IJRS International Journal Reglement & Society
Volume: 2 Issue: 2, May-August 2021: Page 103-110
http://jurnal.bundamediagrup.co.id/index.php/ijrs
ISSN ONLINE: 2745-8350

Cyber Crime According to the ITE Law

Ismail Koto

Faculty of Law, University of Muhammadiyah Sumatera Utara, E-mail: ismailkoto@umsu.ac.id

Abstract

The development of this information technology in turn changes the social order and behavior. In fact, it does not only end there, but also changes the reality of the economy, culture, politics and law. Therefore, behind the positive benefits, internet technology also has a small negative impact. One of them is used as a means of committing crimes, hereinafter known as internet crime or cybercrime. The procedure used to collect data in this study is in the form of documentation, namely the guidelines used in the form of notes or quotes, searching legal literature, books and others related to the identification of problems in this study offline and online. Analysis of legal materials is carried out using the content analysis method (centent analysis method) which is carried out by describing the material of legal events or legal products in detail in order to facilitate interpretation in the discussion. In relation to the regulation of criminal penalties for cybercrime in Indonesia, until now the majority of cybercrime acts in Indonesia have not been regulated in clear legal norms in the legislation, therefore in adjudicating cybercrime the provisions of the Criminal Code and provisions in laws outside the Criminal Code are applied. Provisions in the Criminal Code that can be used to prosecute cybercrimes by means of extensive interpretation are provisions concerning the crime of counterfeiting (as regulated in Articles 263 to 276), the crime of theft (as regulated in Articles 362 to 367), criminal acts of fraud (how it is regulated in Articles 378 to 395), and criminal acts of destruction of goods (as regulated in Articles 407 to 412). Law Number 11 of 2008 concerning Information and Electronic Transactions (IET). The rules of criminal acts committed in it are proven to threaten internet users. Since the enactment of Law no. 11 of 2008 concerning Information and Electronic Transactions on April 21, 2008, has caused many victims. Based on the monitoring that has been carried out by the alliance, there are at least four people who are called the police and become suspects because they are suspected of committing criminal acts stipulated in the ITE Law.

Keywords:
Cyber Crime, ITE Law

How to cite:
Koto, Ismail. (2021). "Cyber Crime According to the ITE Law", IJRS: Internasional Journal Reglement Society 2, No. 2, Pages 103-110.

A. Introduction

Developing countries that lead to implementation and of course bring positive impacts and new services must be identified negatively, for example with science in anticipation of knowledge and technology currently solving various technical problems that are developing rapidly which are of course considered new so that they can be used as also have an impact on the level of material for the preparation of various human civilizations that carry implementing regulations. Third, the enrichment of a major change in the fields of law that is in nature shaping the patterns and behavior of the community. sectoral (new legal regime) will increase. In the State of Indonesia, in particular, adding to the lively dynamics of the law will lead to progress in science becoming part of the national legal system. computer is very fast.

The term information technology has started in the Criminal Code which is not widely used in the Act. This technology is ITE. Such as negligence or mistake, which is a development of negligent technology and mistakes are sentences that are often computerized which are combined with what is done by humans in cyberspace and telecommunications technology. Technology causes harm to itself, information itself is defined as one's own and other's, regulated technologically related to itself by using articles on processing data into information and certain articles. However, in cyberspace (the cyber process of distributing data/information is space) negligence is a fatal act that can cause losses that are

not within the boundaries of space and time. Even though the trend continues to develop in the country, technology also certainly brings various distributions of information, the implications of which must be immediately anticipated to contain the content of distribution and also to be wary of. This effort now and/or transmits and/or has given birth to a legal product to make information accessible in the form of Law Number 11 electronically and/or electronic documents of 2008 concerning Information Transactions containing insults and/or Electronics (UU ITE). But with defamation. Thus, the birth of the ITE Law has not been able to handle all the many factors that influence the problems concerning the effectiveness of the ITE law.

The problem is between being professional and optimal for other implementations because: first, with the birth of the role, authority and function of Law No. 11 of 2008 law enforcement officers, both in terms of Information and Electronic Transactions, explain the tasks that are charged not only by Law this can be known to themselves or in the community using information technology and legal practitioners. Second, various forms of technological developments in developing countries that lead to implementation and of course bring positive impacts and new services must be identified negatively, for example with science in the context of anticipating knowledge and technology currently solving various technical problems that are developing rapidly which are of course considered so that it can be used as an impact on the level of material for the preparation of various human civilizations that carry implementing regulations. Third, the enrichment of a major change in the fields of law that is in nature shaping the patterns and behavior of the community. sectoral (new legal regime) will be more and more In the State of Indonesia, especially adding to the lively dynamics of the law will lead to progress in science to become part of the national legal system.[1]

The development of this information technology in turn changes the social order and behavior. In fact, it does not only end there, but also changes the reality of the economy, culture, politics and law. Therefore, behind the positive benefits, internet technology also has a small negative impact. One of them is used as a means of committing crimes, hereinafter known as internet crime or cybercrime. Besides being known as cybercrime, this term is also called computer-related crime, which is a type of human crime that is committed in cyberspace or the internet through computer facilities to earn money.profit as much as possible from others, either by deceiving, deceiving the public, breaking into other people's accounts, or by randomizing a country's information system. This action is carried out by a handful of people who use it for their own interests but harm others. In fact, in some cases, this type of crime has the potential to cause greater harm to its victims than conventional or traditional types of crime. For example, theft through hacking mode.[2]

Based on the description above, the main problem can be drawn, namely how is the regulation of cyber crime law in Indonesian criminal law? And How is Cyber Crime Legal Arranged in the ITE Law? This research is a normative legal research, so according to the type and nature of the research, the data sources used are secondary data consisting of primary legal materials and secondary legal materials consisting of books, scientific journals, scientific papers and articles that can provide an explanation of the material primary law.[3] The data collection technique was carried out by library research with qualitative data analysis.[4] The procedure used to collect data in this study is documentation, namely the guidelines used in the form of notes or quotes, searching legal literature, books and others related to the identification of problems in this study both offline and online. Analysis of legal materials is carried out using the content analysis method (centent analysis method) which is carried out by explaining the material of legal events or legal products in detail in order to facilitate interpretation in the discussion.[5] This research was conducted using the problem approach, namely by approaching the results of theoretical empirical studies by looking at various opinions of experts, writers and studies of laws and regulations relating to issues based on legal principles and formulating legal definitions.[6]

[1] Rini Retno Winarni, "Efektivitas Penerapan Undang-Undang ITE Dalam Tindak Pidana Cyber Crime", Jurnal Hukum dan Dinamika Masyarakat 14 No. 1, (2016): p. 17.
[2] Nuria Siswi Enggarani, "Penanggulangan Kejahatan Di Indonesia", *Jurnal Ilmu Hukum* 15 No. 2, (2012): p. 149-169.
[3] Zainuddin dan Rahmat Ramadhani, *"The Legal Force Of Electronic Signatures In Online Mortgage Registration",* Jurnal Penelitian Hukum De Jure 2, No. 21, (2021): p. 244.
[4] Rahmat Ramadhani, *"Legal Consequences of Transfer of Home Ownership Loans without Creditors' Permission",* IJRS: International Journal Reglement & Society 2, No. 1, (2020): p. 33.
[5] Peter Mahmud Marzuki, *Penelitian Hukum,* Jakarta: Kencana Prenada Media Group, (2011), p.171.
[6] Rahmat Ramadhani, "*Peran Poltik Terhadap Pembangunan Hukum Agraria Nasional*", SOSEK: Jurnal Sosial dan Ekonomi 1, No. 1, (2020): p. 2.

B. Discussion

1. Cyber Crime Legal Regulations in Indonesian Criminal Law

The development of information technology has also formed a new world society that is no longer hindered by territorial boundaries and has turned everything that is far away from being near what is imaginary into reality. But behind this progress, has also given birth to new unrest with the emergence of sophisticated crime in the form of cybercrime.[7] Crimes using technology, namely information technology, especially computers and the internet (cybercrime) have reached an alarming stage. Advances in information technology, in addition to bringing to the business world a revolutionary (digital revolution era) that is all practical, turns out to have a terrible dark side, such as pornography, computer crime, even digital terrorism, waste information wars, and hackers. The problem of violating the law or by other names, crime is the responsibility of every element of society. Because apart from that crime is as old as the history of community life, it is also the embryo and construction of society itself. It's called social vulnerability and dangerous disease, of course it's logical if people show their attitude.

With regard to cybercrime perpetrators with unique characteristics, the author argues that the imposition of imprisonment on cybercrime perpetrators as practiced in Indonesia so far is an unwise move. This is caused by a discrepancy between the characteristics of the perpetrators of criminal acts with the system of fostering prisoners in the Correctional Institution, so that the purpose of punishment as regulated in the social law will not be achieved. The author argues that the type of imprisonment can be replaced with social work or criminal sanctions supervision, because there is a match between the characteristics of cybercrime perpetrators with the paradigm of punishment in social work crimes and criminal supervision, so that the purpose of punishment can be achieved. Social work and supervision crimes are more humane and prospective than imprisonment. The results of research in several countries, social work and supervision crimes are sufficient effectively applied to perpetrators of crime, including cybercrime. Eight countries in the world threaten cybercrime perpetrators with social work crimes, and this is not against the provisions of the convention on cybercrime. Legal instruments provide a basis or guideline for law enforcers to be applied to cybercrime perpetrators. As a positive law, its creation is of course through the mechanism of making legislation and at the same time attaching the nature of the ius constitutum, namely being a positive law that provides sanctions for criminal events or acts that use computers.

The formation of laws and regulations in the cyber world is also based on the public's desire to obtain guarantees of security, justice, and legal certainty. As the norm Cyber law or cyber law will be binding for each individual to submit and follow all the rules contained therein. There are four components in the criminal justice system, namely the police, prosecutors, courts, and correctional institutions. These four components of the criminal justice system must be able to work together and be able to form an integrated criminal justice system. The examination stage is regulated in detail in the Criminal Procedure Code, which in principle gives certain authorities (administrative-bureaucratic) institutions to implement the system, regulatory mechanisms, and guarantee the rights of suspects in the examination process.

In relation to the regulation of criminal penalties for cybercrime in Indonesia, until now the majority of cybercrime acts in Indonesia have not been regulated in clear legal norms in the legislation, therefore in adjudicating cybercrime the provisions of the Criminal Code and provisions in laws outside the Criminal Code are applied. Provisions in the Criminal Code that can be used to prosecute cybercrimes by means of extensive interpretation are provisions concerning the crime of counterfeiting (as regulated in Articles 263 to 276), the crime of theft (as regulated in Articles 362 to 367), criminal acts of fraud (how it is regulated in Articles 378 to 395), and criminal acts of destruction of goods (as regulated in Articles 407 to 412).

The following describes the application of criminal law provisions to prosecute cybercrime perpetrators in Indonesia:[8]

a. The application of the articles of the Criminal Code in cases that make computers the target of crime and cases that use computers as a means of crime:

[7] Andri Winjaya Laksana, "Cybercrime Comparison Under Criminal Law In Some Countries", Jurnal Pembaharuan Hukum, 5 No.2, (2018), p.217-226.
[8] Andri Winjaya Laksana, "Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif", Jurnal Hukum Unisulla 35 No. 1, (2019): p. 59-60.

1) The category of destruction of goods used for proof before the authorities, In the case of Unauthorized Transfer Payment at Bank Negara Indonesia (BNI) New York Agency Branch (1986), the Central Jakarta District Court in addition to imposing imprisonment on the defendant for being legally and convincingly proven violates Article 363 of the Criminal Code, namely theft committed by more than two or more people together, also proves that the defendant is legally and convincingly proven to have violated Article 233 of the Criminal Code, namely destroying goods used to prove something before the authorities. The decision was confirmed by the Jakarta High Court Decision and the Supreme Court Decision.
2) The category of theft, In the case of anauthirized Transfer Payment at Bank Negara Indonesia (BNI) New York agency branch (1986), the Central Jakarta District Court sentenced the defendant to imprisonment for being legally and convincingly proven to have violated Article 363 paragraph (1) of the Criminal Code, namely theft committed by more than 2 people together. The decision was upheld by the decision of the Jakarta High Court, and the Supreme Court's Decision.
3) The category of fraudulent competition, In the case of "domain name" PT. Mustika Ratu, the Supreme Court through Supreme Court Decision No.1082 K./Pid./2002, dated January 24, 2003, decided that the domain name mustika-ratu.com fulfills the offense of fraudulent forgery as stipulated in Article 382 bis of the Criminal Code. For that, the defendant (Chandra Sugiono) was sentenced to 4 (four) months in prison. This Supreme Court decision annuls the decision of the Central Jakarta District Court which in its decision acquitted the defendant of all charges.
4) Forgery category, the Defendant Petrus Pangkur was sentenced to 15 months in prison by the Sleman District Court (Yogyakarta) because it was proven legally and convincingly commit the crime of counterfeiting through the internet. Perpetrators buy goods using credit belonging to United States citizens through online trading (e-commerce). commerce). The provisions used as the basis for trying the accused are Article 378 of the Criminal Code. The total price of goods purchased is Rp. 4,000,000.00 (four million rupiah). The time required for the investigation of the case is eight months.

Based on the description of the crime case and the application of criminal law above, it can be concluded as follows:

a. Provisions in criminal law are applied by means of extensive interpretation;
b. The statutory regulations that explicitly regulate crimes that attack computers are only the Telecommunications Law. While the law which specifically regulates the piracy of computer programs only the Copyright Act;
c. Types of punishment imposed are imprisonment and fines;
d. When compared with the provisions in the Convention on Cybercrime, the forms of cybercrime in Indonesia that have been tried are data interference (ie the case of breaking into the KPU website), computer realeted fraud (ie cases of corruption in several banks), computer realeted forgery (ie cases of credit card fraud). by Petrus Pangkur), offenses realeted to infrigement of copyright and related rights.

Responding to the demands and challenges of global communication via the internet, the expected law (ius constituendum) is a legal instrument that is accommodating to developments and is anticipatory to problems, including the negative impact of internet abuse with various motivations that can cause victims such as material and non-material losses. . Countermeasures against information technology crimes need to be balanced with improvements and development of the criminal law system as a whole, which includes the development of culture, structure, and substance of criminal law. In this case, criminal law policy occupies a strategic position in the development of modern criminal law.

2. Cyber Crime Legal Arrangements in the ITE Law

The development of today's society is increasingly advanced and is supported by the growth of telecommunications technology, so that the bonds between countries are global in nature, resulting in a new world order. Thus, it cannot be denied that its impact on the development of the Indonesian people who are developing in the reform era has been faced with various crises, both political, economic, and socio-cultural, and these must be handled so that the Indonesian nation and state are still considered to

exist among the nations. in this world. The development of information and communication technology continues to grow rapidly, it is now possible to use information and communication technology through mobile devices. Activities that are usually carried out in the real world are now widely traded through gadgets (such as banking and mailing into virtual world activities). development of. Transfer transactions using i-Pad, Smartphone, cellphone, laptop. We no longer have trouble accessing information from all corners of the world. In addition to the many information and communication technologies that have provided support for many mobile devices, as well as the many availability of free hotspots in many places. The rapid development of information and communication technology is also accompanied by widespread abuse of information and communication technology, so that it becomes a very troubling problem, namely the occurrence of crimes that carried out in cyberspace or commonly known as "cybercrime".

Various crimes have occurred in this virtual world, these cases are of course detrimental and have a negative impact, this kind of cyber crime does not only cover Indonesia, but also covers the whole world. Some of the crimes that occur are caused by the widespread use of e-mail, e-banking and e-commerce in Indonesia. The increasing number of cybercrime cases (especially in Indonesia) has attracted the attention of the government to immediately enact laws that can be used to trap criminals in the world. virtual. The Indonesian government itself has incorporated the Cybercrime Law (UU Cyber) into the ITE Law Number 11 of 2008, and hopes that the ITE Law Number 11 of 2008 can overcome, reduce, and stop criminals in cyberspace. The Indonesian legal system does not specifically control cyber law, but several laws have regulated the prevention of cyber crimes, such as Law No. 36 of 1999 concerning Telecommunications, Law No. 19 of 2002 concerning Copyright, Law No. 15 of 1999. 2003 concerning the Eradication of Terrorism, as well as Law No. 11 of 2008 concerning Information and Electronic Transactions. These laws and regulations have criminalized the type of cybercrime and the threat of punishment for each violator.[9]

As something inherent in humans, crime also changes along with the development of communication technology developed by humans. Evil is imprinted on the human world itself. Technological developments in turn gave birth to a new world called cyberspace. This world is lived by the following humans by including the actions of their daily activities. This world, which is actually a tool and an intermediate world or “mediator” that connects individuals at long distances, has become a destructive space. It has become a new tool and medium for the birth of a new type of crime, hereinafter referred to as cybercrime, crimes committed in the community Internet Network. Although the essence of the crime remains the same, the motives and forms are different. Because it takes place in the internet network, the mode and form are also different. With in other words, it adapts to the space in which the crime is committed. As previously explained, this crime has different types and modes. Because it varies so that the resulting losses also vary, starting from the smallest to the largest. In other words, from the simplest to the most complex. In Indonesia, for example, these crimes were carried out ranging from credit card theft, hacking of several sites, tapping other people's data transmissions, for example via email, and manipulating data by preparing unwanted commands into computer programs to stealing other people's money. At a certain level, this Cybercrime crime can be become a threat to the stability of the country where it is difficult for the government to compensate for the techniques of crime committed with computer technology, especially internet and intranet networks.[10]

The following acts of cybercrime (cybercrime) are regulated in Law no. 11 of 2008 concerning Information and Electronic Transactions and Law no. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions, as follows:[11]

a. In Article 27 paragraph (1) of Law no. 11 of 2008 it is stated that "Every person intentionally and without rights shares or distributes or makes accessible Electronic Information or Electronic Documents that have contents that violate decency". However, the act of sharing/distributing/creating content of electronic information/electronic documents that violates decency (decency) is not explained by itself in Law no. 11 of 2008. Violation of ethics/decency

[9] Thantawi, “Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia,” *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala*, No. 1, (2014): p. 37
[10] Zaenal Abidin, “Kejahatan Dalam Teknologi Informasi Dan Komunikasi”, *Jurnal Ilmiah Media Processor*, 10 No.2, (2015), p. 509-516.
[11] Miftakhur Rokhman Habibi, “Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia”, *Jurnal Al-Qanun* 23 No. 2, (2020): p. 414-418.

through internet media itself refers to the Criminal Code. In the context of acts that violate decency through electronic media, Article 27 paragraph (1) of Law Number 11 of 2008 regulates information and electronic transactions, including online pornography and online prostitution. . If this crime is committed against children, it will become even more serious. One of the problems caused by the development of information technology through the internet is the number of sites that display pornographic scenes. It seems that nowadays, it is very difficult to protect the Internet from the interference of entertainment dealers who sell pornography.

b. Online gambling is regulated in Article 27 paragraph (2) of the Electronic Information and Transaction Law. The same regulation also states that: "Everyone intentionally and without rights shares/distributes/make accessible electronic information/electronic documents containing gambling content".
c. Defamation or humiliation in cyberspace is a prohibition regulated in Article 27 paragraph (3) of Law no. 11 of 2008, which reads: "Everyone intentionally, and without rights, shares/distributes/make accessible electronic information/electronic documents that contain insults or defamation contents." Lawmakers equate humiliation and defamation. Humiliation itself is an act, while one form of humiliation is pollution.
d. In Article 27 paragraph (4) of Law no. 11 of 2008 prohibits extortion or threats in cyberspace. In the article it is explained: "Anyone who knowingly and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents containing extortion and/or threats". Article 368 (1) of the Criminal Code includes qualifications acts that count as extortion or threats, namely: "Every person who intends to benefit himself or another person unlawfully (illegally), forces someone to give something belonging to that person or another person in whole or in part with violence or threats of violence or creates debt or write off a debt, will be punished with extortion and can be sentenced to up to 9 years in prison."
e. Law No. 11 of 2008 Article 29 stipulates that: "Any person who intentionally and without rights sends Electronic Information or Electronic Documents containing threats of violence or intimidation aimed at personally". The provisions regarding electronic information and transactions in Article 29 regulate acts of harassment, threats, or other actions taken to cause fear, including certain words or actions. These provisions are similar to cyberstalking arrangements in the United States, Canada, the United Kingdom and other countries. This action is carried out by utilizing information and communication technology, such as mail bombs, unsolicited hate mail, obsence or threatening email, and others.
f. The spread of fake news is regulated in Law no. 11/2008 Article 28 paragraph (1), reads: "Everyone intentionally and without rights spreads false/false and misleading news, which results in consumer losses in Electronic Transactions."
g. Article 28 paragraph (2) of Law Number 11 of 2008 concerning Information and Electronic Transactions regulates the crime, which reads: "Everyone intentionally and without rights disseminates information designed to cause hatred or hostility to certain individuals/community groups based on ethnicity, religion, race, and inter-group (SARA)".
h. Law No. 11 of 2008, Article 30 stipulates as follows:
    1) Anyone who knowingly, without rights or against the law (illegally) accesses another person's Computer or Electronic System in any way.
    2) Anyone intentionally, without rights or against the law (illegal) accesses (opens) a Computer or Electronic System in any way with the intention of obtaining Electronic Information or Electronic Documents.
    3) Anyone who violates, breaks through, exceeds, or breaks into the security system intentionally, without rights or against the law (illegal) accessing a Computer or Electronic System."

Law Number 11 of 2008 concerning Information and Electronic Transactions (IET). The rules of criminal acts committed in it are proven to threaten internet users. Since the enactment of Law no. 11 of 2008 concerning Information and Electronic Transactions on April 21, 2008, has caused many victims. Based on the monitoring that the alliance has done there are at least four people who are called the police and become suspects because they are suspected of committing criminal acts regulated in the ITE Law. The suspect or victim of the ITE Act is an active internet user who is accused of insulting or relating to defamatory content on the internet. Those accused under the IET Law tend to be subject to Article 27

paragraph 3 in conjunction with Article 45 paragraph 1 of the IET Law which is six years in prison and a fine of 1 billion rupiah. IET law can be used to defeat all cybercrime activities on the internet without exception.[12]

In the ITE Law, determining the existence of criminal provisions means determining the existence of prohibited acts, and which are therefore threatened with criminal sanctions. This is nothing but the formulation of criminal acts in the field of information and electronic transactions. By reviewing the articles in the ITE Law, it is possible to group actions that are prohibited in relation to criminal acts in the field of information and electronic transactions. The grouping is as follows:[13]

a. Deliberately and without rights distributing and/or transmitting and/or making accessible Electronic Information and/or Electronic Documents that have content that violates decency, gambling content, insults and/or defamation, extortion and/or threats; spreading false and misleading news that results in consumer losses in electronic transactions, disseminating information aimed at causing hatred or hostility to certain individuals and/or community groups based on ethnicity, religion, race, and inter-group (SARA); contains threats of violence or personal intimidation.
b. Intentionally and without rights or against the law accessing other people's computers and/or electronic systems in any way aims to obtain electronic information and/or electronic documents, violate, break through, exceed or break the security system.
c. Deliberately and without rights or against the law interception or wiretapping of electronic information and/or electronic documents in a computer and or certain electronic systems belonging to other people, and whether it does not cause any changes or causes changes, disappearances and/or termination of information electronics being transmitted.

Deliberately and without rights or against the law in any way change, add, reduce, transmit, damage, remove, transfer, hide an Electronic Information and/or Electronic documents belonging to other Persons or public property; move or transfer Electronic Information and/or electronic documents to the Electronic System of another person who is not entitled; changing, adding, reducing, transmitting, destroying, removing, transferring, hiding an Electronic Information and/or Electronic Document belonging to another Person or belonging to the public, resulting in the disclosure of an Electronic Information and/or Electronic Document that is confidential in nature to be accessible to the public with improper data integrity; and any action that results in disruption of the Electronic System and/or cause the Electronic System to not work properly.

C. Conclusion

In relation to the regulation of criminal penalties for cybercrime in Indonesia, until now the majority of cybercrime acts in Indonesia have not been regulated in clear legal norms in the legislation, therefore in adjudicating cybercrime the provisions of the Criminal Code and provisions in laws outside the Criminal Code are applied. Provisions in the Criminal Code that can be used to prosecute cybercrimes by means of extensive interpretation are provisions concerning the crime of counterfeiting (as regulated in Articles 263 to 276), the crime of theft (as regulated in Articles 362 to 367), criminal acts of fraud (how it is regulated in Articles 378 to 395), and criminal acts of destruction of goods (as regulated in Articles 407 to 412).

Law Number 11 of 2008 concerning Information and Electronic Transactions (IET). The rules of criminal acts committed in it are proven to threaten internet users. Since the enactment of Law no. 11 of 2008 concerning Information and Electronic Transactions on April 21, 2008, has caused many victims. Based on the monitoring that the alliance has done there are at least four people who are called the police and become suspects because they are suspected of committing criminal acts regulated in the ITE Law. The suspect or victim of the ITE Act is an active internet user who is accused of insulting or relating to defamatory content on the internet. Those accused under the IET Law tend to be subject to Article 27 paragraph 3 in conjunction with Article 45 paragraph 1 of the IET Law which is six years in prison and a fine of 1 billion rupiah. IET law can be used to defeat all cybercrime activities on the internet without exception. In the ITE Law, determining the existence of criminal provisions means determining the

[12] Andysah Putera Utama Siahaan, "Pelanggaran Cybercrime dan Kekuaan Yurisdiksi Di Indonesia", *Jurnal Teknik dan Informatika* 5 No. 1, (2018): p. 8.
[13] Supanto, "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy", *Jurnal Yustisia* 5 No. 1, (2016): p. 59-60.

existence of prohibited acts, and which are therefore threatened with criminal sanctions. This is nothing but the formulation of criminal acts in the field of information and electronic transactions. By reviewing the articles in the ITE Law, it can be grouped into actions that are prohibited in relation to criminal acts in the field of information and electronic transactions.

References

Abidin, Zaenal. (2015). "Kejahatan Dalam Teknologi Informasi Dan Komunikasi", *Jurnal Ilmiah Media Processor*, 10 No.2.

Enggarani, Nuria Siswi. (2012). "Penanggulangan Kejahatan Di Indonesia", *Jurnal Ilmu Hukum* 15 No. 2.

Habibi, Miftakhur Rokhman. (2020). "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia", *Jurnal Al-Qanun* 23 No. 2.

Laksana, Andri Winjaya. (2018). "Cybercrime Comparison Under Criminal Law In Some Countries", Jurnal Pembaharuan Hukum, 5 No.2.

Laksana, Andri Winjaya. (2019). "Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif", Jurnal Hukum Unisulla 35 No. 1.

Marzuki,Peter Mahmud. (2011).*Penelitian Hukum*, Jakarta: Kencana Prenada Media Group.

Ramadhani, R. (2021). *"Legal Consequences of Transfer of Home Ownership Loans without Creditors' Permission".* IJRS: International Journal Reglement & Society 2, No. 1.

Ramadhani, R. (2021). "*Peran Poltik Terhadap Pembangunan Hukum Agraria Nasional*". SOSEK: Jurnal Sosial dan Ekonomi 1, No. 1.

Siahaan, Andysah Putera Utama. (2018). "Pelanggaran Cybercrime dan Kekuaan Yurisdiksi Di Indonesia", *Jurnal Teknik dan Informatika* 5 No. 1.

Supanto. (2016). "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) Dan Antisipasinya Dengan Penal Policy", *Jurnal Yustisia* 5 No. 1.

Thantawi. (2014). "Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia," *Jurnal Ilmu Hukum Pascasarjana Universitas Syiah Kuala*, No. 1.

Winarni, Rini Retno. (2016). "Efektivitas Penerapan Undang-Undang ITE Dalam Tindak Pidana Cyber Crime", Jurnal Hukum dan Dinamika Masyarakat 14 No. 1.

Zainuddin dan Rahmat Ramadhani. (2021). "The Legal Force Of Electronic Signatures In Online Mortgage Registration", *Jurnal Penelitian Hukum De Jure* 21 No. 2.