both positive and negative aspects (Suseno & Barmawi, 2004).

Human awareness to get education and knowledge, brings these humans to always experiment and compete in developing technology in this modern era, such as computer and internet devices which were originally created for military or defence needs and have now been developed and are increasingly easy for all people to feel the product of an advance in human thought in the field of technology. The sophistication of computer technology has provided conveniences, especially in helping human work (Hermawan, 2015; Pirog & Roberts, 2007). The positive impact of advances in information technology can be seen in everyday life. Among other things, the convenience in daily work. The simplest example, we can see in the Word Processor program, such as Microsoft Word, Open Office. Besides, one of the products of science and technology is information technology or what is commonly known as telecommunication technology which has used the internet network. Telecommunication technology has helped mankind to interact with humans in other communities more easily, in the sense that this can be done without leaving the place or community where it is located and this activity can be done anywhere and anytime (Wahid & Labib, 2005).

The presence of the progress of the era is impactful negative users. Related to the existence of trading transactions via the internet or online, the crimes that are felt by users that often occur in Indonesia, one of which is a theft whose object is a card or what is often referred to as carding. Carding is fraud on a credit card, the perpetrator looks for information or someone's credit card number data that is still valid, with that the perpetrator can misuse it for his personal interests, such as spending on online media where the bill is charged to the original owner of the credit card, while the perpetrator is called a carder (Indradi, 2006; Pujiuono, 2020; Hartono, 2013). Based on the crime, the legal owner of the credit card will lose the money or balance on the credit card because it was misused by the criminal. by stealing the credit card owner's credit card account. This kind of account theft can be done by breaking through the security of online shops that the victim has previously made transactions with. If these online shops are not equipped with stronger security, more and more credit card accounts can be stolen by the perpetrator.

Referring to the facts of cybercrime that often occurs in Indonesia, we can conclude that cybercrime is a serious threat in the non-traditional security sector. Where a crime that uses computer devices and internet networks (cybercrime) in Indonesia, has entered the highest order in the world.

The term security is currently known as one of the capabilities of a country in defining the concept of a threat, which focuses on military aspects in its resolution. As stated by Walt, security studies are a phenomenon of war which is defined as, the study of threat, use, and control of the military force (Indradi, 2006; Fuady, 2005; Abidin, 2017). However, after the end of the cold war, the term security underwent a change in meaning, that security includes broader aspects such as environmental, social, cultural, human rights, economic and so on. This change in the concept and meaning of security, is due to the increasing progress that has occurred, such as globalization with a revolution in the scope of communication technology that allows no distance and is supported by the easier means of transportation in the world. This condition affects the development of problematic issues in global politics, including security issues in Indonesia.

In addition to the threat and security instability due to the fast pace of technological development at this time, the people's need for convenience in carrying out daily activities has made credit cards a payment instrument that is increasingly popular in the world community and even Indonesia. Credit card as a means of payment is a type of APMK which has been in use for the longest time in this country since the 1980s. Initially, credit card holders were still limited to certain social groups and their use was intended for special payments. This development was actually driven by various factors relating to ease of use, practicality and cardholder self-image (Muhammad & Murniati, 2000; Ahmad, 2012). Therefore, it is necessary to have special handling in preparing and dealing with crimes committed by individuals who have special expertise in the field of technology.

2. METHOD

The author uses the case study method by taking the Carding cases which is currently rife in Indonesian society,

and with the normative juridical method, which is based on the main legal material by examining the laws and regulations related to this research. In sampling was not carried out on people, but library materials, especially related to information regulations and electronic transactions. The data used are secondary data. Secondary data comes from library materials and legal materials that are accurate and valid. How to identify problems by collecting library data in the form of archives, official documents, other library data that is closely related to research problems, namely Analysis of Credit Card Abuse or Carding in Indonesia. The final result of data processing are qualitative, then analyzed by qualitative-normative methods, the method of interpretation in law. It is hoped that the results of this writing can be useful and as a reference for the knowledge of other readers.

3. RESULT AND DISCUSSION

A. Credit or Carding Misuse as Cybercrime in Indonesia

The term Carding is quite widely used in activities related to credit cards, for example e-commerce transactions. Why is it called carding, because in e-commerce website transactions the payment system is made using a credit card, and not a physical credit card, but it is enough to know the credit card numbers and the expiration date. Carding is fraud on a credit card if a perpetrator knows a person's credit card number is still valid, then the perpetrator can buy goods online where the bill is charged to the original owner of the credit card or victim, while the perpetrator is called a carder (Indradi, 2006). Another term for crimes of this type is cyber fraud, aka fraud in cyberspace (Raharjo, 2002). Carding has two scopes, namely, national, and transnational. National scope, is the carding actor committing his crime within the scope of a particular country and Transnational, is the actor carding across certain country borders. Furthermore, there are two ways to misuse credit cards (Ibrahim, 2004; Mansur, 2005), namely:

1) credit card is valid but not used in accordance with the regulations specified in the agreement agreed by the credit card holder with the bank as the credit card manager.
2) invalid credit card or fake credit that is used illegally as well.

Carding is a crime that is included in cybercrime. The forms of cybercrime that are generally recognized in society are divided into 3 (three) general qualifications (Arief, 2006), namely:

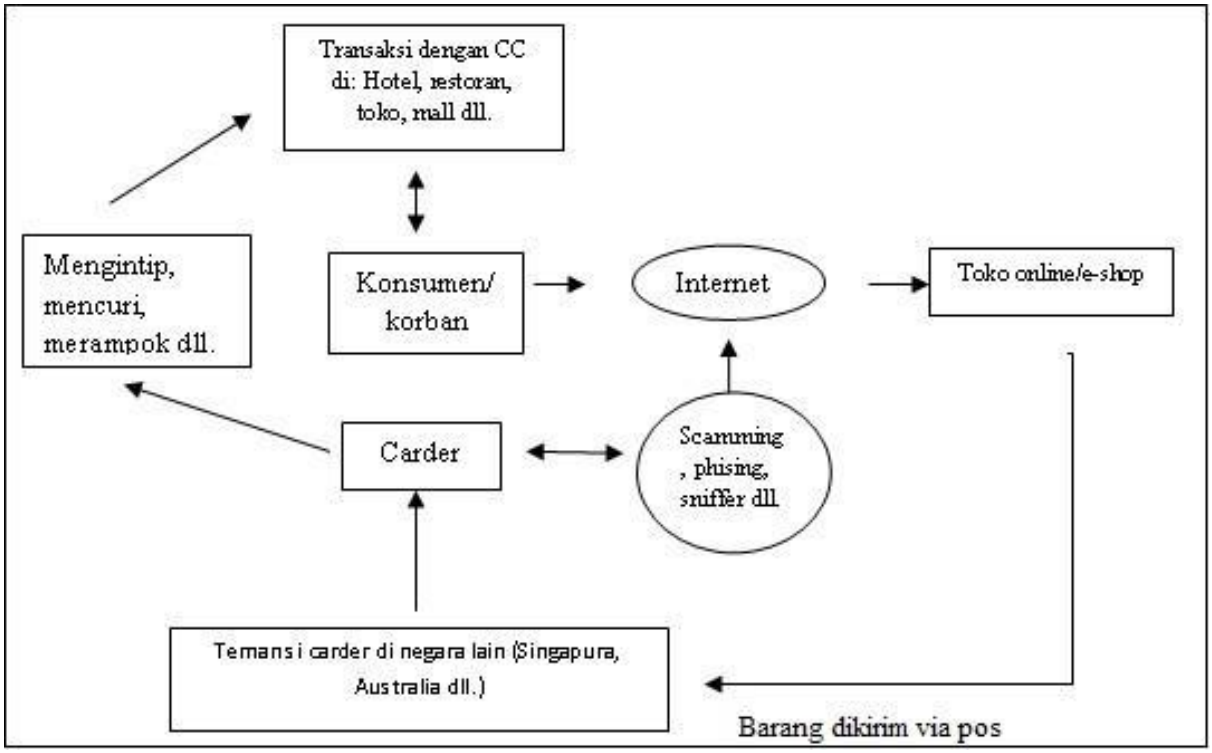
1) Evil cyberspace relating to the confidentiality, integrity and existence of data and computer systems.
2) Evil cyberspace that uses computers as a tool of crime.
3) Evil cyberspace relating to the content or content of data or computer systems.

Of the several forms of crime in cyberspace or what is often referred to as cybercrime that has been described above, it often occurs in Indonesia, one of which is the carding crime itself, this type of crime is more focused on buying and selling transactions whether it is carried out online (in network) or physically or directly.

Furthermore, carding is done by using a credit card belonging to another person whose number has been stolen to shop at a shop or shopping place that accepts payment using a credit card such as modern shopping places, malls, jewellery stores, and all places with logos. Master, Visa, Maestro, Cirrus, American-Express and other types. Credit card multiplication is done by reading the victim's credit card data using MSR (*Magnetic StripeCard Reader*), after which the data is written into a blank card or what is often called a fake card using MSR. The next step is to spend directly to various places that serve credit card payments (Muhammad & Murniati, 2000; Putra, 2016; Zuraidah, 2015).

Another case with the online method, carding is done by using a credit card belonging to another person or a victim or someone else's credit card number to shop at online shopping places. Credit card hacking technique aka carding, which is to steal transaction data from the manager of an online shopping service by a black hacker. Furthermore, the data on the credit card owner from this database is stolen by the perpetrator used for the transaction, then the bill will automatically go to the owner of the credit card or the victim of the carding crime.

In simple terms, the mode used by most carders is as follows:



B. The Occurrence of Carding in Indonesia

The loss of time and space boundaries on the Internet changes many things. The rapid development in the use of internet services in the end invites the occurrence of crime, which is better known as Cybercrime. Indonesia as one of the most densely populated countries in the world cannot be separated from this problem (Arifah, 2011). Just as the needs of modern society in facilitating daily activities seem to be primary needs, because modern society is now starting to shift to carry out activities instantly and quickly. Such as the need for a payment instrument that users feel is more efficient, comfortable, and easy to use. This credit card payment tool is one of the most sought after or most in demand by the public. Based on the Bank Indonesia Payment and Money Circulation System Report Data or BI LSPPU, it is stated that, in 2009, the number of credit card holders in Indonesia had reached more than 12 million credit card holders from a total of 20 issuers in Indonesia.

The development of the number of credit card holders from 2000 to 2009 in Indonesia shows that the need for credit cards has increased in line with the advancement of the banking industry. The increasing trend in society, the number of cards during this period of time contributed to an

increase in their use. On the value side, annual growth reaches 30%, meanwhile, on the volume side, it reaches 19%. This can be seen from Figure 1 (LSPPU BI, 2009; Panjaitan, 2012) below:

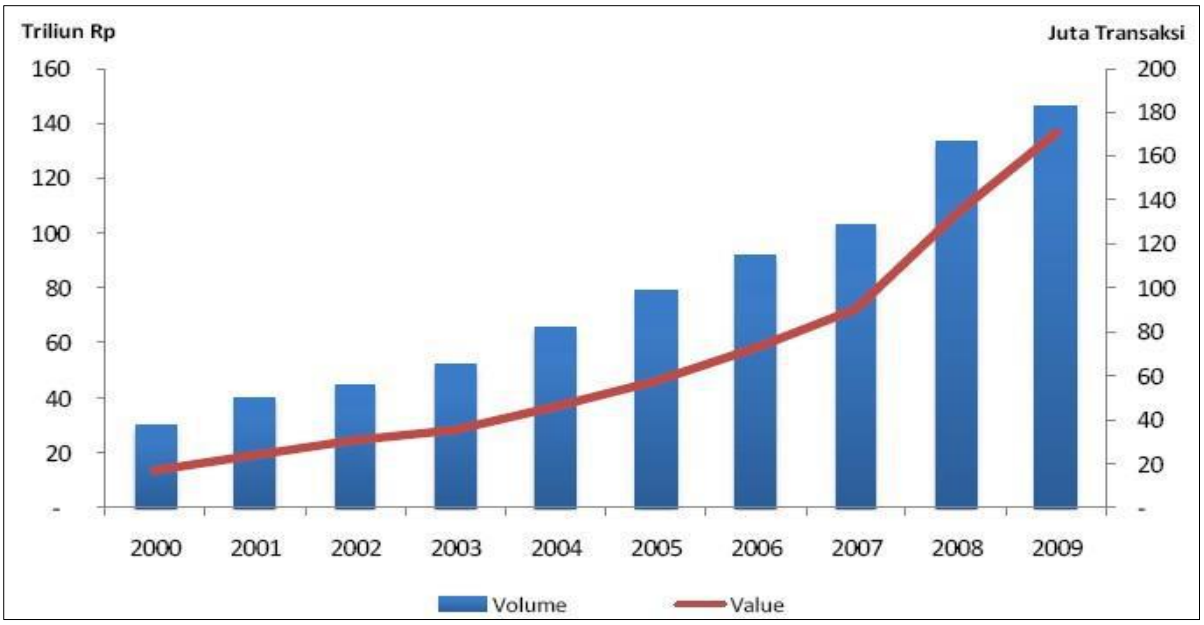


Figure 1 Total Value and Volume of Credit Card Transactions in Indonesia

Based on this table, it can be concluded that modern society wants things that are easier, more efficient, safer, and faster. However, the practice of the credit card industry in Indonesia is not completely safe from credit card criminals or hackers who are always looking for profit from their victims.

Carding as a type of cybercrime has become a crime that has troubled many credit card users in Indonesia, therefore the Indonesian Police (POLRI) responded by forming a special unit at the POLRI Headquarters level called the Directorate of Cyber Crime, which is manned by personnel are trained to handle cases of this kind, not only in investigation and investigation techniques, but also they master special techniques for security, and confiscation of evidence electronically (Mahfud MD, 2000).

The phenomenon of cybercrime has to be watched out for because this crime is somewhat different from other crimes in general. Cybercrime can be carried out without knowing territorial boundaries and there is no need for direct interaction between the perpetrator and the crime victim (Sudarwanto, 2009).

With so many credit card users in Indonesia, it will bring a crime described above, namely Carding, often law enforcement officials arrest the perpetrator who has troubled many of the credit card users in Indonesia. As was the case in Indonesia in March, The East Java Regional Police have succeeded in uncovering ITE crimes committed by spamming and carding. The mode used by the perpetrator in carrying out his crimes is by stealing other people's credit card data which is then used to buy goods through shopping stores on the internet with that credit card. The perpetrator of the carding crime was arrested by the East Java Regional Police. It is known that the perpetrator with the initials IIR is a 27-year-old resident of Bojonegoro and his friend, ZU, a resident of Malang, East Java.

This case developed from online transactions, using a modified credit card to commit crimes (Rinanda, 2018). The spamming and carding perpetrators committed crimes using smart phones. First, they signed in with fake accounts on Apple and Paypal. From this account, they can steal data in the form of credit card numbers and expiration dates. After the perpetrator succeeds in stealing, the perpetrator then spends it on shopping sites in cyberspace. The perpetrator will then sell these goods so that they can be used as money for the perpetrators' living expenses. Based on the perpetrators' information, they had successfully broken into credit cards totalling Rp. 500,000,000.

The perpetrator was charged under Article 30 paragraph (2) and / or Article 32 paragraph (1) RI Law No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 1 of 2008 concerning Information and Electronic Transactions (ITE) and Article 46 (2) of Law of the Republic of Indonesia No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 1 of 2008 concerning Electronic Information and Transactions, with a maximum imprisonment of seven years and a maximum fine of Rp. 700 million.

C. Law Enforcement Efforts Against Carding Players in Indonesia

Cybercrime which is basically the impact of technological developments that have changed the habits of society from a conventional nature to a habit that is more modern or can be called a high technology society (Putra,

2016). *Cybercrime* can be called a crime related to the interests of a person or group of people. There is someone who uses or is used to expand the reach of cybercrime. The interests of business, politics, culture, religion and so on can be motives, reasons and arguments that make a person and a group of people fall into cybercrime (Ismail, 2009).

Based on the current state of cybercrime that is rife in Indonesia, we can see that cybercrime by means of Carding is a serious threat to the non-traditional security sector as described above. Crime using computer equipment and internet networks (cybercrime) in Indonesia, is among the highest in the world (Mehda, 2015). Factors causing the rate of development of cybercrime tend to increase from year to year (Mansur & Gultom, 2005), namely:

1) Public Legal Awareness
   There is a lack of legal awareness among the people in responding to cybercrime activities. This is due, among others, to the lack of understanding and knowledge of the public regarding the types of cybercrime. This lack of understanding and knowledge causes the efforts to overcome cybercrime to experience obstacles. In this case, the constraints are related to legal structuring and the process of public monitoring of any activity that is suspected of being related to cybercrime.
2) Safety factor
   The criminals will feel a sense of security when they are carrying out the action. This is because the internet is generally used in relatively closed places. As a result, when the perpetrator is committing a crime, it is very rare for people to know about it. If the perpetrator has committed a crime, the perpetrator can easily erase all traces of the crime that has been committed. When the perpetrator is caught, it is difficult for law enforcement officials to find evidence of the crime.
3) Law Enforcement Factors
   Law enforcement factors are often one of the causes of the rampant cybercrime. This is motivated by the lack of law enforcement officers who understand the ins and outs of information technology, so that when a criminal is arrested, law enforcement officials find it difficult to find evidence that can be used to ensnare the perpetrator, especially if the crime committed has a very complicated operating system.

Another factor in influencing someone to commit this carding crime is the necessity of life, as has been reported in various mass media and electronic media which shows that someone commits a crime, including theft of various types, due to insufficient economic needs. someone thinks that stealing can make ends meet, but for whatever reason stealing cannot be justified and needs serious attention because it cannot be separated from community life and can disturb the stability of social harmony (Firmansyah, 2012).

Furthermore, criminal law as social control is used to tackle crimes in the form of violations of norms related to the use of potentially criminal information technology, in order to provide protection to the public from the dangers of these crimes (Supanto, 2016).

In Indonesia, at the beginning of this carding case, in its handling of carding it was categorized as a crime of theft, in which the definition of theft according to the law and its elements has been formulated in Article 362 Indonesian Penal Code (KUHP) that: *Whoever takes an object entirely or part of the property of another person, with the intention of being illegally owned, is threatened with theft, with a maximum imprisonment of 5 years or a maximum fine of nine hundred rupiahs*". In this crime, then after the existence of the ITE Law, which specifically regulates cases of crimes in cyberspace, one of which is carding crimes which can be criminalized by applying Article 31 paragraphs 1 and 2 which discusses hacking. Because one of the steps or practices is to get other people's credit card numbers by or hacking into official websites of institutions that provide credit cards to penetrate the security system and steal the card numbers.

The sound of article 31 which explains about acts that are considered to be against the law according to the ITE Law in the form of illegal access: Article 31 paragraph 1: "*Every person intentionally and without right or against the law intercepts or eavesdrops on electronic information and / or electronic documents in a computer and / or electronic system in a certain way belonging to another person*." Article 31 paragraph 2: "*Every person intentionally or without right or against the law conducts interception or electronic transmission and / or electronic documents that do not have a public status from, to and within a computer and / or certain electronic system belonging to another person, whether it does not cause change, removal and or*

termination of electronic information and or electronic documents transmitted. "

So far, carding cases in Indonesia can be resolved with the old regulations, namely article 362 in the Criminal Code and Article 31 paragraphs 1 and 2 in the ITE Law. In handling carding cases, special regulations are needed to regulate carding crimes, so that cases like this can be reduced and even no longer exist because it is very detrimental to the people who use them. However, in addition to special regulations, it must also be supported by system security both software and hardware, stronger and stronger guidelines against hacker threats, and making policies related to computer-related crime and support from special institutions (Ahmada, 2012; Sidik, 2013).

5. CONCLUSION

This research concluded that with the progress of the times, the human mindset will increasingly advance to compete in technological science to facilitate all human activities. So, the advancement of technology has provided a very broad source of information and communication from what humans already have. The internet activities cannot be separated from the human factor and its legal consequences also touch humans in society who are in the physical world, then there is a thought about the need for legal rules to regulate activities in cyberspace. Furthermore, in the development of a society that is experiencing rapid changes and advances due to globalization and technology, especially information technology, it is necessary to have legal regulations that can regulate human activities in relation to the use of information technology, so that in using or utilizing it, it does not harm or can be harmed personally. With the rise of cybercrime, the Indonesian government seeks to overcome and suppress these crimes, because most and the majority of the population in Indonesia have used and depend on technology.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Abidin, D. Z. (2017). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor*, *10*(2), 509-516.

Ahmad, A. (2012). Perkembangan Teknologi Komunikasi Dan Informasi: Akar Revolusi dan Berbagai Standarnya. *Jurnal Dakwah Tabligh*, *13*(1), 137-149. https://doi.org/10.24252/jdt.v13i1.300.

Arief, B. N. (2006). *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Rajawali Pers.

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2), 185-195.

Buzan, B. (2008). *People, States & Fear: An Agenda for International Security Studies in The Post-Cold War Era*. New York: Ecpr Press.

Firmansyah, D. (2012). Upaya Polri Dalam Penanggulangan Tindak Pidana Pencurian Sepeda Motor Dengan Kekerasan (Studi Pada Kepolisian Sektor Pakuan Ratu). *Jurnal Poenale, 2*(4), 413-422.

Fuady, M. E. (2005). "Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. *Mediator: Jurnal Komunikasi*, *6*(2), 255-264. https://doi.org/10.29313/mediator.v6i2.1194.

Hartono, B. (2013). Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding. *Pranata Hukum*, *8*(2), 168-177. http://jurnal.ubl.ac.id/index.php/PH/article/view/197.

Hermawan, R. (2015). Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta*, *6*(1), 43-50. http://dx.doi.org/10.30998/faktorexacta.v6i1.217.

Ibrahim, J. (2004). *Kartu Kredit: Dilematis antara Kontrak dan Kejahatan*. Jakarta: Refika Aditama.

Indradi, A. A. S. (2006). *Carding: Modus Operandi, Penyidikan, dan Penindakan*. Jakarta: PTIK.

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(3), 242-247.

Mahfud M.D. (2000). *Politik Hukum Nasional*. Bandung: Alumni.

Mansur, D. M. A. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Semarang: Tiga Serangkai.

Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Muhammad, A., & Murniati, R. (2000). *Segi Hukum Lembaga Keuangan dan Pembiayaan*. Jakarta: Citra Aditya Bakti.

Panjaitan, L. T. (2012). Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2018. *IncomTech: Jurnal Telekomunikasi dan Komputer*, *3*(1), 1-26. http://dx.doi.org/10.22441/incomtech.v3i1.1111.

Pirog, S. F., & Roberts, J. A. (2007). Personality and credit card misuse among college students: The mediating role of impulsiveness. *Journal of Marketing Theory and Practice*, *15*(1), 65-77. https://doi.org/10.2753/MTP1069-6679150105.

Pujoyono, N. W. (2020). Penal Policy dalam Upaya Preventif Kejahatan Carding di Indonesia. *Jurnal Panji Keadilan: Jurnal Ilmiah Nasional Mahasiswa Hukum*, *3*(1), 86-98. https://doi.org/10.36085/jpk.v3i1.1183.

Putra, A. K. (2016). Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime. *Jurnal Ilmu Hukum*, *7*(1), 22-54.

Raharjo, A. (2002). *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Jakarta: Citra Aditya Bakti.

Republic of Indonesia. (2008*). Law Number 11 of 2008 concerning Information and Transactions Electronic.*

Republic of Indonesia. *Indonesian Penal Code (Kitab undang-Undang Hukum Pidana).*

Rinanda, H. M. (2018, March). "Pelaku Spamming dan Carding dibekuk Bobol Kartu Kredit Rp. 500 juta", *News Detik Online,* retrieved from https://news.detik.com/berita-jawa-timur/d-3927140/pelaku-spamming-dan-carding-dibekuk-bobol-kartu-kredit-rp-500-juta.

Sidik, S. (2013). Dampak Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terhadap Perubahan Hukum dan Sosial dalam Masyarakat. *Jurnal Ilmiah Widya*, *1*(1), 1-7.

Sudarwanto, A. S. (2009). Cyber-Bullying Kejahatan Dunia Maya Yang Terlupakan. *Jurnal Hukum Pro Justitia*, *27*(1), 1-16.

Supanto, S. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy. *Yustisia, 5*(1), 92-117. https://doi.org/10.20961/yustisia.v5i1.8718.

Suseno, S., & Barmawi, S. A. (2004). Kebijakan Pengaturan Carding dalam Hukum Pidana di Indonesia. *Sosiohumaniora*, *6*(3), 245. https://doi.org/10.24198/sosiohumaniora.v6i3.5532.

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cybercrime)*. Bandung: Refika Aditama.

Zuraida, M. (2015). Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia. *Jurnal Analisis Hubungan Internasional, 4*(1), 1627-1641.

Cybercrime is the greatest threat to every company in the world.

Ginni Rommety

ABOUT AUTHORS

Abid Nor Fuad, SH is a researcher and activist in the Indonesian Technology Law Society Movement. He graduated from the Faculty of Law Universitas Negeri Semarang, Indonesia. Besides his activities as a researcher he also actively advocates for some people, especially on cybercrime cases.

RESEARCH ARTICLE

Hate Speech and Hoaxes in Social Medias: The Dark Portrait of Uncertainty in Law Enforcement

Ahmad Nizar Numani
Anti Hoaxes & Hate Speech Community, Indonesia
✉ nizarnumajiri@gmail.com

OPEN ACCESS

Citation: Numani, A. N. (2021). Hate Speech and Hoaxes in Social Medias: The Dark Portrait of Uncertainty in Law Enforcement. *Law Research Review Quarterly, 7*(1), 97-110. https://doi.org/10.15294/lrrq.v7i1.43166

Submitted : October 23, 2020
Revised : December 13, 2020
Accepted : January 9, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

Social media is like a basic need for some people, the use of social media is very much, but the misuse of social media is often encountered, one of which is spreading hoaxes or hate speech through social media. This research is intended to analyze and examine hate speech and hoaxes spreading from the perspective of law enforcement as well as a legal instruments in Indonesia. This research emphasized and found that the prohibition of spreading hate speech itself is regulated in Article 28A of Law Number 11 of 2008 concerning Electronic Information and Transactions jo. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. One of the recent cases that occurred was a high school teacher in Banten who spread hoax stories of hatred with the aim of reminding SMA 1 Sajiro Banten students to be aware of the latent dangers of communism that would emerge.

Keywords: *Hate Speech; Hoaxes; Criminal Law; Law Enforcement*

1. INTRODUCTION

Social media is one of the communication media which is currently loved by many groups because it is considered as an effective, transparent and efficient communication media so that it has an important role as an agent of change and renewal. Meanwhile, the definition of social media according to Xarella (Aditya, 2015: 51; Marwan & Ahyad, 2016) states that social media is a site where people communicate with their friends, whom they know in the real

world and cyberspace. The advantages of social media compared to other conventional media are:

1) Fast, concise, compact and simple. If we see, every conventional media production requires special skills, standard standards and superior marketing skills. On the other hand, social media is so easy to use (user friendly), even users without an Information Technology (IT) knowledge base can use it. All you need is a computer, tablet, smartphone, plus an internet connection
2) Creating a more intense relationship. Conventional media only communicate one way. To overcome this limitation, conventional media tries to build relationships with 27 models of interaction or live connection via telephone, sms or Twitter. Meanwhile, social media provides wider opportunities for users to interact with partners, customers, and relationships, and build reciprocal relationships directly with them.
3) Wide and global reach. Conventional media have global reach, but to sustain it is expensive and takes longer. Meanwhile, through social media, anyone can communicate information quickly without geographical barriers. Social media users are also given great opportunities to design content, according to the targets and desires of more users.
4) Control and scalable. In social media with the available tracking system, users can control and measure the effectiveness of the information provided through feedback and reactions that arise. Meanwhile, in conventional media, it still takes a long time (Pranesti & Arifin, 2019; Sirait, 2020).

The use of social media from year to year tends to increase causing new problems where everyone is free to reveal what their think in their social media accounts or share news sites to their social media accounts but this freedom creates another problem where there are many hoaxes, hatespeech or hate speech that thrives on social media. Problems like this that sometimes bother social media users, especially those who play social media, just want to increase their interaction with their friends online, especially the one most frequently discussed lately, namely Hate Speech social media (Astrini, 2017; Nurlatifah, 2019; Rifauddin & Halida, 2018).

One of the most recent cases is an act committed by a high school teacher named Yayi Haidar Aqua as the owner of me facebook Ragil Proyooda Hartajo who is suspected of spreading hoaxes about the existence of PKI members who want to massacre clerics whose purpose is to spread this to his social media accounts to remind SMA 1 Sajiro Banten students to be vigilant against the latent danger of communism, however, the police consider Yayi Haidar Aqua's actions to be a form of hoax spreading with hate speech (Ferdiawan, et.al, 2019; Rahmatullah, 2019; Utami, 2018).

Indonesia itself in overcoming hate speech has given birth to several regulations, namely the Chief of Police Circular Letter Number SE/06/X/2015 which states that hate speech is getting more attention from the public both nationally and internationally along with increasing concern for the protection of human rights, in addition to hate speech through social media. is also a criminal act that has been regulated in article 28 paragraph (2) of the Law on Electronic Information and Transactions, then whether the government's action by giving birth to this law is an act of dealing with hate speech or to silence the public's freedom of opinion because the article is considered an article rubber.

2. METHOD

Soekanto & Mamudji (2007) argue that legal research based on its objectives consists of: first, normative legal research which includes research on legal principles, research on legal systematics, research on the level of legal synchronization, legal history research, and comparative legal research. Second, sociological or empirical legal research which includes research on legal identification (unwritten) and research on the effectiveness of law. The type of research used in the research "Hate Speech Handlers in Social Media" is normative legal research because it is a study of legal principles or legal foundations, legal theories, and legal concepts. The data source used in this research is literature study. This research was conducted through literature study techniques, namely: how to collect data by studying legal materials, both primary legal materials, secondary legal materials and tertiary legal materials and/or non-legal materials. Searching for legal materials can be done by

reading, seeing, listening, and nowadays there are many searches for legal materials through the internet. The primary legal materials consist of:

1) The 1945 Constitution of the Republic of Indonesia.
2) Law Number 11 of 2008 concerning Electronic Information and Transactions jo. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.
3) Criminal Code.
4) UU no. 40 of 2008 concerning the elimination of racial and ethnic discrimination.
5) Chief of Police Circular Number SE / 06 / X / 2015 concerning Hate Speech.

Data analysis was carried out using a qualitative approach, where existing data were linked, compared, and described in words and / or sentences. After the analysis is carried out, the deductive thinking method is carried out, namely a pattern of thinking that is based on general matters, then spreads specific things.

3. RESULT AND DISCUSSION

A. The Rise of Hoaxes in Indonesia

Hoax or false information has become a phenomenon that is disguised to make it look true, this is not without the characteristics of Indonesian people who use social media a lot. The sad thing is that most of the people can easily believe in hoax news and do not hesitate to share it with the public. According to Professor of Communication Studies at Padjajaran University Bandung, Deddy Mulyana stated several factors causing the rapid circulation of hoax news are:

1) The Indonesian people themselves are considered unusual for a healthy democracy.
2) Most people are not used to recording and storing data, so they often talk without data.
3) Indonesian people, who are chatty in nature, then the information received is then shared again without verification (Septanto, 2018; Siregar, 2018).

In essence, a news is a description or idea that is processed based on editorial to be broadcast to the public. The use of social media causes the public to be interested in using communication media more often to get information as desired. However, there are several things that need to be

expanded from an early age, namely related to the circulation of hoaxes that aim to form public opinion, the ability of social media to provide facilities to the public in responding to these hoaxes to shape public opinion.

There are 7 types of hoax information (Rahadi, 2017; Utami, 2018), namely:

1) Fake News, Fake News is news that aims to fake or include things that are untrue in a news
2) Clickbait: Trap links are links that are strategically placed on a site that aim to attract people to another site, where the content is factual but the title is too much.
3) Confirmation Bias, confirmation bias is the tendency to interpret recent events as well as evidence of existing beliefs
4) Misinformation, Misleading or false information intended to deceive
5) Satirem, an article that uses exaggerated humor, irony, to comment on hot events
6) Post-truth, post truth is an incident where emotions play a role more than facts to form opinions
7) Propaganda, namely the activity of disseminating information, facts, arguments, half-truth gossip or truth to form public opinion.

Several aspects that are often the subject of hoaxes are related to religion, politics and economics. Some of the hoax cases that have occurred in Indonesia are Iron Man Bali. Vacuum Power Plant, Saracen Case, therefore, as smart citizens in using social media, we should not be easily provoked by the news that appears and must verify the information we get (Manihuruk & Tarina, 2020; Gunawan, Wijaya, & Idrus, 2018).

The government itself in tackling the frequent hoax phenomenon has formed a National Cyber Agency, this agency is tasked with tracking down sources of hoax news and protecting government sites from hackers. In addition, in terms of sanctions, Indonesia already has the ITE Law, the Criminal Code and the Law on the Elimination of Racial and Ethnic Discrimination (Iqbal, 2019; Siregar, 2018).

B. Hate Speech Handling Regulations in National Regulations

Freedom of opinion has been guaranteed by the 1945 Constitution as stipulated in Article 28E paragraph 3 of the

1945 Constitution which states "*Everyone has the right to freedom of association, assembly and expression of opinion*" but this right to freedom of opinion is often misinterpreted and misused to create hoax news aimed at spreading hate speech (Rahardi, 2017: 66; Hidayat & Mahardiko, 2020).

Hate speech is speech, behavior, writing or performance that is prohibited because it can trigger acts of violence and commotion in people's lives, in the Chief of Police Circular Number SE / 06 / X / 2015 concerning Hate Speech, it is stated that Hate Speech is a criminal act regulated in Criminal Code and other criminal provisions outside the Criminal Code, in the form of:

1) Insult
2) Defamation
3) Blasphemy
4) Unpleasant acts
5) Provoke
6) Addressing
7) Spread fake news

The purpose of hate speech as mentioned above is to incite and incite hatred against individuals and / or groups of people in various communities who in conducting Hate Speech can be carried out using various media including:

1) In the campaign activity oration
2) Banners or banners
3) Social media network
4) Expression of opinion in public (demonstration)
5) Religious lectures
6) Print or electronic media
7) Pamphlet (Diantha, 2016; Chazawi, 2016).

Handling of suspected hate speech crimes has basically been regulated in national legislation, including:

1) Article 156 of the Criminal Code
2) Article 157 of the Criminal Code
3) Article 310 of the Criminal Code
4) Article 311 of the Criminal Code
5) Article 28 paragraph (2) jo. Article 45 paragraph (2) of Law number 11 of 2008 concerning Information and electronic transactions
6) Article 16 of Law no. 40 of 2008 concerning the elimination of racial and ethnic discrimination.

The operational level of the Chief of Police's circular letter SE / 06 / X / 2015 regarding Hate Speech is seen in the

handling procedures regulated in the circular (Mangantibe, 2016; Chazawi & Ferdian, 2011), namely:

1) Take preventive actions, where these preventive actions include e*very member of the National Police so that they have knowledge and understanding of forms of hate speech that arise in society* and in order to make effective and prioritize the intelligence function to find out the real conditions in conflict-prone areas.
2) If preventive action has been taken by a member of the National Police but does not solve the problem as a result of this action, the solution can be done in several ways including through:
    a. Law enforcement on suspicion of criminal acts of hate speech by referring to the provisions,
    b. In the event that there has been a social conflict with the background of hate speech, the handlers hold on to:
        i. Law Number 7 of 2012 concerning Management of Social Conflict.
        ii. Regulation of Chief of the National Police of the Republic of Indonesia Number 8 of 2013 concerning Technical Social Conflict Management.

Furthermore, many regulations governing hate speech as described above law enforcers most often use Article 28 paragraph (2) jo. Article 45 paragraph (2) of Law number 11 of 2008 concerning information and electronic transactions, in which Article 28 paragraph (2) states that "*everyone deliberately and without rights disseminates information aimed at causing hatred or enmity for individuals and / or groups. certain society based on ethnicity, religion, race and intergroup*".

Based on the sound of the article above, what is meant by the act of expressing hatred there is no clear explanation, but referring to article 156 of the Criminal Code, the act of spreading hatred is an act of stating with words whose contents are viewed or judged by the general public as hating a group of Indonesian population where the act is. its contents are considered by the public to be derogatory, degrading, insulting against a group of the Indonesian population (Chazawi, 2016; Sitompul, 2012).

The absence of explanation related to hate speech is a weakness in its own right from Article 28 paragraph 2 of Law No. 11 of 2011 concerning Electronic Information and

Transactions because there are no restrictions related to actions that are deemed to violate the provisions of this article even though it serves to prevent restrictions or violations of freedom of opinion due to the fact that there are many actions which in fact may not violate statutory regulations which exists (Rahadi, 2017; Ahnaf & Suhadi, 2014).

If described in Article 28 paragraph (2) of Law no. 11 of 2011 concerning Electronic Information and Transactions, the elements can be seen as follows:

1) Subjective: Everyone in this case is a person or a corporation
2) Error: deliberately, according to the theory of deliberation, deliberation is divided into 3, namely deliberate intent, conscious deliberate possibility, deliberate conscious certainty
3) Deed: spread
4) Object: Information
5) Purpose: to cause resentment or hostility to certain individuals and / or groups of people based on ethnicity, religion, race and between groups.

So that when it is related to the actions of a high school teacher named Yayi Haidar Aqua as the owner of me on Facebook, Ragil Proyooda Hartajo, who is suspected of spreading hoaxes about the existence of a PKI member who wanted to massacre clerics whose purpose was to spread this to his social media accounts to remind SMA 1 Sajiro students Banten to be aware of the latent dangers of communism will emerge as shown in the Figure 1.

For Yayi Haidar Aqua's actions, he could face a maximum sentence of 6 years and / or a maximum fine of Rp. 1,000.0000., 00 (one billion rupiah), but before that the mistake of Yayi Haidar Aqua must be proven beforehand in court based on existing evidence. For evidence in Law No. 11 of 2011 concerning Electronic Information and Transactions other than referring to Article 184 of the Criminal Procedure Code, which consists of:

1) Witness statement
2) Expert Statement
3) Letter
4) Guidance and
5) Statement of the Defendant

Figure 1. Screen capture of fake and hoax news in Social Media

There are also other evidence which is one of the special characteristics of the Special Law on ITE, namely:

1) Electronic information and /or electronic documents.
2) Printout of electronic information and/or electronic documents.

Regarding electronic information evidence and/or electronic documents, there are two views (Isma, 2014; Retnaningsih, 2015; Juliswara, 2017), namely:

1) The first view states that electronic evidence is categorized as existing evidence so that it does not stand alone, which is an extension of documentary evidence as regulated in article 184 of the Criminal Procedure Code.
2) Second view, states that electronic evidence is evidence in itself, electrical evidence is separate from evidence as stipulated in article 184 of the Criminal Procedure Code.

In proving a hate speech criminal case which is a means of evidence, namely witness statements, expert statements, letters, instructions, statements of the defendants, electronic information and electronic documents and / or printed results thereof. However, what must be considered in

submitting electronic information and electronic documents as evidence in court (Prisgunarto, 2015; Retnaningsih, 2015), are:

1) The authenticity of the evidence
2) The content or substance of the evidence
3) Conformity between one evidence and another.

4. CONCLUSION

This research concluded that hoax information is made aiming to influence and shape public opinion. There are 7 types of hoax information, starting from Fake News, Clickbait: Confirmation Bias, Misinformation, Satirem, and Post-truth, Propaganda. The provisions of laws and regulations that regulate the crime of hate speech are: Article 156, Article 157, Article 310, and Article 311 of the Criminal Code. Furthermore, another laws, article 28 paragraph (2) jis, Article 45A paragraph (2) Law Number 19 of 2016 concerning Electronic Information and Transactions, and Article 16 of Law Number 40 of 2008 concerning the Elimination of Racial and Ethnic Discrimination. Which man, if it is related to the case experienced by a high school teacher from Banten, then referring to the lex specialis derogat legi generalis principle used is Article 28 paragraph (2) jis. Article 45A paragraph (2) Law Number 19 Year 2016 concerning Electronic Information and Transactions. Evidence besides Article 184 of the Criminal Code, there are also other forms of evidence that are regulated in Law Number 19 of 2016 concerning Electronic Information and Transactions, namely Electronic Information and Electronic Documents and / or printouts.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Ahnaf, M. I., & Suhadi, S. (2014). Isu-isu Kunci Ujaran Kebencian (Hate Speech): Implikasinya terhadap Gerakan Sosial Membangun Toleransi. *Harmoni*, *13*(3), 153-164. https://103.7.13.84/index.php/harmoni/article/view/120.

Astrini, A. (2017). Hoax dan Banalitas Kejahatan (Studi Pustaka tentang fenomena hoax dan keterkaitannya dengan Banalitas Kejahatan). *Transformasi*, *2*(32), 76-167.

Chazawi, A. (2016). *Hukum Pidana Positif Penghinaan (Edisi Revisi). Cet. II.* Malang: Media Nusa Creative.

Chazawi, A., & Ferdian, A. (2011). *Tindak Pidana Informasi & Transaksi Elektronik Penyerangan Terhadap Kepentingan 14 Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*. Malang: Bayumedia Publishing.

Diantha, I. M. P. (2016). *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*. Jakarta: Prenada Media.

Ferdiawan, Y. I., Nurjanah, P. A. D., Krisdyan, E. P., Hidayatullah, A., Sirait, H. J. M., Rakhmawati, N. A., ... & Ferdiawan, Y. I. (2019). HOAX Impact to Community Through Social Media Indonesia. *Cakrawala- Jurnal Humaniora*, *19*(1), 121-124. https://doi.org/10.31294/jc.v19i1.4452.

Gunawan, M. K., Wijaya, A., & Idrus, A. H. (2018). Handling of hoax messages from the legal perspective: a comparative study between Indonesia and Singapore. *International Journal of Global Community*, *1*(2), 125-140. https://journal.riksawan.com/index.php/IJGC-RI/article/view/22.

Hidayat, T., & Mahardiko, R. (2020). The effect of social media regulatory content law in Indonesia. *Journal of Telecommunications and the Digital Economy*, *8*(2), 110-122. http://doi.org/10.18080/jtde.v8n2.247.

Iqbal, M. (2019). Efektifitas Hukum Dan Upaya Menangkal Hoax Sebagai Konsekuesni Negatif Perkembangan Interkasi Manusia. *Literasi Hukum*, *3*(2), 1-9.

Isma, N. L., & Koyimatun, A. (2014). Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana. *Jurnal Penelitian Hukum Gadjah Mada*, *1*(2), 109-116.

Juliswara, V. (2017). Mengembangkan Model Literasi Media yang Berkebhinnekaan dalam Menganalisis Informasi Berita Palsu (Hoax) di Media Sosial. *Jurnal Pemikiran Sosiologi*, *4*(2), 142-164. https://doi.org/10.22146/jps.v4i2.28586.

Mangantibe, V. (2016). Ujaran Kebencian dalam Surat Edaran Kapolri Nomor: Se/6/X/2015 tentang Penanganan Ucapan Kebencian (Hate Speech). *Lex Crimen*, *5*(1). 159-162.

Manihuruk, H., & Tarina, D. D. Y. (2020). State Defense Efforts through Strengthening Cyber Law in Dealing with Hoax News. *International Journal of Multicultural and Multireligious Understanding*, *7*(5), 27-36. http://dx.doi.org/10.18415/ijmmu.v7i5.1590.

Marwan, M. R., & Ahyad, A. (2016). Analisis penyebaran berita hoax di Indonesia. *Jurusan Ilmu Komunikasi, Fakultas Ilmu Komunikasi Universitas Gunadarma*, 5(1), 1-16.

Nurlatifah, M. (2019). The Figth Against Hoax: An Explorative Study towards Anti-hoax Movements in Indonesia. *Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia*, *4*(1), 46-54.

Pranesti, D. A., & Arifin, R. (2019). Perlindungan Korban dalam Kasus Penyebaran Berita Hoax di Media Sosial di Indonesia. *Jurnal Hukum Media Bhakti*, *3*(1), 8-17. https://doi.org/10.32501/jhmb.v3i1.28.

Prisgunanto, I. (2015). Pengaruh sosial media terhadap tingkat kepercayaan bergaul siswa. *Jurnal Penelitian Komunikasi dan Opini Publik*, *19*(2), 101-112.

Rahadi, D. R. (2017). Perilaku Pengguna dan Informasi Hoax di Media Sosial. *Jurnal Manajemen dan Kewirausahaan*, *5*(1), 58-70. https://doi.org/10.26905/jmdk.v5i1.1342.

Rahmatullah, T. (2019). Hoax dalam Perspektif Hukum Indonesia. *Jurnal Hukum Media Justitia Nusantara*, *8*(2), 103-111. http://103.66.199.204/index.php/MJN/article/view/673.

Republic of Indonesia. (1945). *Constitution of Republic of Indonesia 1945* [Undang-Undang Dasar Negara Republik Indonesia Tahun 1945].

Republic of Indonesia. (2008). *Law Number 11 of 2008 concerning Information and Transactions Electronic* [Undang-Undang Nomor 11 Tahun 2008 tentang

Informasi dan Transaksi Elektronik].

Republic of Indonesia. (2008). *Law Number 40 of 2008 concerning the Elimination of Racial and Ethnic Discrimination* [Undang-Undang Nomor 40 Tahun 2008 tentang Penghapusan Diskriminasi Ras dan Etnis].

Republic of Indonesia. (2015). Chief of Police Circular Letter Number SE/06/X/2015 concerning Hate Speech [Surat Edaran Kapolri Nomor SE/06/X/2015 tentang Ujararan Kebencian].

Republic of Indonesia. (2016). *Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions* [Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik].

Republic of Indonesia. *Indonesian Penal* Code [Kitab Undang-Undang Hukum Pidana].

Retnaningsih, H. (2015). Ujaran Kebencian Di Tengah Kehidupan Masyarakat. *Jurnal Info Singkat Kesejahteraan Sosial. Sekretariat Jenderal DPR RI*, *7*(21), 9-12.

Rifauddin, M., & Halida, A. N. (2018). Waspada cybercrime dan informasi hoax pada media sosial facebook. *Khizanah al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan*, *6*(2), 98-111.

Septanto, H. (2018). Pengaruh hoax dan ujaran kebencian sebuah cyber crime dengan teknologi sederhana di kehidupan sosial masyarakat. *Jurnal Kalbiscientia: Jurnal Sains dan Teknologi*, *5*(2), 157-162.

Sirait, F. E. T. (2020). Ujaran Kebencian, Hoax dan Perilaku Memilih (Studi Kasus pada Pemilihan Presiden 2019 di Indonesia). *Jurnal Penelitian Politik*, *16*(2), 179-190. https://doi.org/10.14203/jpp.v16i2.806.

Siregar, K. M. (2018). Integrasi Politik Hukum terhadap Tindak Pidana Pemberitaan Palsu (Hoax) di Indonesia. *FITRAH: Jurnal Kajian Ilmu-ilmu Keislaman*, *4*(2), 227-242. https://doi.org/10.24952/fitrah.v4i2.955.

Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: PT Tatanusa.

Soekanto, S., & Mamudji, S. (2007). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: Raja Grafindo Persada.

Utami, P. (2018). Hoax in modern politics: the meaning of hoax in Indonesian politics and democracy. *Jurnal Ilmu Sosial dan Ilmu Politik*, *22*(2), 85-97. ttps://doi.org/10.22146/jsp.34614.

"The claim "hate speech is not free speech" implies "free" is a type of speech, as opposed to how speech is treated in a free society."

Michael Malice

ABOUT AUTHORS

Ahmad Nizar Numani is a social movement activist on Anti Hoaxes and Hate Speech. Many of his activities are to educate the public about the dangers of fake news and hate speech. In addition, the author is also actively collaborating with various community groups, communities, and the government in tackling hoaxes in Indonesia.

RESEARCH ARTICLE

Typosquatting Crime in the Electronic Transactions

Alif Kharismadohan
Postgraduate Program, Faculty of Law, Universitas Negeri Semarang, Indonesia
✉ alifkharismadohan@gmail.com

OPEN ACCESS

Citation: Kharismadohan, A. (2021). Typosquatting Crime in the Electronic Transactions. *Law Research Review Quarterly, 7*(1), 111-124. https://doi.org/10.15294/lrrq.v7i1.43188.

Submitted : October 25, 2020
Revised : December 19, 2020
Accepted : January 19, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

Today's technological developments have brought many changes to human life. This change will certainly bring benefits to life, including making all transactions easier and faster. However, there are still some parties who take advantage of technology to act crimes. Among them is typosquatting, which is impersonating a domain name that is almost similar to the original domain name and has the same contents as the original domain. This will be detrimental to transaction service users. This research aims to analyze and study typosquatting in electronic transactions in Indonesia and its law enforcement. This study found that these crimes often committed on the internet were used to trick internet users by creating a fake website using names that were very similar to well-known websites. Furthermore, this research underlines that typosquatting legal arrangements in Indonesia can be seen in the Trademark Law, the Criminal Code, as well as the Information and Electronic Transaction Law.

Keywords: *Typosquatting; Cybercrime; Law Enforcement*

1. INTRODUCTION

In this 21st century, which is better known as the information century, the role of information technology is increasingly important. The importance of this role is further spurred by the need for the fast-paced activities of the modern world and the demands of an all-globalizing era. As a result, the activities of the modern world really require efficient communication technology and can reach large areas without being hindered by national borders (Wijaya & Arifin, 2020). One technology that has successfully

answered these needs is the internet (Rosidawati & Santoso, 2013).

Internet as a form of advancement in information technology, has changed the lifestyle of humans. Internet is almost used in every area of life. For example, education, banking, business and so on.

In today's era, almost all transactions can be done electronically. This of course is a form of progress because business transactions can be done anytime and anywhere as long as there is an internet network. Marketing that used to be done conventionally is now mostly done with the help of technology (Maherni, 2015; Muthia & Arifin, 2019; Mooere & Edelman, 2010). However, of course there are negative impacts with the existence of these electronic transactions such as fraud, spread of personal data and typosquatting. Typosquatting is site plagiarism that can mislead internet users (Widodo, 2013; Spaulding, Upadhyaya, & Mohaisen, 2016). Typosquatting can be detrimental to internet users who might make a typo in typing the domain.

In Indonesia, crime through the internet is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008. However, in reality cyber crime in Indonesia still occurs in the community, especially in typosquatting cases. In the case of typosquatting, that is, if an internet user types the wrong domain name, but the pages and contents of the domain are the same. So, it can create confusion for internet users about the original website. Because, this fake domain can cause various losses if we have entered our personal data (Dharmaadi, Bakhrun, Saputra, & Putra, 2014).

2. METHOD

For this research, the author uses several sources and types of data, namely: *Source and type of data*: the source of data that the authors use is secondary data, namely data arranged in the form of documents (Suryabrata, 1987). Secondary data needed in this paper is data regarding various definitions of cybercrime, typosquating and applicable laws to solve typosquating problems. While the types of data obtained are quantitative and qualitative. *Data collection*: in the method of writing this paper, the authors collect data using the literature study method. Literature study was conducted to obtain data using literature related to writing this paper,

namely about typosquatting. *Data analysis*: the data that has been collected is then selected again and examined again. After that researched using descriptive and argumentative analysis techniques. *Conclusion***:** draw research conclusions always have to base themselves on all data obtained in research activities (Arikunto, 2015).

3. RESULT AND DISCUSSION

A. Definition Cybercrime: Limitation based on Law

When we discuss cybercrime, it will not be separated from the network security problem. Cybercrime comes from the word cyber which means cyberspace or the internet and crime which means crime (Rahardjo, 2002; Zulkefli, Singh, Shariff, & Samsudin, 2017). So, cybercrime is a crime in cyberspace. Cybercrime is all kinds of use of computer networks for criminal purposes and/or technology criminals by misusing the convenience of digital technology (Wahid & Labib, 2005; Rosidawati & Santoso, 2017). Cybercrime, is not a crime that should be underestimated. Even though they do not meet in person, cyber crime can have fatal consequences. *Cybercrime* has a distinctive character compared to conventional crime (Setiawan, 2005; Tamara, 2016):

1) Acts that are carried out illegally, without rights or unethical occur in cyberspace / areas, so it cannot be ascertained which country's legal jurisdiction will apply to it.
2) This action is carried out using any equipment that can be connected to the internet.
3) These acts result in material and immaterial losses (time, value, services, money, goods, self-respect, dignity, and confidentiality of information) which tend to be greater than conventional crimes.
4) The perpetrator is a person who masters the use of the internet and its applications. These acts are often carried out transnationally / across countries.

In Indonesia, cyber crime has been regulated in Law Number 11 of 2008 concerning electronic information and transactions in Article 35 which stated that: "*Every person intentionally and without right or against the law manipulates, creates, changes, removes, destroys electronic information and / or electronic documents with the aim that the electronic information and / or electronic documents are considered as authentic data.*"

Apart from the Law on Information and Electronic Transactions, the basic regulations in the handling of cyber crime cases in Indonesia are the implementing regulations for the ITE Law and also the technical regulations for investigations in each investigating agency (Ansyahrul, 2003; Sirait & Simangungsong, 2020).

B. Forms of Cybercrime

There are some types and forms of cybercrime occurred in Indonesia, as follows:

1) Based on the type of activity
   a. *Unauthotized Access to Computer System and Service*
      Crimes committed by infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network that he entered (Sofwan & Naufal, 2012).
   b. *Illegal Contents*
      It is a crime to enter data or information on the internet about something that is untrue, unethical, and can be considered to violate the law or disturb public order. For example, the posting of fake news or slander that will destroy the dignity and self-respect of other parties and so on (Hius & Nasution, 2012).
   c. *Data Forgery*
      The crime was falsifying data on important documents stored as scripless documents via the internet. This crime is usually shown in e-commerce documents by making as if a 'typo' occurred which will ultimately benefit the perpetrator because the victim will enter personal data and credit card numbers which can be misused. For example the case *www.klikbca.com* by hacker Steven Haryanto (Arifah, 2011).
   d. *Carding*
      Carding is counterfeiting and illegally using credit cards belonging to other parties to shop online for the benefit of the perpetrator (Widodo, 2003).
   e. *Cybersquatting* and *typosquatting*
      Cybersquatting is registering the domain name of a certain person or company and trying to sell it to that company at a higher price. Meanwhile, typosquatting is a crime by creating a pun domain, which is a

domain that is similar to someone else's domain name.

f. *Cyber Espionage*
It is a crime that utilizes the internet network to carry out spying against other parties, by entering the target party's computer network system. These crimes are usually directed against business rivals whose important documents or data are stored in a computerized system (Tahir, Raza, Ahmad, Kazi, Zaffar, Kanich, & Caesar, 2018).

g. *Cyber Sabotage* and *Extortion*
This crime is committed by disturbing, destroying or destroying data, computer programs or computer network systems connected to the internet. Usually this crime is carried out by inserting a logic bomb, computer virus or a certain program, so that data, computer programs, or computer network systems do not run as they should and run as the perpetrators want. In some cases that have occurred, the perpetrator of the crime will offer to repair the computer program data or computer network system that has been sabotaged, of course for a certain fee. This crime is often referred to as cyberterrorism (Saputra & Nasution, 2014).

2) Based on the Motive of Activity
   a. Cybercrime as a *pure crime*
   Crimes that are purely criminal acts are crimes committed because of the motive of crime. This type of crime usually uses the internet only as a means of crime (Ketaren, 2016).
   b. Cybrcrime as a "*gray*" crime
   With the type of crime on the internet that falls into the "*gray*" area, it is quite difficult to determine whether it is a crime or not. Given that the motive for his activities is sometimes not for crime (Ketaren, 2016).

3) Based on Activity Objectives
   a. Cybercrime that *attacks individuals*
   Crimes committed against other people with the motive of vengeance or fun which aims to destroy one's good name, to try or play with someone to get personal satisfaction (Ketaren, 2016).

b. Cybercrime that *attacks copyright*
Crimes committed against someone's work with the motive of creating, marketing, modifying the purpose of personal / public interest or for material / non-material purposes.

c. Cybercrime that *attacks the government*
Crimes committed with the government as an object with a terror motive, are hijacking or destroying the security of a government which aims to disrupt the government system, or destroy a country.

C. Domain Name in Cybercrime Cases

Definition of Domain Name is the internet address of a person, association, organization or business entity which is one of the important factors that must be taken in using the internet for commercial purposes or not. The address serves as a medium of liaison between a person or legal entity that posts information on an internet website and users of internet services (Rosidwati & Santoso, 2013; Marheni, 2013; Irfan, Ramdhani, Darmalaksana, Wahana, & Utomo, 2018).

Registration system domain name, is done by applying the principle of first come first served, meaning, whoever registers first, he is entitled to the domain name. Another system that is implemented is that domain name registration is carried out without going through a first examination process, so that to find out whether a domain name has been registered by another party or not, registrants must first contact the domain name registrar's organization (Moeljatno, 2005; Iman, Susanto, & Inggo, 2019).

In relation to cybercrime protection, several problems arise relating to brands and *Domain name* on the internet network (Rosidwati & Santoso, 2013; Ersya, 2017), namely:

1) A dispute arises if a third party deliberately registers a domain name that he thinks other people will be interested in. This method is widely used by someone who has no relationship at all with a brand that is registered as a domain name.
2) A dispute arises if a third party registers a list name that is the same or similar to someone else's trademark with the intention of being used by the registrant himself.
3) Domain name registrars are carried out by third parties based on the brands they own and without realizing it

have the same brands as other companies, but in different class categories of goods and services.

D. Understanding Typosquatting

Typosquatting is a trick on the internet that is used to trick internet users by creating a fake website using names very similar to the famous website. This method is almost the same as phishing, it's just that this method relies on a typo or typo on the website domain name that will be visited via an Internet browser (Sukayasa & Suryantho, 2018; Chintia, Nadiah, Ramdhani, Haedar, Febriansyah, & Kom, 2019). This sneaky trick is very widespread, website Indonesia is the most widely used for typosquatting tricks including bank sites. Because indeed many users in Indonesia often visit website banks to make transactions, for example on such as website click bca. What this bank's web domain address should be *www.klikbca.com* and there are parties who are not responsible for creating a fake website address of the BCA bank with the address *www.kilkbca.com*. So if a user makes a transaction via website such as *kilkbca.com*, he will enter the fake BCA website bank.

The fake website made by irresponsible parties is also very much like the real thing and has been targeted to trap typosquatting victims. And if an internet user will transact and get into the fake website and log in on the website, then the user's login identity will be easily stolen.

Typosquatting is basically an act of buying and operating domain names that are the result of variations of a well-known domain name, in the hope that the site is visited by internet users due to spelling or typing errors from the original site that the user wants to visit (Bunga, 2019; Jhon, 2018).

In 2001, the world of banking through the internet (e-banking) in Indonesia was shocked by the act of a man named Steven Haryanto, a hacker and journalist for the master web magazine. This man from Bandung deliberately created a genuine site but a fake internet banking service for Bank Central Asia (BCA). This idea arose when Steven also mistyped the website address. Steven buys domains with similar names *http://wwww.klikbca.com* (BCA internet banking original site), namely *http://www.klik-bca.com*, *http://www.kilkbca.com*, *http://www.clikbca.com*, *http://www.klickca.com*, *http://www.klikbac.com*. If we log in to

the five sites, users will get the same internet site as the klikbca.com site, except there is no transaction security and fake login from. When logging in, you will not enter the BCA internet banking facility and will display the message "*the page cannot displayed*". Fatal, by logging on to these sites, your internet username and pin will be sent to the site owner (Raodia, 2019; Widodo, 2013; Sjahdeini, 2018).

E. Laws Regarding Typosquatting

In connection with cases of disputes over domain names that have begun to spread in Indonesia, based on the description above, it is clear that the statutory instruments that can be used in this matter are Law Number 14 of 1997 concerning marks for typosquating cases.

1) Article 72
   a. Anyone who deliberately and without right commits the act as referred to in Article 2 paragraph 1 or Article 49 paragraph 1 and paragraph 2 shall be punished with a minimum of 1 month and / or a fine of at least IDR 1,000,000.00 (one million rupiah) or criminal a maximum imprisonment of 7 years and or a maximum fine of Rp.5,000,000.00 (five million rupiah).
   b. Anyone who broadcasts, exhibits, circulates, sells to the public a work or goods resulting from a copyright infringement or related things as referred to in paragraph 1 shall be punished with imprisonment for a maximum of 5 years and / or a maximum fine of Rp. 500,000,000.00 (five hundred million rupiah.)
   c. Anyone who deliberately and without rights reproduces the commercial use of a computer program, shall be punished with a maximum imprisonment of 5 years and / or a maximum fine of Rp. 500,000,000.00 (five hundred million rupiah).
2) Article 82
   Any person who deliberately and without rights uses the same mark substantially as the registered mark of another person or other legal entity, for goods and / or the like that is produced and / or traded, shall be punished with a maximum imprisonment of 5 years and a maximum fine of Rp. 000.00 (fifty million rupiah).

3) Article 378 of the Criminal Code concerning Fraud
   Anyone who with the intention of illegally benefiting himself or another person by using a false name or fake dignity with trickery or a series of lies moves another person to surrender something to him or to give a debt or to write off a debt, is threatened with fraud by imprisonment for the longest 4 years (Moeljatno, 2005).
4) Article 362 of the Criminal Code concerning Theft
   Anyone who takes property wholly or partly belonging to another with the intention of illegally possessing it, shall be punished for theft by a maximum imprisonment of 5 years or a maximum fine of sixty rupiahs (Moeljatno, 2005).

Meanwhile, the provisions state that someone who is without rights or not related to the owner of the mark or owner of a well-known name protected by trademark law can be sued by the trademark owner if:

1) Register, trade or use as a domain name
2) At the time of registering the domain name uses the same or identical or similar marks to the mark
3) When registering to use a well-known mark that is the same or similar to a well-known mark so it can be confusing.

4. CONCLUSION

It is clear, that cybercrime cases according to law recognized as all kinds of criminal activity through the internet network. In Indonesia the law regarding cybercrime has been regulated in Law number 11 of 2008 concerning electronic information and technology, which emphasized that everyone deliberately and without rights or against the law manipulates, creates, changes, removes, destruction of electronic information and/ or electronic documents with the aim that electronic information and electronic documents are considered as if the data is authentic. Cybercrime is not a crime that should be underestimated. Even though they do not directly visit the perpetrators, cybercrime can have fatal consequences for the victims. This research concluded and emphasized that typosquatting is a type of cybercrime crime where the perpetrator makes a play on a domain name that he wants to impersonate. After that the perpetrator will copy the entire contents of the

domain to be copied. So that if a user makes a typo they don't realize that he is accessing a mock web. Typosquatting generally attacks the banking domain or other payment transactions. Thus the perpetrator can obtain a username and password from the bank user. This of course will be detrimental to bank users and the bank itself because it will get a bad image. Therefore, there needs to be protection regarding typosquatting cases so that this crime does not spread widely. Furthermore, legally, typosquatting is considered a criminal act, but until now there is no law that explicitly and specifically regulates typosquatting. However, only in Law No. 14 of 1997 on trademarks for typosquatting. In this case, Indonesia in particular has not been given too much attention. So this crime can arise because of legal incapacity and including the authorities who reach him because this crime is virtual in which the perpetrator is not physically visible. Therefore it is necessary to have a special rule of law that regulates firmly and has permanent strength.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Ansyahrul, A. F. (2003). *Domain Name dalam Hukum Indonesia* (Doctoral Dissertation, Universitas Airlangga).

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2), 185-195.

Arikunto, S. (2013). *Prosedur Penelitian Suatu Pendekatan Praktik*. Jakarta: Rineka Cipta.

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. *Padjadjaran Journal of Law*, *6*(1), 69-89. https://doi.org/10.22304/pjih.v6n1.a4.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di

Indonesia dan Penanganannya. *JIEET (Journal of Information Engineering and Educational Technology)*, *2*(2), 65-69. http://dx.doi.org/10.26740/jieet.v2n2.p65-69.

Dharmaadi, I. P. A., Bakhrun, A., Saputra, D., & Putra, A. M. A. (2014, November). Typo-squatting crime in Indonesia online banking. In *2014 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 269-272). IEEE.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50-62.

Hius, J. J., Saputra, J., & Nasution, A. (2014). Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan dan Industri Dan Aspek Hukum Yang Berlaku. *Prosiding SNIKOM*.

Iman, N., Susanto, A., & Inggi, R. (2019). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *InComTech: Jurnal Telekomunikasi dan Komputer*, *9*(3), 186-192. http://dx.doi.org/10.22441/incomtech.v9i3.7210.

Irfan, M., Ramdhani, M. A., Darmalaksana, W., Wahana, A., & Utomo, R. G. (2018, November). Analyzes of cybercrime expansion in Indonesia and preventive actions. In *IOP Conference Series: Materials Science and Engineering* (Vol. 434, No. 1, p. 012257). IOP Publishing.

Jhon, R. M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *3*(1), 25-34. https://doi.org/10.15294/ijcls.v3i1.16945.

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35-42. https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/556.

Marheni, N. P. D. (2013). Perlindungan Hukum Terhadap Konsumen Berkaitan Dengan Pencantuman Desclaimer Oleh Pelaku Usaha Dalam Situs Internet (Website). *Thesis,* Universitas Udayana, Bali.

Moeljatno, M. (2005). *Kitab Undang-undang Hukum Pidana*. Jakarta: PT Bumi Aksara.

Moore, T., & Edelman, B. (2010, January). Measuring the perpetrators and funders of typosquatting. In *International Conference on Financial Cryptography and*

Data Security (pp. 175-191). Springer, Berlin, Heidelberg.

Muthia, F. R., & Arifin, R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia. *RESAM Jurnal Hukum*, *5*(1), 21-39. https://doi.org/10.32661/resam.v5i1.18.

Rahardjo, A. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: PT.Citra Aditya Bakti.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah dan Hukum*, *6*(2), 230-239. https://doi.org/10.24252/jurisprudentie.v6i2.11399.

Rosidawati, I., & Santoso, E. (2017). Pelanggaran Internet Marketing Pada Kegiatan E-Commerce Dikaitkan dengan Etika Bisnis. *Jurnal Hukum & Pembangunan*, *43*(1), 27-53. http://dx.doi.org/10.21143/jhp.vol43.no1.1507.

Setiawan, D. (2005). *Sistem Keamanan Komputer*. Jakarta: PT. Elex Media Komputindo.

Sirait, T. N., & Simangungsong, J. B. (2020). Analisis Yuridis Pelaksanaan Tugas Pokok Pengelola Domain Internet Indonesia. *Nommensen Journal of Legal Opinion*, *1*(01), 52-62. https://ejournal.uhn.ac.id/index.php/opinion/article/view/38.

Sjahdeini, S. R. (2018). e-commerce Tinjauan dari Perspektif Hukum. *Jurnal Hukum Bisnis*, *6*(6), 6-15.

Sofwan, H., & Naufal, M. (2012). *Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif dan Hukum Islam.* Yogyakarta: Universitas Islam Indonesia.

Spaulding, J., Upadhyaya, S., & Mohaisen, A. (2016, August). The landscape of domain name typosquatting: Techniques and countermeasures. In *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 284-289). IEEE.

Sukayasa, I. N., & Suryathi, W. (2018). Law Implementation of Cybercrime in Indonesia. *Soshum: Jurnal Sosial dan Humaniora*, *8*(2), 123-130.

Suryabrata, S. (1987). *Metode Penelitian*. Jakarta: Rajawali Press.

Tahir, R., Raza, A., Ahmad, F., Kazi, J., Zaffar, F., Kanich, C.,

& Caesar, M. (2018, April). It's all in the name: Why some URLs are more vulnerable to typosquatting. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications* (pp. 2618-2626). IEEE.

Tamara, A. D. (2016). *Analisis Kasus-Kasus Kejahatan Perbankan Melalui Internet Banking di Indonesia* (Doctoral dissertation, University of Muhammadiyah Malang).

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime).* Jakarta: PT.Refika Aditama.

Widodo, W. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Asswaja Presindo.

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63-74. https://doi.org/10.15294/ijcls.v5i1.23273.

Zulkefli, Z., Singh, M. M., Shariff, A. R. M., & Samsudin, A. (2017). Typosquat cyber crime attack detection via smartphone. *Procedia Computer Science*, *124*, 664-671. https://doi.org/10.1016/j.procs.2017.12.203.

Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact.

James Scott
Sr. Fellow, Institute for Critical Infrastructure Technology

ABOUT AUTHORS

Alif Kharimadohan is a Postgraduate Student at Faculty of Law Universitas Negeri Semarang. His area of research interests are concerning Criminal Law, Cybercrime Law, Cyberlaw, as well as Law and Technology.

FACULTY *of* LAW
UNIVERSITAS NEGERI SEMARANG, INDONESIA

Member of
APJHI, INDONESIA

Law Research Review Quarterly ■
Author Guidelines (2020 Version)

9 772716 341005

■ Author Guidelines

Law Research Review Quarterly (*L. Research Rev. Q.*) will publish the only paper strictly following Journal guidelines and manuscript preparation. All submitted manuscripts are going through a double-blind peer review process.

The aim of this journal is to provide a venue for academicians, researchers, and practitioners for publishing the original research articles or review

articles in legal studies, especially in law reform studies. The scope of the articles published in this journal deal with a broad range of topics, including: Criminal Law; Civil Law; International Law; Constitutional Law; Administrative Law; Islamic Law; Economic Law; Medical Law; Customary Law; Environmental Law and another section related contemporary issues in legal studies.

Review Policy

Manuscripts submitted will be subject to reviews by an editorial team board and a peer reviewer who are experts and familiar with the relevant field of research. After review process, the Managing Editor will inform the authors of the acceptance, rejection, or necessity of revision of the manuscript. All manuscript submitted will undergo the ***first stage*** of the review process carried out by the Internal Editor, which includes: suitability of the manuscript with focus and scope, manuscript template; writing standards (including the number of words), and similarity (plagiarism check by Turnitin). Regarding plagiarism check, the percentage limit allowed does not exceed 20%. After passing the first stage, the manuscript will be sent to be processed in ***the second stage***, namely the review process (through a double-blind peer-review system).

In carrying out article publication services, we refer to the following service time standards

Services	Duration
First Step Review (Internal Review)	1 week (7 working days)
Similarity Check	1 week (7 working days)
Second Step (Peer Review Process by External Reviewers)	1-2 month
Review Decision	Conditional
Notification of Acceptance (after the Author submitted the revised version of manuscript)	1 week (7 working days)
Copyediting & Proofreading	1-2 weeks
Publication	Conditional (based on the publishing schedule)

Open Access Policy

This journal provides immediate open access to its content on the principle that making research freely available to the public supports a greater global exchange of knowledge.

Paper Format

The word limit for the submission is 4000-15000 words (including of footnotes (if any) and abstract). Type in Times New Roman 11pt

The sequence of manuscripts following: Title; Abstract; Keywords; Introduction; Method (for original research articles); Results and Discussion; Conclusion; and References.

Main Headings of Manuscripts. Following main headings should be provided in the manuscript while preparing. Main headings, sub-headings and sub-sub headings should be numbered in the manuscript with the following example:

Main Heading
Main Heading
A. Sub-Heading
1. Sub-Sub Headings
**please follow and check our manuscript template*

- **Title**
  Title of articles are written with Cambria (26pt) and preferably not more than 14 words. Author(s) name, affiliations, and e-mail.

- **Abstract**
  The abstract should be clear, concise, and descriptive. This abstract should provide a brief introduction to the problem, objective of paper, followed by a statement regarding the methodology and a brief summary of results. Font Calibri (10 pt) and preferably not more than 250 words.

- **Keywords**
  Keywords arranged by alphabetically and should have at least two keywords and maximum five keywords separated by a semicolon (;).

- **Introduction**
  The introduction should be clear and provide the issue to be discussed in the manuscript. At the end of the paragraph, the author/s should end with a comment on the significance concerning identification of the issue and the objective of research.

- **Method**

  The method written in descriptive. This Method are optional, only for original research articles.

- **Result and Discussion**

  This section is the most important section of your article. Contains the results of the object of study and should be clear and concise. The title of Result and Discussion may not be used, Author can directly mention the main heading title.

- **Conclusion**

  Conclusion contains a description that should answer the objectives of research. Do not repeat the Abstract or simply describe the results of the research. Give a clear explanation regarding the possible application and/or suggestions related to the research findings.

- **References**

  References at the end of the manuscript should be written in *APA (American Psycho-logical Association)* Citation Style. Please use Reference Manager Applications like EndNote, Mendeley, Zotero, etc. (we suggest Mendeley). All publications cited in the text should be included as a list of Bibliography, arranged alphabetically by author.

  Books with an author:

  Suhadi, S. (2020). *Regulasi dan Implementasi Ganti Kerugian Tanah Desa dan Tanah Wakaf dalam Pengadaan Tanah.* Semarang: BPFH UNNES.

  Ali, A. (2012). *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicialpru-dence) Termasuk Interpretasi Undang-Undang (Legisprudence).* Jakarta: Kencana.

  Books with an editor or more:

  Sulistiyono, T., et.al. (eds). (2020). *The Implementation of Law and Its Implication to The Citizen: In the Public and Private Law Perspectives*. Semarang: BPFH UNNES.

  Irianto, S. (ed). (2009). *Hukum Yang Bergerak; Tinjauan Antropologi Hukum*. Jakarta: Yayasan Obor Indonesia.

  Journal articles:

  Das, D. Z., & Rohilla, B. S. (2020). Conflicting Interests of Legislators in India: An Exploratory Study. *Journal of Law and Legal Reform, 1*(4), 605-616. https://doi.org/10.15294/jllr.v1i4.39867

  Online sources:

  British Broadcasting Corporation. (2012). *Noken Papua Mendapat Pengakuan UNESCO*. Available from: *http://www.bbc.co.uk/indonesia/berita_indonesia/2012/12/121205_noken_unesco.* [Accessed May 16, 2015].

- **Footnotes**

  Bibliography citations are provided in bodynotes, however footnotes may be allowed with format:

  Books:

  Werner Menski, *Comparative Law in a Global Context, The Legal Systems of Asia and Africa*, London, Platinum Publishing Ltd, 2000, p. 16

  Section from a book:

  Eddy O.S. Hiariej. "Pemilukada Kini dan Masa Datang Perspektif Hukum Pidana" on Achmad D. Haryadi (ed), *Demokrasi Lokal: Evaluasi Pemilukada di Indonesia,* Jakarta, Konstitusi Press, 2012, p.182.

  Journal articles:

  Deb Zyoti Das & Bhanu Singh Rohilla, "Conflicting Interests of Legislators in India: An Exploratory Study", *Journal of Law and Legal Reform*, Vol. 1 No. 4, 2020, pp. 605-610

- **Figures/Graphics**

  The figures should be clearly readable and at least have a resolution of 300 DPI (Dots Per Inch) for good printing quality.

- **Table**

  Table made with the open model (without the vertical lines).

Publication Ethics

Law Research Review Quarterly (*L. Research Rev. Q.*) is a peer-reviewed journal as committed to keep and uphold the highest standards of publication ethics. All articles not in accordance with these standards will be removed from the publication at any time even after the publication. This statement explains the ethical behavior of all parties involved in the act of publishing an article in this journal, including the author, the editor in chief, the editorial board, the peer-reviewers and the publisher (Faculty of Law, Universitas Negeri Semarang). This statement is based on COPE's Best Practice Guidelines for Journal Editors.

Faculty of Law, Universitas Negeri Semarang as publisher of The Journal takes its duties of guardianship over all stages of publishing seriously and we recognize our ethical behavior and other responsibilities. We are committed to ensuring that advertising, reprint, or other commercial revenue has no impact or influence on editorial decisions. In addition, the Faculty of Law

Universitas Negeri Semarang and Editorial Board will assist in communications with other journals and/or publishers where this is useful and necessary.

Reprints

Upon final publication, the new issue will be made available online at:
https://journal.unnes.ac.id/sju/index.php/snh/index

Submission Manuscript

All manuscripts must be submitted online at:
https://journal.unnes.ac.id/sju/index.php/snh/user/register

If authors have any problems on the online submission, please contact Editorial Office at the following e-mail: *lawquarterly.journal@mail.unnes.ac.id*