DYNAMICS OF THE ELECTRONIC TRANSACTION INFORMATION LAW IN TACKLING *CYBERCRIME* IN INDONESIA

Lusia Sulastri[1], Rowela Cartin-Pecson[2]
[1]Bhayangkara Jakarta Raya University, Indonesia
[2]University of Mindanao, Philippines
lusia.sulastri@dsn.ubharajaya.ac.id[1], rowela_cartin@umindanao.edu.ph[2]

DOI: http://dx.doi.org/10.33603/hermeneutika.v3i2
Diterima: 14 Mei 2024; Direvisi: 15 Juli 2024; Dipublikasikan: Agustus 2024

Abstract: *The initial promulgation of Law Number 11 of 2008 concerning Information and Electronic Transactions had a different objective pendulum than the current use of the ITE Law. It turns out that some of these problems have actually raised the government's concern regarding the implementation of articles that are deemed not in accordance with the aims and objectives of making these regulations and even lead to a distortion of the democratic climate in Indonesia. This research is aimed at examining the legal politics of the enactment of the Electronic Transaction Information Law in Indonesia. This research is also aimed at examining the dynamics of the Electronic Transaction Information Law (UU ITE) in tackling* cybercrime *in Indonesia. Apart from that, it also analyzes the effectiveness of the Electronic Transaction Information Law (UU ITE) in tackling* cybercrime *in Indonesia. This research was conducted using empirical and normative research methods.*

Keywords: *Dynamics; ITE Law; Cyber crime*

I. INTRODUCTION

In early 2024, the Electronic Transaction Information Law was amended again through the issuance of Law (UU) Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. Amendments to the Electronic Transaction Information Law (UU ITE) aim to protect the public interest from all types of disturbances of order as a result of misuse of electronic information, electronic documents, information technology, or electronic transactions. Apart from that, the implementation of the previous regulations still gave rise to multiple interpretations and controversy in society, so changes needed to be made to create a sense of justice in society and legal certainty. One of the points of the revision of the new ITE Law is that there are no more 'rubber articles', namely Articles 27A, 27B, and 28 paragraph (3).

The first amendment to the ITE Law, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, is deemed unable to resolve problems that have sparked controversy in society, such as Articles 27, 28, 29, 36 , and 45 of the Electronic Information and Transactions Law. The application of these articles is considered problematic and will trigger debate in society regarding aspects of justice, apart from that, the government is also concerned about the application of articles which are deemed not in accordance with the aims and objectives of making these regulations. The use of these articles is considered to be able to capture subjects that should not be the target of the ITE Law, resulting in international attention regarding the democratic climate in Indonesia.

The implementation of the ITE Law has quite a large philosophical *legal gap* . The philosophy and objectives of the ITE Law were originally intended to ensure that electronic transactions or *e-commerce* run well and consumer rights are protected. The philosophy of enacting the ITE Law also aims to maintain Indonesia's digital space so that it is clean, healthy, ethical and can be used productively. However, in its implementation the ITE Law actually creates a sense of injustice. However, in reality, the existence of the ITE Law has often been used to ensnare people or groups of people for subjective reasons, so that law enforcement in implementing the ITE Law has so far caused concern, uncertainty and anxiety among the community in expressing their opinions (Agus Sahbani, https://www . Hukumonline.com/berita/a/filosofi-uu-ite-mestinya-returned-awal-pembangunan-lt602f6358dcc57/).

Cyber crime is increasingly common along with the rapid development and use of technology. Cases of data theft, *phishing* , *ransomware , online* fraud , *skimming* , OTP *fraud* , website/email hacking, SIM *swapping,* and illegal content are some types of cyber crime that are often found in Indonesia. Lecturer at the Faculty of Law, Pasundan University, Maman Budiman, said that currently Indonesia does not have strong regulations to prevent and take action against cyber crimes. Law No. 19/2016 concerning Information and Electronic Transactions (UU ITE) is considered insufficient to handle all aspects of cyber crime *(*https://www.unpas.ac.id/tunjungi-maraknya-case-cyber-crime-dosen-fh- unpas-need-special-regulation/). On the other hand, Ahmad M Ramli Professor of *Cyber* Law & Digital Regulations UNPAD, quite a lot of *cyber* crime articles of the ITE Law were revoked by the Criminal Code Law, namely: Article 27 paragraph (1), Article 27 paragraph (3), Article 28 paragraph (2) , Article 30, Article 31 paragraph (1), Article 31 paragraph (2), Article 36, Article 45 paragraph (1), Article 45 paragraph (3), Article 45A paragraph (2), Article 46, Article 47, and Article 51 paragraph (2). These articles were variously normatively reconstructed, reformulated and codified into the New Criminal Code Law. The Criminal Code Law was promulgated on January 2 2023 and will come into effect after a transition period of 3 years, starting from the date of promulgation (https://nasional.kompas.com

/read/2023/02/13/06450041/pasal-pasal-*cyber*-crime-uu-ite-revoked-by-uu-kuhpbaru?page=all#google_vignette).

This of course raises the question of what cyber crimes are in electronic commerce transactions and other legal acts in cyberspace such as *carding, hacking, cracking, phishing, booting, viruses, cyber squatting,* pornography, gambling, fraud, terrorism, dissemination of destructive information (how to make and use bombs) which is *cybercrime,* has been effectively tackled through the ITE Law. In fact, the cases that are handled through ITE are mostly just about issues of freedom of expression which actually accommodate human rights **(**Directorate General of Aptika, https://aptika.kominfo.go.id/2022/09/ahli- Hukum-dan-akademisi-besar -revision-uu-ite-narrow-space-multi-interpretation/). Moreover, the articles in the ITE Law were variously normatively reconstructed, reformulated and codified into the New Criminal Code Law.

Based on the discourse above, the author intends to conduct research with the following title: "The Dynamics of the Electronic Transaction Information Law (UU ITE) in Tackling *Cybercrime* in Indonesia" with a focus on studying problems including:

1. What are the dynamics of the Electronic Transaction Information Law (UU ITE) in tackling *cybercrime* in Indonesia?
2. Is the Electronic Transaction Information Law (UU ITE) effective in tackling *cybercrime* in Indonesia?

II. RESEARCH METHOD

In this study the approach method used is normative juridical, normative legal research is a process to find legal rules, legal principles, to answer legal problems, normative legal research is carried out to produce arguments, theories or new concepts as prescriptions (assessments) in the problems faced. Namely legal research that prioritizes research on norms or rules, literature studies and is supported by field studies on problems in the point of view of legal culture**.**

IV. DISCUSSION

1. Dynamics of the Electronic Transaction Information Law (UU ITE) in Tackling *Cybercrime* in Indonesia

Information technology has changed people's behavior and lifestyle globally, making the world borderless, and resulting in significant changes in various aspects such as social, cultural, economic and law enforcement. Although it contributes to human progress and welfare, information technology is also an effective means for unlawful acts. To maintain security in *cyberspace* , there are three approaches: technological, socio-cultural-ethical, and legal.

A technological approach is very important because without it, networks can easily be infiltrated, intercepted, or accessed illegally and without permission (Ramli, 2004: 2-4) . Therefore, legal and socio-cultural-ethical approaches as the next form of approach are very important. Legal approach in the form of the availability of positive law, it will provide guarantees of certainty and serve as a basis for law enforcement *if* violations occur.

The essence of the existence of the cyber world is a construction virtual world created by a computer which contains data abstract which functions as follows: (1) self-actualization; (2) container exchange ideas; and (3) a means of strengthening democratic principles. Humans can enter data systems and computer networks then get a feeling that they have truly entered a space of not having complete attachment to physical realities. Therefore, Activities in the cyber world have characters, namely: (1) easy, (2) the distribution is very fast and widely accessible by anyone and anywhere, and (3) can be destructive from posting insulting and/or defamatory material with using electronic media is extraordinary because has a pattern

of victimization which is unlimited. By understanding the nature of the cyber world and its character, regulation is needed separately to accommodate development and convergence Information Technology, which can be used as a tool in committing a crime (BPHN: 2015: 4).

The Indonesian government is aware of the birth of a new legal regime known as cyber law or telematics. This term refers to laws related to the use of information and communication technology, and is the result of convergence between telecommunications, media and informatics law. Apart from that, it is also known as the legal terms information technology, cyberspace, and mayantara. These terms arise because activities are carried out through computer and communication system networks, both locally and globally, using computer system-based information technology that can be viewed virtually. Legal problems often arise related to the delivery of information, communication and electronic transactions, especially related to the proof and implementation of legal acts through electronic systems .

Based on the historical background, the idea for an ITE Law began around the beginning of 2000 during the era of President Abdurrahman Wahid. At that time, there was still a legal vacuum in the realm of cyberspace. So that 2 state universities, the University of Indonesia and the University of Padjadjaran, each drafted a draft *cyberlaw bill* . Unpad led by Prof. Mieke Komar Kantaatmadja, drafted the *cyber* law bill as an umbrella law for all information technology regulations, called the Information Technology (IT) Utilization Bill. Meanwhile, the UI version of the *cyber* law bill was initiated by the Institute for Legal Technology Studies (LKHT) at the Faculty of Law, University of Indonesia, led by Edmon Makarim. The concept of the UI version of the *cyber law* bill is specific, and is called the Electronic Information and Electronic Transactions (IETE) Bill (Kumparan News, https://kumparan.com/kumparannews/wisata-terbesarnya-uu-ite-disahkan-era-sby-sempat-direvisi-era-jokowi-1vC3v5AMrhJ/full).

The drafting of the ITE Law is a combination of two bills, the Information Technology Crime Bill from Padjadjaran University and the E-Commerce Bill from the University of Indonesia. In 2003 the two bills were merged into one draft bill for discussion in the DPR (Rizkinaswara, https://aptika.kominfo.go.id/2019/02/menilik-histori-uu-ite-dalam-tok-tok-kominfo- 13/) . Even though it was passed in 2008, the history of the Information and Electronic Transactions (ITE) Law began in 2003, when the Law was officially discussed. In early May 2003, the government began discussing the Bill on the Utilization of Information Technology and the Bill on Electronic Information and Electronic Transactions (Kurniawan, https://narasi.tv/read/narasi-daily/histori-uu-ite).

The government stated that it had completed discussions on the ITE Bill in August 2003, four months after the bill began to be discussed. However, discussion of the ITE Bill stalled because it was never sent to the DPR for ratification. A year later, in November 2004, the new ITE Bill entered the DPR for discussion and processing. In 2005 the Ministry of Communication and Information was established and a Working Committee (Panja) was formed with 50 members (Rizkinaswara, https://aptika.kominfo.go.id/2019/02/menilik-histori-uu-ite-dalam-tok-tok- comminfo-13/). The DPR then held hearings on the ITE Bill in May-July 2006 with a composition of 13 chapters and 49 articles. After going through a series of hearings, the ITE Bill was only approved by the DPR for ratification on April 21 2008 (Kurniawan, https://narasi.tv/read/narasi-daily/histori-uu-ite).

There are several philosophical bases for the birth of Law of the Republic of Indonesia Number 11 of 2008 Regarding Information and Electronic Transactions, including:

a. National development is a continuous process that must always be responsive to various dynamics that occur in society;
b. The globalization of information has placed Indonesia as part of the world information society, necessitating the establishment of regulations regarding the management of Information and Electronic Transactions at the national level so

that the development of Information Technology can be carried out optimally, evenly and spread to all levels of society in order to make the nation's life more intelligent;

c. The rapid development and progress of Information Technology has caused changes in human life activities in various fields which have directly influenced the birth of new forms of legal acts;
d. The use and utilization of Information Technology must continue to be developed to safeguard, maintain and strengthen national unity and unity based on the Laws and Regulations in the national interest;
e. The use of Information Technology plays an important role in trade and national economic growth to realize social welfare;
f. The government needs to support the development of Information Technology through legal and regulatory infrastructure so that the use of Information Technology is carried out safely to prevent its misuse by paying attention to the religious and socio-cultural values of the Indonesian people;

Member of Commission II DPR RI Guspardi Gaus stated that the philosophy and objectives of creating the ITE Law should be returned to the initial intention of its formation, namely ensuring that electronic transactions or *e-commerce* run well and consumer rights are protected (Sahbani, https://www. Hukumonline .com/berita/a/philosofi-uu-ite-should-be-returned-initial-formation-lt602f6358dcc57/?page=1). When linked to the philosophical basis of the birth of Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions, it is clear that the use of Information Technology plays an important role in trade and national economic growth to realize social welfare, Law of the Republic of Indonesia Number 11 of 2008 Regarding Information and Electronic Transactions, it was born to support the development of Information Technology through legal infrastructure and regulations so that the use of Information Technology is carried out safely to prevent its misuse.

Technological information media has become an effective tool for committing unlawful acts, so it is important to regulate electronic acts in law to ensure that perpetrators do not escape legal responsibility. The distribution of pornographic material, pornographic material, gambling and acts of violence are examples of unlawful acts that are often carried out electronically, so the law must prohibit these kinds of acts. A common electronic crime is hacking or cracking, which can be committed from within or outside the country, so it is important for Indonesian law to cover actions that harm the interests of the state or citizens, both at home and abroad.

These crimes involve unauthorized use of or access to computers or electronic systems, whether private or government owned, with the aim of obtaining, changing, destroying, or eliminating information for personal gain. Electronic systems protected by the government include banking institutions, government institutions and other private parties. Electronic crime can also involve damage to transmission systems protected by the state as well as prohibiting anyone from using or accessing a computer without permission.

Other electronic crimes include disseminating, trading, or exploiting access information that could damage or abuse computers or electronic systems protected by the government. Therefore, it is important for the law to deal with all types of electronic crimes in order to protect the interests of society and the state. In everyday life, the actions of crackers and hackers can have far-reaching and serious impacts. For example, the disruption to the General Election Commission (KPU) website of the 1999 Legislative Election data is a clear example. Apart from that, power outages in several large cities in the United States and damage to the flight control system in Kansas are other examples of the negative impacts that can be caused by the actions of hackers and crackers (Mandala, 2004: 4-5).

The journey of the first 8 (eight) years of the ITE Law, namely from when the ITE Law was promulgated in 2008 until it underwent changes in 2016, namely with the enactment of Law no. 19 of 2016, shows the dynamics in society that want improvements to the articles of the ITE Law, especially regarding the criminal provisions for illegal content. The amendments to the ITE Law in 2016 were based on efforts to strengthen guarantees of recognition and respect for the rights and freedoms of other people and to fulfill fair demands in accordance with considerations of security and public order in a democratic society in order to realize justice, public order and legal certainty. .

Since its promulgation on April 21 2008 until now, the implementation journey of the ITE Law has experienced the following problems:

a. Public objections to Article 27 paragraph (3) of the ITE Law, especially regarding defamation and insults on the internet, resulted in two requests for constitutional review to the Constitutional Court. Examples of cases such as Prita Mulyasari versus Omni International Hospital and Saiful Mahdi from Unsyiah Aceh show the controversy surrounding the application of this article.
b. The first amendment to the ITE Law in 2016 was deemed insufficient to resolve existing problems, resulting in the issuance of a Joint Decree by the Minister of Communication and Information, the Attorney General and the National Police Chief as a responsive effort.
c. The initiative to create guidelines by the Minister of Communication and Information, the Attorney General and the National Police Chief regarding several controversial articles such as Articles 27, 28, 29, 36 and 45 is still considered inadequate due to problems related to the existence of the SKB and varying understanding among law enforcement officials.
d. The application of controversial articles not only raises debates about fairness, but also government concerns regarding interpretations that do not comply with the objectives of the law.
e. The use of articles that are not in accordance with their original purpose can pose a risk of attracting subjects who should not be the target of these regulations, as in the case of Saiful Mahdi, who attracted international attention to the situation of democracy in Indonesia.
f. The development of the need for law enforcement shows the need for criminal provisions that regulate the spread of fake news that can cause riots. (BPHN: 2021: 6-8).

Changes to the ITE Law were only realized in 2016 with several changes. There are 8 (eight) changes to the articles in Law 11 of 2008, namely:

a. Article 1 point 6 adds a new definition to the ITE Law which states that an Electronic System Operator is an entity that provides, manages and/or operates an Electronic System for its own or other parties' needs.
b. Article 5 remains with a new explanation that recognizes Electronic Information and/or Electronic Documents as valid evidence in the Implementation of Electronic Systems and Electronic Transactions, including in related legal processes.
c. Article 26 is expanded to protect the rights of personal data subjects regarding the deletion of irrelevant Electronic Information and/or Electronic Documents at the request of a court and the provision of a deletion mechanism in accordance with the provisions.
d. Article 27 has undergone changes with an emphasis on the norms of insult and defamation, as well as its implicit link to the Criminal Code.

e. Article 31 paragraph (3) and paragraph (4) have undergone changes regarding illegal interceptions.
f. Article 40 is expanded by adding the Government's obligations to prevent the dissemination of Electronic Information and/or Electronic Documents that violate the law and provides the authority to terminate access to them.
g. Article 43 has undergone changes regarding the investigation of cyber crimes, including searches and seizures that are adapted to the Criminal Procedure Code, as well as strengthening the authority of Civil Servant Investigators.
h. Article 45 was amended by reducing the threat of imprisonment for criminal offenses of insult, as well as inserting Article 45A and Article 45B related to this matter.

In the 13 years of implementing the ITE Law, there have been 10 cases of applications for judicial reviews to the Constitutional Court aimed at assessing the constitutionality of several articles in it, such as Article 27 paragraphs (2) and paragraphs (3), Article 28 paragraphs (2), Article 5, and Article 1 number 6. The main problem faced is related to the principles of lex certa and lex stricta of criminal offense norms in the ITE Law, the implementation of which varies in various regions. This gives rise to the view that the ITE Law has multiple interpretations, is elastic, and is considered to threaten press freedom and freedom of opinion.

To overcome the problem of diverse interpretations, the government chose to issue a Joint Decree between the Minister of Communication and Information, the Attorney General, and the Chief of Police on June 23 2021. This Joint Decree regulates Implementation Guidelines for Certain Articles of the ITE Law, in response to multiple interpretations and Controversy has arisen in society regarding several articles regulating criminal acts in the ITE Law.

Freedom of speech and freedom of opinion, as well as the right to obtain information through Information Technology, are recognized as means of advancing general welfare and making the life of the nation intelligent. Maintaining this independence and freedom is also the key to maintaining the integrity of the digital space, so that it is clean, healthy, ethical, productive and fair, as well as providing a sense of security and legal certainty for users and administrators of electronic systems.

In reality, in implementing Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, there are problems. The problems in question include:

a. the emergence of objections by some members of the public to several criminal provisions such as in Article 27 paragraph (3) and Article 28 paragraph (2), which have been submitted to *Judicial Review several times* at the Constitutional Court;
b. the first amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, which is considered still unable to resolve the problem;
c. the emergence of different understandings of several articles so that their application can be imposed on subjects that should not be the target of these provisions.

The Draft Law concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) was officially ratified on January 2 2024. The Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions was then amended by Law Number 1 of 2024. The philosophical basis for the promulgation of Law Number 1 of 2024 includes:

a. that in order to maintain Indonesia's digital space which is clean, healthy, ethical, productive and just, it is necessary to regulate the use of Information Technology and Electronic Transactions which provides legal certainty, justice and protects the public interest from all kinds of disturbances as a result of misuse of Electronic Information, Electronic Documents, Information Technology, and/or Electronic Transactions that disrupt public order;
b. that several provisions in Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, in their implementation still give rise to multiple interpretations and controversy in society so that changes need to be made to create a sense of social justice and legal certainty;

The second amendment to the ITE Law reflects the government's strategic policy in maintaining the integrity of Indonesia's digital space, ensuring clean, healthy, ethical, productive and just sustainability. It aims to strengthen guarantees of individual rights and freedoms, in line with the need for security and public order in the context of a democratic society. Several revised articles, such as Article 5 concerning electronic evidence, Article 13 concerning electronic certification, and Article 27 concerning prohibited acts, as well as criminal provisions, show a commitment to improving regulations related to technology and electronic transactions.

Apart from that, the changes also complement material covering digital identity in electronic certification, child protection in the use of electronic systems, and international electronic contracts. The main goal of this change is to create a digital ecosystem that is fair, accountable, safe and innovative. Multiple interpretations and controversial issues since the birth of the ITE Law, especially related to criminal provisions, are the focus of this change. The third generation of the ITE Law, which is inspired by Law Number 1 of 2023 concerning the Criminal Code, aims to eliminate the ambiguity that existed previously.

The formation of cyber law in Indonesia responds to rapid developments in the field of Information Technology, but also faces new challenges related to law enforcement in cybercrime cases, especially regarding defamation and insults. The dynamics of the ITE Law since its inception until now reflects efforts to adapt to technological changes and respond to problems that arise in society. The second amendment to the ITE Law is a step towards resolving the multi-interpretive and controversial problem which is a major concern.

2. The Effectiveness of the Electronic Transaction Information Law (UU ITE) in Tackling *Cybercrime* in Indonesia

Cybercrime or often known as *cybercrime* has many variations (Wahid and Labib, 2005: 43). Initially, in the academic text of Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions, legal violations in electronic trading transactions and other legal actions in cyberspace were a very worrying phenomenon, considering the actions of *carding, hacking, cracking, phishing, booting. , viruses, cybersquatting,* pornography, gambling, fraud, terrorism, dissemination of destructive information (how to make and use bombs) have become part of the activities of internet criminals and *Information and Communication Technology* (*ICT)* (Academic Manuscript, 2006: 4) .

This means that the concept *of cybercrime* that is intended to be addressed by Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions is aimed at tackling legal violations in electronic commerce transactions and legal actions in cyberspace. This is because violations of the law using information technology instruments are often difficult to solve, because in addition to the unlawful acts

being carried out by subjects using sophisticated technological means and their whereabouts are difficult to trace. The activities referred to are often carried out from outside Indonesian territory or vice versa where the subject is in Indonesia but the mode and *lex loci delicti* occur outside Indonesia, this makes the proof more difficult than ordinary unlawful acts (Academic Manuscript, 2006: 4) .

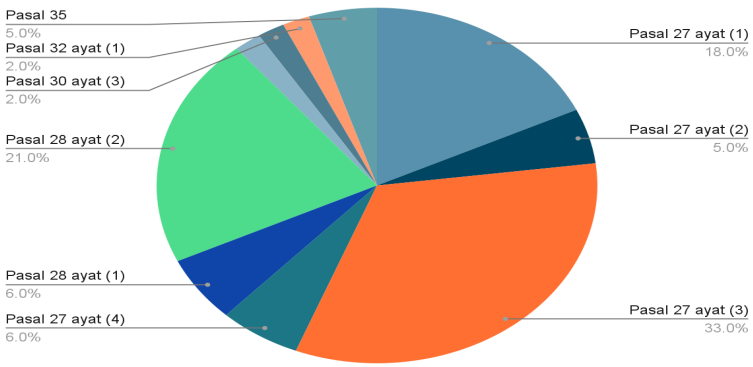
Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions regulates *cybercrime* into two forms , namely new crimes that use computers or electronic systems (*carding, hacking, cracking, phishing, booting, viruses, cybersquatting)* and old crimes (in the Criminal Code) carried out using electronic systems (violating decency / pornography, gambling, insulting and/or defaming , blackmailing and/or threatening , false and misleading news , spreading feelings of hatred or enmity towards certain individuals and/or community groups based on ethnicity, religion , race and intergroup (SARA) , and threats of violence or intimidation aimed at personally).

The effectiveness of the Electronic Transaction Information Law (UU ITE) in tackling *cybercrime* in Indonesia can be seen from the perspective of law enforcement **.** Conceptually, the meaning of law enforcement lies in the activity of harmonizing the relationship between values described in stable and embodied rules and attitudes of action as a series of final stages of value elaboration, to create, maintain and maintain peaceful social life (Soekanto, 2011). Law enforcement related to a system consists of sub-sub systems or elements that determine how a law works in synergy.

ID CERT in mid-2018 released a cyber report that occurred in May and June. From the reports issued, it is known that intellectual property rights crimes in digital technology occurred in 8,053 cases, spam reports occurred in 4,233 cases, network incidents occurred in 2,700 cases. Within a period of two months, the number of cyber incidents occurred was very high (Marwan, *et al.* , 2019: 1).

Based on data from Dittipidsiber (directorate of cyber crime), it turns out that from 2017-2020 there were 15 thousand reports investigated by Dittipidsiber. Of the 15 thousand reports, 32 percent or 5,064 reports were related to defamation, 1,169 reports were related to hate speech, and 1,050 reports were related to the distribution of pornography. From SAFEnet data, Damar explained specifically that those reported were groups of journalists, activists, academics, university students and workers who were targeted with problematic articles in the ITE Law. As for the people who report the ITE Law most often, Damar said that 68 percent are people who have power, including 42 percent are public officials, 22 percent are professional people, and 4 percent are rich people (Muldani, 2022: 154-155).

Data from a study by Kominfo and *The Institute for Digital Law and Society* (Tordilas), states that of the 350 decisions, Tordilas has compiled 193 decisions whose use of articles is divided as in the chart below:



Based on the chart above, Article 27 paragraph (3) of the ITE Law shows that it is the article that is widely used in judges' considerations in deciding on cyber incidents, namely

33% or 63 decisions out of 193 decisions compiled by Tordilas until the end of April 2020. This number is quite far apart. far compared to the order of the second and third articles, namely Article 28 paragraph (2) of the ITE Law, which has 40 decisions and Article 27 paragraph (1) of the ITE Law, which has 35 decisions (BPHN: 2021: 86). Based on complete law enforcement, namely up to the decision, of the 193 decisions downloaded and analyzed from the Supreme Court decision directory, 33 percent of the decisions relate to defamation articles, then 21 percent of the decisions relate to hate speech. 18 percent of the decisions relate to article 27 paragraph 1 or crimes of moral content and the remainder relate to crimes of illegal access, threats, forgery and extortion.

Based on data from the Civil Society Coalition which has compiled reports from 2016 to February 2020, it was found that cases related to articles 27, 28 and 29 of the ITE Law, showed a conviction *rate* of up to 96.8% (744 cases) of the total 768 cases occurred in 137 regencies/cities and the imprisonment rate reached 88% (676 cases) (Amnesty International Indonesia, et al., https://icjr.or.id/kertas-politik-dataan-dandesakan-community-sipil -top-revision-uu-ite/).

From the distribution of cases from 2016 to February 2020, it is known that cases subject to Article 27 paragraph (3) reached 286 cases, while those subject to Article 28 paragraph (2) reached 217 cases, and are not much different from those charged against Article 27 paragraph (1), namely reaching 238 cases. Meanwhile, in 2020, the SAFEnet Digital Rights Situation Report showed that there were 84 criminal cases, some of which used articles that were considered rubber.

The effectiveness of the Electronic Transaction Information Law (UU ITE) in tackling *cybercrime* in Indonesia can be seen from the security aspect of the technological approach, the substance and legal structure of which is absolutely necessary, because without security including law enforcement, network resources will be very easily infiltrated, the role of law enforcement officials. as well as being intercepted or accessed illegally and the community in the context of enforcement without the right to anticipate all laws and must also be supported by facilities and crime problems that intersect with infrastructure so that law enforcement with government information technology can be realized (Winarni, 2016: 23).

Based on the data presented by the author, law enforcement against *cybercrime* in cases such as violating decency / pornography, gambling, insulting and/or defamation , extortion and/or threats , false and misleading news , spreading individual hatred or enmity and/or certain community groups based on ethnicity, religion, race and intergroup (SARA) , and threats of violence or intimidation aimed at personally) are carried out well. In fact, cases related to articles 27, 28 and 29 of the ITE Law, show a conviction *rate* of up to 96.8% (744 cases) from a total of 768 cases that occurred in 137 districts/cities and with an imprisonment rate reaching 88% (676 case).

On the other hand, in cases of new crimes that use computers or electronic systems (*carding, hacking, cracking, phishing, booting, viruses, cyber squatting)* the handling of cases that use this technology actually experiences many problems. The results of a study by Kominfo and *The Institute for Digital Law and Society* (Tordilas) stated that the use of Article 35 of the ITE Law was only 5%, Article 32 paragraph (1) of the ITE Law was 2% and Article 30 paragraph (3) of the ITE Law was 2%. Thus, the number of cybercrime cases in the form of *Unauthorized Access to Computer Systems and Services, Illegal Access* , *Data Forgery, and Illegal Contents* regulated in Article 35, Article 32 paragraph (1), 30 paragraph (3) of the ITE Law is very small, even less than 10 %.

Winarni stated that law enforcement officials, in this case the police, were in the spotlight of *cracker victims* in handling *hacking activities* . The police have not been able to catch *the cracker* who hacked a site, including their inability to catch *the cracker* who attacked the National Police's own site, so the initial step in the labeling process was actually

obtained from mass media reports which intensively reported on *hacking activities* , this is related to the human resources of the enforcers The law is inadequate so it is necessary to improve its quality, because it is an obstacle in the process of disclosing *cyber crimes* , where the mode of *cyber crime* is developing rapidly (Winarni, 2016: 25).

Indonesia is the country with the second highest information technology crime rate in the world. This was reported by kominfo.go.id, it was stated that Indonesia was ranked second in the country with the highest information technology crime rate in the world after Japan. The high frequency of cybercrime in Indonesia is caused by the increasing number of internet users. Cybersecurity or *cybersecurity* is needed to anticipate the emergence of information technology crimes. Cyber security is an activity carried out to protect cyber space users from various threats or attacks in cyber space (Prayudi, Budiman, Ardipandato, & Fitri, 2018: 2)

The number of cyber security crimes in Indonesia has increased from 2014 to 2019. Based on 2020 research conducted by Lalugi. et. al, it was reported that in Indonesia there were 98 cases of cyber security crimes in 2014, 305 cases in 2015, 1207 cases in 2016, 1763 cases in 2017, 4000 cases in 2018 and 3000 cases in 2019. Based on the explanation above , in 2018 there was a drastic increase in the number of cyber security crime cases in Indonesia, reaching 4000 cases from 1763 cases in 2017. This shows that cyber security in Indonesia is still weak and needs improvement (Palinggi, Palelleng, & Allolinggi, 2020: 58).

In recent years, there have been three types of cybercrime in the public sector that have developed in Indonesia, namely *hacking, phishing* and *malware* . *Hacking* is an activity carried out by *hackers* to access or infiltrate a computer network illegally or without permission from the owner of the network (Kwarto & Angsito, 2018, p. 102). *Phishing* is a cyber crime that has the nature of threatening or trapping someone with the concept of luring that person. This crime is committed so that the victim is willing to provide information regarding personal data such as username and password or other important information (Wibowo & Fatimah, 2017: 5). Malware is a computer program that is created to break into or damage *software* or the operating system on a computer. One method used to spread malware is by inserting it into an application or certain file (Kwarto & Angsito, 2018, p. 103).

In its development, cases of cyber attacks in Indonesia have increased drastically in the last few years. Based on the 2018 annual report of *the Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center* or ID-SIRTII/ CC, there were around 232,447,974 cases of cyber attacks on networks in Indonesia. The biggest cyber threat in 2018 was the threat of *malware* whose activity was reported in 122 million cases in Indonesia (ID-SIRTII/CC, 2018). Then in 2019, according to the annual report of the BSSN National Cyber Security Operations Center, the number of cyber attack cases in Indonesia increased, reaching 290,381,238. In 2019 the biggest cyber threats in Indonesia were data leaks and cyber attacks using *malware* (BSSN, 2019). Furthermore, according to the 2020 National Cyber and Crypto Agency Annual Report, the number of cyber attacks in Indonesia reached 316,167,753 cases (BSSN, 2020).

The large number of cases of cyber threats that occur in Indonesia shows that the technological capacity and expertise in the cyber field possessed by the Indonesian government is still lacking compared to the capacity possessed by the perpetrators of these cyber threats. Technological developments that are becoming increasingly sophisticated also cause the threats that exist in cyberspace to become more sophisticated as well. This shows that BSSN as a national cyber security institution needs to always increase cyber security capacity in Indonesia and increase the expertise of various parties within it. These efforts are important to reduce the level of threats that exist in Indonesian cyberspace.

Winarni added that, in cases such as *cyber attacks,* there are often obstacles, especially in terms of arresting suspects and confiscating evidence, often the police cannot determine for sure who the perpetrator is, because the perpetrators carry out their actions via computers in

internet cafes. ", where in internet cafes it is rare to carry out "registrations", this is what makes it difficult for investigations to look for evidence. Likewise with *carding cases* , most of the victim witnesses are abroad, making it very difficult to carry out reporting and examinations to be questioned in the minutes of the examination of victim witnesses (Winarni, 2016: 25).

The Electronic Transaction Information Law (UU ITE) has not been effective in tackling *cybercrime* in Indonesia. The Electronic Transaction Information Law (UU ITE) currently touches more on old crime cases with new modes, namely using electronic means, such as defamation and hate speech. The Electronic Transaction Information Law (UU ITE) has not actually touched on many cases of crimes against cyber security such as *Unauthorized Access to Computer Systems and Services, Illegal Access* , *Data Forgery, and Illegal Contents*.

The Electronic Transaction Information Law (UU ITE) should not only be able to resolve the problem of defamation of hate speech, but return to its initial goal, namely ensuring that electronic transactions or *e-commerce* run well and consumer rights are protected from cybercrime . Thus, the Electronic Transaction Information Law (UU ITE) should prioritize cyber security. Cyber security is important for a country because it covers various aspects that can affect state security. However, Indonesia does not yet have official regulations or policies in law related to cyber security. The Indonesian government only has regulations and policies regarding information security in the ITE Law, which policies are not enough to build national defense through cyber security.

IV. CONCLUSION

The dynamics of the Electronic Transaction Information Law (UU ITE) in tackling *cybercrime* in Indonesia experiences a gradation of objectives, initially ensuring that electronic transactions or *e-commerce* run well and consumer rights are protected. from *cybercrime,* to focus on the punishment of defamation/insults in the world of *cyber* / *cyberspace* . Since it was promulgated on April 21 2008 until now, the implementation journey of the ITE Law has experienced various problems such as objections by some people to Article 27 paragraph (3) concerning defamation and/or insults, the first amendment to the ITE Law, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions which are considered unable to resolve the problem, and the implementation of articles which are considered problematic not only triggers debate in society regarding aspects of justice.

The Electronic Transaction Information Law (UU ITE) has not been effective in tackling *cybercrime* in Indonesia. The Electronic Transaction Information Law (UU ITE) currently touches more on old crime cases with new modes, namely using electronic means such as pornography, gambling, insulting and/or defamation , extortion and/or threats , false and misleading news . , spreading individual feelings of hatred or hostility . The Electronic Transaction Information Law (UU ITE) has not actually touched on many cases of crimes against cyber security such as *Unauthorized Access to Computer Systems and Services, Illegal Access* , *Data Forgery, and Illegal Contents* .

The Electronic Transaction Information Law (UU ITE) should not only be able to resolve the problem of defamation of hate speech, but return to its initial goal, namely ensuring that electronic transactions or *e-commerce* run well and consumer rights are protected from cybercrime. Apart from that, Indonesia should have official regulations or policies in law related to cyber security.

REFERENCES

Abdul Latif and H. Hasbi Ali. (2011). *Politics of law* . Jakarta : Sinar Graphics.

Abdul Wahid and Mohamad Labib. (2005). *Cyber Crime* .Bandung : PT. Refika Aditama .

Ade Maman Suherman. (2004). *An Introduction to Comparative Legal Systems* . Jakarta: Raja Grafindo Persada.

Agus Raharjo . (2002). *Cyber Crime*. Bandung : Citra Aditya.

Agus Sahbani, *The Philosophy of the ITE Law Should Have Been Returned Early in Its Formation,* https://www. Hukumonline.com /berita/a/filosofi-uu-ite-mestinya-returned-awal-pembesaran-lt602f6358dcc57/ .

Ahmad M. Ramli. (2004). *Cyberlaw and Haki in the Indonesian Legal System* . Bandung: Refika Aditama.

Amnesty International Indonesia. et al.. " *Policy Paper Notes and Civil Society Pressure on the Revision of the ITE Law"* . https://icjr.or.id/kertas-politik-dataan-dandesakan-community-sipil-atas-revisi-uu-ite/.

Awaluddin Marwan. *et al.* . (2019). *"Exploring the Decisions of the ITE Law. " The Institute for Digital Law and Society/Tordilas. Deus Media Van Tordillas (DMT)* (Volume 3. 2019).

BSSN. (2020). *Honeynet Project BSSN - IHP.* Jakarta: National Cyber and Crypto Agency.

Budiman Prayudi, A. Ardipandato. A.. & Fitri. A. 2018. *Cyber Security and Democracy Development in Indonesia.* Jakarta: DPR RI Expertise Agency Research Center.

Didi Krishna. (1993). *Dictionary of International Politics* . Jakarta: Grasindo.

Directorate General of Aptika, *Legal Experts and Academics Value of Revision of ITE Law to Narrow Multitafsir Space, https://aptika.kominfo.go.id/2022/09/ahli- Hukum-dan-akademisi- Value-revisi-uu-ite-persempit-ruang -multiple interpretations/*

E. Brata Mandala. (2004). *The threat of cyber terrorism and strategies for overcoming it in Indonesia.* Seminar Paper *The Importance of Information System Security in E-Government.* Jakarta : Indonesian Telematics Coordination Team.

Esmi Warassih. (2005) . *Legal Institutions A Sociological Study.* Semarang : PT. Suryandaru Utama.

F. Sugeng Istanto. (2004) . *Politics of law.* Yogyakarta : Gajah Mada University .

ID-SIRTII/CC. (2018). *Indonesia Cyber Security Monitoring Report 2018.* Jakarta: Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center.

Indra Safitri. (1999) . *Crime in the Cyber World" in Insider* . Jakarta: Legal Journal From Indonesian Capital & Investment Market.

KJ Holsti. (19 88). *International Politics. A Framework For Analysis* . Volume II. Translated by M. Tahrir Azhari . Jakarta: Erlangga.

Kumparan News. *History of the Formation of the ITE Law: Passed by the SBY Era. It was revised during the Jokowi era* . https://kumparan.com/kumparannews/bisnis-terbesarnya-uu-ite-disahkan-era-sby-sempat-direvisi-era-jokowi-1vC3v5AMrhJ/full.

Lawrence M Friedman. (2011) . *Legal System from a Social Science Perspective.* Translated by M. Khozim. Bandung: Nusamedia.

Leski Rizkinaswara . *Examining the History of the ITE Law in Tok-Tok Kominfo* . https://aptika.kominfo.go.id/2019/02/menilik-histori-uu-ite-dalam-tok-tok-kominfo-13/ .

M.H Wibowo. & Fatima. N. (2017). " *Phishing Threats to Social Media Users in the World of Cyber Crime"* , *JOIECT. Vol. 1. No. 1* . 1-5. doi://doi.org/10.29100/v1i1.69.g47

Moh. Afaf El Kurniawan. *History of the ITE Law in Indonesia: Regulatory Development and Controversy in the Digital World* . https://narasi.tv/read/narasi-daily/histori-uu-ite .

Mukti Fajar ND. et al. (2010) . *Dualism of Normative and Empirical Legal Research* . Yogyakarta : Student Library.

National Legal Development Agency . (2021). *Results of the Harmonization of the Academic Draft Law Concerning the Second Amendment to Law Number 11 of 2008 concerning*

Information and Electronic Transactions . Jakarta: Ministry of Law and Human Rights. Jakarta .

National Legal Development Agency, Ministry of Law and Human Rights. (2006). *Academic Manuscript of Draft Law Concerning Information and Electronic Transactions* . Jakarta: Ministry of Law and Human Rights.

National Legal Development Agency, Ministry of Law and Human Rights. (2015). *Final Report on Alignment of the Academic Draft Law on Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions* . Jakarta: Ministry of Law and Human Rights.

Quarto. F.. & Angsito. M. (2018). "The Influence of Cyber Crime on Cyber Security Compliance in the Financial Sector" in *Business Accounting Journal Vol. 11 No. 2* . 99-110. doi: http://dx.doi.org./10.30813/jab.v11i2.1382 .

Reta, Responding to the Rise in *Cyber Crime Cases, Unpas FH Lecturer: Needs Special Regulations* , https://www.unpas.ac.id/tunjungi-maraknya-case-cyber-crime-dosen-fh-unpas-perlu-regula-besar .

Rini Retno Winarni. (2016). *Effectiveness of Implementing IT Laws in Cyber Crime Crimes.* Journal of Law and Community Dynamics Vol.14 No.1 October 2016.

S.. Palelleng Sangatgi, S.. & Allolinggi. LR 2020. " *Increasing Cyber Crime Ratio with Socio-Engineering Interaction Patterns in the Final Period of the Society 4.0 Era in Indonesia* ", *Scientific Journal of Social Dynamics Vol. 4 No. 1* . 45-63. doi:10.38043/jids.v4il.2314

Sandro Gatra, " *Cyber Crime Articles of the ITE Law Revoked by the New Criminal Code Law* " , Click to read: https://nasional.kompas.com/read/2023/02/13/06450041/pasal-pasal-cyber- crime-uu-ite-repealed-by-new-uu-kuhp?page=all#google_vignette .

Satjipto Rahardjo. (20 11) . *Legal studies* . Bandung: PT. Aditya Bakti's image.

Soerjono Soekanto. (1989) . *A Sociological Review of Law on Social Problems.* Bandung: Alumni.

Soewarno Handayaningrat S. (20 02). *Introduction to Administrative Science Studies and. Management* . Jakarta: CV Haji Masagung .

Trisno Muldani. (2022). *Initial Implications of the Issuance of the SKB of the ITE Law Article 27 Paragraph (3).* MUKASI: Journal of Communication Sciences Vol. 1 No. 2 (May 2022).

Widodo. (2009) . *Punishment System in Cyber Crime* . Yogyakarta: Laksbang Meditama.