International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 5
May, 2023
Pages: 119-130

Cyber Crime in Terms of the Human Rights Perspective

Muh. Akbar Fhad Syahril

Faculty of Law, Andi Sapada Institute of Social Sciences and Business, Indonesia

http://dx.doi.org/10.18415/ijmmu.v10i5.4611

Abstract

Regulatory efforts related to the ITE Law are a form of recognition and protection of human rights. Its philosophical foundation is Pancasila which is rechtsidee (legal ideals) and the idea of realizing the law in accordance with what it aspires to. This study aims to determine the extent of the handling of cybercrime in the City of Parepare. This research uses normative and empirical methods. The results show that cybercrime, which is essentially a human rights violation, is still very massive, especially in the City of Parepare where the handling process is still not running effectively, because the regulations governing cybercrime have not provided a deterrent effect for the perpetrators, so that until now cybercrime is still very frequent occur.

Keywords: *ITE Law; Cybercrime; Law Enforcement; Crime; Human Rights*

Introduction

Along with the development of technology that is increasingly popular,[1] it is discussed in various media, both print and electronic, observers in newspapers, academics in various scientific journals, and the government in-laws and regulations.[2]

Basically, every technology is created to fulfill a certain human need. Once created, the technology developed to be more effective and efficient to meet the intended needs; Old technology will be abandoned.[3] However, after it was created and developed, the use of technology can be in accordance with the purpose of its creation and development as well as its original purpose, as is known as a double-edged sword.

Technological developments are increasingly widespread and one of them is computer and internet technology, giving birth to a new world called the electronic world of virtual space, or the internet, which marks the start of a new era, namely the digital era or the information age. The electronic world of virtual space, or the internet, is a new world due to the creation of a union between humans and

[1] Karim, K., Herman, B., & Syahril, M. A. F. (2021). Criminological Analysis of Online Buying Fraud. DME Journal of Law, 2(01), 1-15.
[2] Syahril, M. A. F. (2021). Published Privacy Rights via Short Messages. Amsir Law Journal, 3(1), 11-19.
[3] Suardi, S., Asba, P., & Iksan, M. N. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Investasi Melalui Media Internet. *Jurnal Litigasi Amsir*, *10*(1), 72-83.

technology based on science and marks the start of the digital era. Just as in the conventional world, in the electronic world, virtual space is a 'living' community (cybersociety) that consists of millions of internet users from all over the world who communicate or interact with each other through computer networks.

Talking about information and communication technology that makes an electronic world a virtual space where people can be present without the need for physical existence; human existence and activities are manifested through 0's and 1. One's thoughts, intentions, and emotions can be manifested through bits. However, just like in the real world, in virtual space, there are also many crimes that are more often called cybercrimes. Crime in the virtual space can be in the form of crimes or actions of only people which are then discriminated against as a new form of crime that may occur in the virtual space. Therefore, it is necessary to apply legal rules and norms in the electronic world – virtual space to protect the public, including sanctioning criminals.

Cybercrime is also known as cybercrime which is loaded with the use of computers and the internet as well as cross-country which requires handling that cannot always be carried out based on conventional methods or methods. In various cases, the settlement of cybercrimes requires various parties, including law enforcement officers from other countries. Such cooperation can be carried out effectively if it is supported by both regional and international legal instruments that are in line with the national laws of each party.

Information and communication technology is very useful, and the potential for crime in this is also very large. Starting from cases of defamation, government and private websites being hacked, fraud on the internet, and so on, are events that can be read almost every day in various news. Various efforts have been made, starting from the making of law enforcement regulations, socialization, and others.

In addition, the urgency of personal data protection can be seen with the protection of personal data as part of human rights regulated in Article 12 of the Universal Declaration of Human Rights (UDHR) which provides a legal basis for member countries in terms of the state's obligation to protect and respect human rights. on the individual citizens of each country. In addition, in the International Covenant on Civil and Political Rights (ICCPR). This Convention was born on December 16, 1966, through Resolution 2200 A and entered into force on March 23, 1976. This international legal instrument provides more explicit protection of the rights of the human person. Article 17 paragraph (1) of the ICCPR states that no one will suffer arbitrary or unlawful interference with his privacy, home, or correspondence or any unlawful attack on his honor and reputation, everyone has the right to the protection of the law against such interference or attack. This Convention emphasizes that no one can be arbitrarily or unlawfully treated, or interfered with in his personal, family, home, or correspondence affairs. This convention further gives authority to each country to make legal instruments to protect its citizens. So that it is the obligation of countries that have ratified the Convention to implement it.

Like our physical world today, in the electronic world-virtual space, society requires both inter-community and inter-community regulation, from norms to laws. Technology and law are two elements that influence each other and they also affect society.

The development of information technology in such a way that the world has entered a new era of communication. This information technology has changed the behavior of the global community.[4] In addition, the development of information technology has caused the world to become borderless and caused significant social changes to take place so quickly. It is said that today's information technology has become a double-edged sword because, in addition to contributing to the improvement of human

[4] Lestari, S. E. (2017). Kajian Hukum dan Tindakan Bagi Pelanggaran Undang-Undang Nomor 32 Tahun 2009 Tentang Perlindungan dan Pengelolaan Lingkungan Hidup. *Mimbar Yustitia*, *1*(1), 21-35. https://doi.org/10.52166/mimbar.v1i1.567

welfare, progress, and civilization, it is also an effective means for the occurrence of unlawful acts. The occurrence of such unlawful acts, scope of the law must be expanded to be able to reach these acts.[5]

The regulatory approach in principle is the attitude of a person and society's actions (behavior) for violations of which are subject to sanctions by the State. Even though the cyber world is a virtual world, the law is still needed to regulate people's behavior for at least two reasons. First, the people who exist in the virtual world are people who come from the real world; The community has values and interests both individually and collectively that must be protected. Second, even though they occur in the virtual world, transactions carried out by the community have an influence in the real world, both economically and non-economically.

To overcome various legal problems that arise in the electronic world, the government has set various regulations, including enacting Law Number 11 of 2008 concerning Information and Electronic Transactions. In general, the regulations in the Information and Electronic Transaction Law are divided into two major parts, namely the regulation regarding electronic transactions and the regulation regarding prohibited acts (cybercrime).

The Law on Information and Electronic Transactions is the basis for handling cybercrimes, but the fact is that with this law, there are still many cases of cybercrime that until now have not solved many problems in the world of cybercrime.

Method

This study uses normative and empirical.[6] This research is carried out by examining the principles, conceptions, doctrines and legal norms related to cybercrime. This research is descriptive-analytical, using qualitative analysis methods.

Discussion

Prohibited Acts According to Law Number 11 of 2008 concerning Electronic Information and Transactions

From a juridical point of view, what is meant by crime is an act that violates or contradicts what has been determined in the law or more specifically that an act that violates the prohibitions stipulated in the law, and does not fulfill or oppose the orders stipulated in the legal rules applicable in society. where the person concerned lives in a community group.

Everyone who commits a crime will be given a criminal sanction as regulated in Book II of the Criminal Code (KUHPidana) which is stated it as a crime. So juridically, it is a form of behavior that is contrary to human morals, is detrimental to society, is anti-social, and violates the provisions of the Criminal Code.

From a sociological perspective, sociological crime according to non-law or crime according to flow is a human behavior created by society. Although society has a variety of different behaviors, they will have the same pattern. Symptoms of crime are natural processes of interaction between sections in society that have the authority to formulate crimes and which community groups commit crimes. Crime is

[5] Suharyanto, B. 2013, Tindak Pidana Teknologi Informasi (Cyber Crime): Urgensi Pengaturan dan Celah Hukumnya, Jakarta: Rajawali Pers

[6] Sampara, S., & Husen, L. O. (2016). Metode Penelitian Hukum. *Makassar: Kretakupa Print*.

not solely influenced by the amount of loss it causes or because it is immoral, but is more influenced by personal or group interests so that these actions harm the interests of the community, both material loss and loss/danger to life and human health., although it is not regulated in the criminal law.

Cybercrime is defined as a computer crime. Regarding the definition of computer crime itself, until now there is no opinion among scholars about the meaning or definition of computer crime. Computers in English are still not uniform. However, scholars generally accept the term "computer crime" because it is considered more broadly and commonly used in international relations.[7]

The idea of Cybercrime is significantly new, but there is confusion between academics, computer security experts, and actual Cybercrime-level users.[8] (Sarah Gordon, 2006) The gradual development of cybercrime from relatively low levels of crime committed by individual specialist offenders to mainstream or high-volume crimes 'such as organized and industrial'.[9]

The British Law Commission defines "computer fraud" as computer manipulation in any way money is done in bad faith to obtain money, goods or other profits or is intended to cause harm to others. Madeel divided "computer crime" over two activities, namely:

(a) The use of computers to commit acts, theft, or concealment intended to obtain financial gain, profit, property, or services;
(b) Threats to the computer itself such as theft of hardware or software, sabotage, and extortion.

The information technology system in the form of the internet has been able to shift the paradigm of legal experts towards the definition of computer crime as previously stated, that initially, legal experts focused on tools/hardware, namely computers. However, with the development of information technology in the form of an internet network, the focus of the identification of the definition of cybercrime is further expanded, namely the extent of activities that can be carried out in the internet/virtual world through the information system used. So, it is not just the hardware component that the crime is defined as cybercrime, but it can be expanded in the scope of the world explored by the information technology system concerned, so it would be more appropriate if the meaning of cybercrime is information technology crime, as stated by N. A. Barda as a cybercrime.[10]

According to Widodo, crime in the cyber world or cybercrime is a new form of crime based on information technology by utilizing computer hardware and software. Cybercrime is an act that is carried out by using a computer as a means/tool or a computer as an object, whether to gain profit or not, to the detriment of other parties.[11]

The rule of law for cybercrime is something that has its own challenges. This is because the laws and regulations concerning cybercrime in Indonesia are "as long as corn". The laws and regulations have been set forth in Law Number 11 of 2008 concerning Information and Electronic Transactions.

Therefore, with the age of the law still very easy, it takes time to evaluate the law in question. This is because as a new law, it takes time to study and analyze the entire article in the law enforcement process.

[7] Putlitbang Hukum dan Peradilan Mahkamah Agung RI. 2004. *Naskah Akademis Kejahatan Internet* (*cybercrime*).
[8] Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2(1), 13-20. https://doi.org/10.1007/s11416-006-0015-z
[9] Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. The Journal of Economic Perspectives, 23(3), 3–20. https://doi:10.1257/ 089533009789176825
[10] Sitompul, J. (2012). Cyberspace, cybercrimes, cyberlaw: tinjauan aspek hukum pidana. PT Tatanusa.
[11] Nasrullah, R. (2022). *Teori dan riset media siber (cybermedia)*. Prenada Media.

Before constructing the legal regulations regarding the Information and Electronic Transaction Law in detail, it is interesting to review the preparation of the legal instruments regarding cybercrime produced by the G-8 in the communique on 9-10 December 1997.[12] The meeting contained 10 principles and 10 action agendas that could be taken in anticipating the crime in question, namely:

1. There is no safe haven for them to use information technology;
2. Investigations and prosecutions of high-tech international crimes must be coordinated among countries concerned, regardless of where the adverse consequences occur;
3. Law enforcement officers must be trained and equipped in dealing with high-tech crime;
4. The legal system must protect the confidentiality, integrity, and existence of data and systems from unauthorized acts and ensure that serious misuse should be punished;
5. The legal system should allow for the protection and rapid access to electronic data, which is often critical to a successful criminal investigation;
6. Arrangements for mutual assistance must ensure timely collection and exchange of evidence, in cases related to high-tech crime;
7. Cross-border electronic access by law enforcement to the existence of general information, does not require authorization from the country where the data is located;
8. Forensic standards for obtaining and proving the authenticity of electronic data in the context of criminal investigations and prosecutions must be developed and used;
9. For practical purposes, information and telecommunications systems should be designed to help prevent and detect network abuse, and should facilitate the search for criminals and the collection of data;
10. Working in this environment must coordinate with other relevant work in the information age to avoid policy duplication.

The action agenda includes:

1. Use of a network of highly knowledgeable personnel to ensure the timely, effective reaction to high-tech cases of a transnational nature and design a 24-hour ready point of contact;
2. appropriate measures to ensure that law enforcement personnel are adequately equipped and employed to carry out high-tech crime tasks and assist law enforcement agencies in other countries;
3. Reviewing the existing legal system to ensure that there has been the criminalization of the telecommunications and computer systems and to promote the investigation of high-tech crimes;
4. Take into account the various issues raised by high-tech crimes as far as relevant when negotiating mutual assistance agreements;
5. Continue to examine and develop what can be done, with respect to evidence safety before carrying out and fulfilling requests for assistance, cross-border investigations, border investigations, and computer data tracing, where the location of the data is unknown;
6. rapid procedures for obtaining traffic data from across networks and communication links and assessing ways to rapidly add such data internationally;
7. cooperate with industry to ensure that new technologies can facilitate efforts to combat high-tech crime by protecting against gathering harmful evidence;
8. Ensure that in critical and appropriate cases, receive and respond to mutual assistance, and requests relating to high-tech crimes through rapid and trusted means of communication, including voice, fax, or email, with a written confirmation as a follow-up whenever required;
9. Encourage internationally recognized institutions in the field of telecommunications and information technology to continue providing the public and private sector, standards for communication technology and data processing that are safe and reliable;
10. Demand and use appropriate forensic standards to obtain and prove the authenticity of electronic data used for investigation and prosecution.

[12] Maskun, S. H. (2014). *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Prenada Media.

The above description can be used as a reference in the implementation of the Electronic Information and Transaction Law and related national laws and regulations (criminal law), which in this case is still a colonial legacy that is still being maintained. Although it is realized that the ten principles and agenda are something that must be implemented, at least they will be considered in demonstrating the implementation of the law.

Based on empirical experience prior to the enactment of the Electronic Information and Transaction Law, the legal rules that are most often used in Indonesia when cybercrimes occur are positive rules from the Criminal Code (KUHP) and the Criminal Procedure Code (KUHAP). The Criminal Code (KUHP) in particular is still seen as a fairly adequate legal basis, although to be honest this is not entirely true. However, there is no other choice in the middle of the law in the field of technology and information.

To elaborate on cybercrime in the context of positive law, first the criminal element is reduced as regulated in the Criminal Code (KUHP) accompanied by pictures showing the condition of the information system. An act can be punished, if it fulfills the elements of a criminal act (delict), not all acts can be punished if it is stated in the formulation of the offense.

In this context, the act must meet two conditions, namely an act against the law and a disgraceful act. These two conditions are seen as general conditions for a crime to be punished. The formulation of the offense in the law is a benchmark or basis for it to be said that an act is a crime. Regarding the nature of being against the law, it is also divided into the nature of being against the formal law and the nature of being against the material law.

In practice in Indonesia, criminal acts using computers have always been a type of crime that is difficult to classify as a crime. This is because in the enactment of Article 1 paragraph 1 of the Criminal Code there are no acts that can be punished if there are no regulations governing them (*nullun delictum noela poena sine pravia lege poenali*). The provisions of Article 1 paragraph 1 are felt to be obstacles in law enforcement in the field of computer crime and cybercrime in particular.

Therefore, in subsequent developments, both computer crime and cybercrime seem to be moving in place in solving cases of computer crime and cybercrime. Even if the provisions of Article 1 paragraph 1 are ignored, the next problem that arises is the necessity to interpret the meaning of the article so that it is adapted to the problems at hand.

The classification of acts that are prohibited in the Information and Electronic Transaction Law are described in Article 27 to Article 37 of the Electronic Information and Transaction Law. The construction of the article regulates in more detail the development of traditional modes of crime as stated in the Criminal Code (KUHP).

Article 27 of the Electronic Information and Transaction Law, for example, regulates decency, gambling, defamation, as well as acts of extortion and threats. The construction of Article 27 of the Electronic Information and Transaction Law above explains the development of the mode of crime and/or violation by using computer/internet media (in the form of electronic information/documents). This is very important, especially in assisting law enforcement in processing and adjudicating cases that have used electronic information media to smooth the crimes/violations committed.

Furthermore, Article 28 of the Electronic Information and Transaction Law regulates consumer protection and SARA aspects. This is very reasonable considering that many trade transactions are carried out using computer/internet media where both producers and consumers have never met each other. So that the aspect of trust plays an important role in trade transactions.

On the other hand, the issue of SARA is a national issue that is very vulnerable to conflict. Indonesia as a nation that has a fairly high level of heterogeneity makes "SARA" a product of conflict that is very easily ignited. Therefore, the development of the “SARA” optimization mode as a conflict-prone product must be regulated by adjusting the development of modes that use computer/internet media.

Article 29 of the Electronic Information and Transaction Law can be considered as a very significant development in the legislation regarding threats that are often carried out and/or directed at someone using electronic information/document media. The development of electronic products greatly facilitates a person to facilitate his evil steps in achieving the desired goal.

Construction of Article 30 of the Electronic Information and Transaction Law clearly states that an unlawful act is carried out by a person (a criminal) against another person's electronic system with the aim of obtaining electronic information/documents and/or attempts to break in and break into. that violates and exceeds the system. security is prohibited.

According to Romli Atmasasmita, Article 31 implies the legality of wiretapping, especially regarding the rampant wiretapping carried out by law enforcement officers, more specifically the wiretapping action carried out by the Corruption Eradication Commission (KPK) in eradicating corruption cases.

In the practice of countries in the world, wiretapping is only possible by law enforcement agencies in the context of the tasks assigned to them. However, the electronic information and transaction laws do not specifically specify which law enforcement agencies may exercise this authority. This is certainly different from the Telecommunications Law which limits its mention. Therefore, the mandate to establish law enforcement agencies authorized to conduct wiretapping, both in the information and electronic transaction law and the telecommunications law, must be formulated and issued in the form of a Government Regulation (PP) which has not yet been stipulated. reported. For more details, Article 31 of the Law on Information and Electronic Transactions.

Article 32 and Article 33 of the Electronic Information and Transaction Law regulates the protection of confidential information and/or electronic documents, both belonging to other people and public property.

Furthermore, Article 34 to Article 37 of the Electronic Information and Transaction Law is focused on supporting the sound of articles 27 to 33 which are included in the category of prohibited acts, except for Article 34 paragraph (2) of the Electronic Information and Transactions Law. which states that it is not a crime if it is imposed to carry out research activities, testing Electronic Systems, for the protection of the Electronic Systems itself legally and not against the law.

Legal Process for Handling Cyber Crime in Parepare City

Before discussing the legal process of cybercrime, it is necessary to know that cybercrime is a crime that is engaged in computerization using the internet network. According to the grammar of the Big Indonesian Dictionary, computerization is "the use of computers (in calculating, processing data, etc.) on a large scale". (Ministry of National Education. 2008). Of course, in a crime there must be a handling of the crime. To find out the course or legal process for handling cybercrime.

Cybercrime is a tough job for law enforcement officers, especially in the Parepare area. Wahyudi Djafar, researcher and Deputy Director of Research at ELSAM (Institute for Community Studies and Advocacy) revealed that digital attacks can be in the form of active or passive attacks, even in the form of semantics. The majority of NGOs in Indonesia have not seriously taken preventive measures against digital attacks.

Based on the cybercrime case in Parepare City, South Sulawesi, the Criminal Investigation Unit (Reskrim) handles all criminalization's that occur in Parepare City, specifically in handling cybercrime at the National Police Headquarters. Because cybercrime is a special crime that is equated with corruption in terms of the expert investigation process at the Head of the Tipikor Headquarters who handles these special crimes.

Many cybercrimes begin with unauthorized access to computer systems. Information systems can be targeted for the data they contain, including banking and credit card details, commercial trade secrets, or confidential information held by governments. The theft of personal financial details has provided the basis for a growing market in such data, which enables fraud on a significant scale.[13]

The type of cybercrime that is handled is "posting through social media (Facebook)", namely crimes that are engaged in computerization using the internet network, in line with the above, in the rules of Law Number 11 of 2008 concerning Information and Electronics. Transactions in Chapter VII concerning actions prohibited in Article 27 paragraph (3) which reads:

> "Any person intentionally and has the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that have the content of contempt and/or defamation".

The type of cybercrime that is still very prevalent in Parepare is a type of crime of humiliation or defamation against someone committed by cybercrime perpetrators by posting posts/making comments using personal Facebook accounts, where the perpetrator uses the social media means of the Parepare City Government Observer Facebook group which contains writings/comments accusing/attacking someone's honor or self-esteem. Looking at the type of cybercrime handled in Parepare City in enforcing the law, of course, there are efforts to overcome cybercrime in Parepare City. In tackling cybercrime by "conducting investigations". Investigations according to the laws and regulations as referred to in Article 1 number 5 of the Criminal Procedure Code (KUHAP) are as follows:

> "An investigation is a series of investigative actions to investigate and find an event that is suspected to be a criminal offence in order to determine whether or not an investigation can be carried out in the manner provided for in this law".

Based on the sound of Article 1 number 5 of the Criminal Procedure Code, which is an "investigator" in determining an incident that is suspected of being a criminal act explained in Article 1 number 4 of the Criminal Procedure Code is as follows:

> "Investigators are officials of the state police of the Republic of Indonesia who are authorized by this law to conduct investigations"

As stated in Article 1 point 4 of the Criminal Procedure Code above, the police are authorized to carry out investigations. In handling cybercrime in Parepare City, of course, there are obstacles in handling cybercrime in Parepare City. The obstacle in handling cybercrime in Parepare City is the "lack of experts who handle cybercrime". Although cybercrime has problems with experts who handle cybercrime, investigators at the Parepare Police are still trying to handle and overcome cybercrimes that occur in Parepare City like other crimes.

In investigating the handling of cybercrime that occurred in the City of Parepare, of course, a process is needed to resolve the case. That through the stages of the report or complaint as referred to in the report and complaint are contained in Article 1 paragraph 24 and paragraph 25 of the Criminal Procedure Code and the investigator's authority is contained in Article 7 paragraph 1 letter a, namely:

[13] Glenny, M. (2011). Dark Market: Cyberthieves, Cybercops and You. New York: Alfred A. Knopf.

"Receive a report or complaint from a person about the existence of a criminal act".

The process of stages in solving cybercrime cases starts from reporting or complaints then making SP. LIDIK (Examination Warrant) for witnesses, reporters, and reported parties. After the investigation is complete, the investigator then conducts a case title to determine whether or not a crime is sufficient. After determining the proof of a crime in a case title, the investigator makes an SP. SIDIK (Audit Warrant) and SP2A (Notification of Examination Progress) are addressed to the complainant. in SP. SIDIK where witnesses, reporters, reported and expert witnesses are asked for information about a criminal act that they have experienced and felt. Furthermore, it is determined to search and confiscate evidence of alleged criminal acts along with arrests and detentions as regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions in Article 43 paragraph (3) and Article 43 paragraph (6).

In fulfilling the stages of solving a cybercrime case that becomes a Case Report (BAP), the investigator is obliged to submit the case file to the District Attorney for investigation and will then be brought to court at the District Court after the file is complete, as described in Article 14 letter a. up to j the Criminal Procedure Code (KUHAP) that:

a. Receive and examine investigation case files from investigators or assistant investigators;
b. Conduct pre-prosecution if there are deficiencies in the investigation by taking into account the provisions of Article 10 paragraphs 3 and 4, by providing instructions for the completion of investigations from investigators;
c. Provide an extension of detention, carry out further detention or detention and or change the status of the detainee after the case has been delegated by the investigator;
d. make an indictment;
e. Delegating cases to court;
f. Deliver notification to the defendant regarding the provisions regarding the day and time the case will be heard accompanied by summons, both to the defendant and to witnesses, to come at the hearing that has been determined;
g. Carry out prosecutions;
h. Closing the case for the sake of law;
i. Perform other actions within the scope of duties and responsibilities as a public prosecutor according to the provisions of this law.
j. Carry out the judge's determination.

In the description reads Article 14 letters (a) to letter (j) of the Criminal Procedure Code, the District Attorney's Office to examine the case file of the investigator, as for the obstacles to determining an indictment and charge, as in Article 13 of the Criminal Procedure Code (KUHAP) that:

"The Public Prosecutor is the Prosecutor who is authorized by this law to carry out the prosecution and carry out the determination of the judge".

Meanwhile at the Parepare District Attorney's Office, the Prosecution's obstacle in examining the cybercrime case file in determining the indictment is regarding the facilities used by the cybercrime perpetrators themselves, as well as the place where cybercrime occurs, considering that Cybercrime is closely related to technology where cybercrime perpetrators are sometimes difficult to trace if they use an account. false so that the facility factor becomes one of the most important elements in the description of the indictment of the Public Prosecutor and in the description of the criminal charges against the accused later.

The Public Prosecutor (JPU) who handles cybercrimes in Parepare City, the process of resolving cybercrime cases carried out by the Public Prosecutor at the Parepare District Attorney until it reaches the trial stage, which is carried out with the following stages:

a)Pre-Prosecution Phase

As referred to in Article 14 letter b of the Criminal Procedure Code. The Public Prosecutor conducted research on the cybercrime case file to be sent by the Police investigator to the Parepare District Attorney's Office with a period of 7 days to determine the attitude towards the completeness of the cybercrime case file and within 14 days, the JPU must have stated that the attitude will provide instructions to complete the deficiencies in the case file or declare the complete case file to meet the formal and material requirements.

b) Prosecution Phase

a. The Public Prosecutor accepts the submission of the suspect and evidence (if any) for the prosecution process, in this case the Public Prosecutor must prepare a cybercrime indictment;
b. The Public Prosecutor submitted the cybercrime case file to the Parepare District Court accompanied by an indictment against cybercrime;
c. The Public Prosecutor conducts a trial against the perpetrators of cybercrimes after obtaining the determination of the day and date of the trial from the Panel of Judges of the Parepare District Court;
d. The Public Prosecutor conducts trials with reference to the charges against the perpetrators of cybercrimes;
e. The Public Prosecutor proves the charges against the perpetrators of cybercrimes by presenting evidence in the form of witnesses, experts, instructions, and the defendant before the trial;
f. The Public Prosecutor makes an indictment based on the facts in an objective trial in connection with the articles of indictment against perpetrators of cybercrimes;
g. The Public Prosecutor carries out corporate criminal charges against perpetrators of cybercrimes based on the provisions of the criminal threat from the indictment presented at trial;
h. The Public Prosecutor carried out the execution of cybercriminals, after the cybercriminals were found guilty by the Panel of Judges and sentenced to prison in accordance with the Decision of the Panel of Judges of the Parepare District Court.

Seeing from the process of handling cybercrime in Parepare City above, that in the process of handling cybercrime in Parepare City has not been effective, there are many obstacles encountered by law enforcement apparat, such as the lack of experts who handle cybercrime, but the Police and the Parepare District Attorney's Office continue to strive for the implementation of their duties and functions as law enforcement in the midst of the onslaught of cybercrime and crimes that occur in the City Parepare.

Legal Basis for Cyber Crime

In this regard, Sudikno Mertokusumo argues that the law functions as a tool to provide protection for human interests. Meanwhile, Philipus M. Hadjon said that the main goal of a state of law is to provide legal protection for its people. Legal protection for the people for government actions is based on two principles, namely the principle of human rights and the principle of the rule of law.[14]

In line with that, Rudolf Stamler stated that legal ideals are useful as leitsern (guiding stars) in realizing the ideals of society. From these legal ideals, understanding and legal politics in the state are formed. The ideal of law is something that is normative and constitutive. Normative means that it functions as a transcendental prerequisite which is the foundation of dignified positive law, the basis of legal ethics, and at the same time the benchmark of a positive legal system. Constitutive legal ideals mean that *rechtsidee* has the function of directing the law to the goals to be achieved. Gustaf Radbruch states that the ideal of law serves as a constitutive basis for positive law, giving meaning to law. Rechtsidee becomes a benchmark that is regulative, namely testing whether positive law is fair or not. Legal ideals will influence and function as general principles that provide guidance (guiding principles), critical norms

[14] Setiadi, H. E., & SH, M. (2017). Sistem Peradilan Pidana Terpadu dan Sistem Penegakan Hukum di Indonesia. Prenada Media.

(evaluation rules), and driving factors in the administration of law (formation, discovery, application of law, and legal behavior).

Law Number 11 of 2008 concerning Information and Electronic Transactions is the legal basis that regulates cybercrime, namely the special law that regulates Electronic Information and Transactions.

"The Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions is a special law or commonly referred to in Dutch terms as a foot expert". The legal basis for prosecuting cybercriminals by the Public Prosecutor (JPU) in setting charges is articles that are directly related to the actions of cybercriminals themselves, for example, cybercriminals who have committed acts of posting good articles in the form of comments that contain writing attacking someone's honor/accusing someone commits an act in such a way that information can be spread through Facebook accounts on social media, so that based on his actions, the prosecutor will apply the article in the indictment that is directly related to the act, namely: Article 27 paragraph (3) in conjunction with Article 45 paragraph (1) Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) with article elements, namely:

> "Intentionally and without rights, distributing and or transmitting and or making accessible Electronic Information and or Electronic Documents, has the content of contempt and or defamation".[15]

Furthermore, the articles of indictment will be proven in court and the facts of the trial relating to the actions of the cybercrime perpetrators themselves will later be used by the public prosecutor as the legal basis for criminal prosecution against cybercrime perpetrators.

Of course, it becomes the legal basis for the analysis of the Parepare City Police in ensnaring cybercrime. The person in charge of cybercrime in the City of Parepare, at the head of the KPK, a case was held to determine whether or not a criminal act was sufficient by posting through social media as referred to in Article 27 paragraph (3) of the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions.

The analysis of the legal basis of cybercrime entanglement is based on the existence of valid evidence, namely where the Public Prosecutor always uses analysis in ensnaring cybercrime perpetrators with reference to the existence of evidence as regulated in the Criminal Procedure Code (KUHAP). there is evidence in the case file at least 2 valid pieces of evidence in relation to cybercrime, the public prosecutor states that the cybercrime case file investigated by the investigator is complete or fulfills the formal and material requirements of a criminal act in order to carry out the prosecution process.

Conclusion

There is a shift from conventional crime to cybercrime by utilizing various devices. It is important to classify information and ensure the security of the network used to avoid or at least minimize the potential for cybercrimes such as hacking social media accounts, mobile banking, cybercrimes, pornography, and other cybercrimes. Cybercrime, which is essentially a human rights violation, is still very massive, especially in the City of Parepare where the handling process is still not running effectively, because the regulations governing cybercrime have not provided a deterrent effect for the perpetrators so that until now Cybercrime is still very common.

[15] *Vide* Pasal 45 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

References

Glenny, M. (2011). Dark Market: Cyberthieves, Cybercops and You. New York: Alfred A. Knopf.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2(1), 13-20. https://doi.org/10.1007/s11416-006-0015-z.

Karim, K., Herman, B., & Syahril, M. A. F. (2021). Criminological Analysis of Online Buying Fraud. DME Journal of Law, 2(01), 1-15.

Komnas HAM. (2020). Serangan Digital Mengancam Pembela HAM. Available at: https://www.komnasham.go.id/index.php/news/2020/8/3/1508/serangan-digital-mengancam-pembela-ham.html. (Accessed: 1 Mei 2022).

Lestari, S. E. (2017). Kajian Hukum dan Tindakan Bagi Pelanggaran Undang-Undang Nomor 32 Tahun 2009 Tentang Perlindungan dan Pengelolaan Lingkungan Hidup. *Mimbar Yustitia*, *1*(1), 21-35. https://doi.org/10.52166/mimbar.v1i1.567.

Maskun, S. H. (2014). *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Prenada Media.

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. The Journal of Economic Perspectives, 23(3), 3–20. https://doi:10.1257/ 089533009789176825.

Nasrullah, R. (2022). *Teori dan riset media siber (cybermedia)*. Prenada Media.

Putlitbang Hukum dan Peradilan Mahkamah Agung RI. (2004). *Naskah Akademis Kejahatan Internet* (*cybercrime*).

Sampara, S., & Husen, L. O. (2016). Metode Penelitian Hukum. *Makassar: Kretakupa Print*.

Setiadi, H. E., & SH, M. (2017). Sistem Peradilan Pidana Terpadu dan Sistem Penegakan Hukum di Indonesia. Prenada Media.

Sitompul, J. (2012). Cyberspace, cybercrimes, cyberlaw: tinjauan aspek hukum pidana. PT Tatanusa.

Suardi, S., Asba, P., & Iksan, M. N. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Investasi Melalui Media Internet. *Jurnal Litigasi Amsir*, *10*(1), 72-83.

Suharyanto, B. (2013), Tindak Pidana Teknologi Informasi (Cyber Crime): Urgensi Pengaturan dan Celah Hukumnya, Jakarta: Rajawali Pers.

Syahril, M. A. F. (2021). Published Privacy Rights via Short Messages. Amsir Law Journal, 3(1), 11-19.

Kitab Undang-undang Hukum Pidana (KUHP).

Kitab Undang-undang Hukum Acara Pidana (KUHAP).

Undang-Undang Nomor 11 Tahun (2008) Tentang Informasi dan Transaksi Elektronik.