Center for Open Access in Science ▪ https://www.centerprode.com/ojls.html
Open Journal for Legal Studies, 2020, *3*(1), 1-22.
ISSN (Online) 2620-0619 ▪ https://doi.org/10.32591/coas.ojls.0301.01001r

Construction of Law Enforcement Against Money Laundering Crime with Cyber Laundering Mode

Muhamad Rakhmat

Majalengka University, Faculty of Law, INDONESIA

Received: 5 January 2020 ▪ Accepted: 7 March 2020 ▪ Published Online: 10 March 2020

Abstract

If it is understood that all economic crimes (financial crimes) will lead to money laundering, then there should also be a lot of UUTPPU applications for economic crime cases. But in reality the court's decision on financial crimes related to UUTPPU is not up to 20 decisions, even though the economic crimes that reached the court were very large (especially those that are still in the investigation stage, the number is far more), namely corruption, banking crime, illegal logging, smuggling and others. Based on these data, it can be imagined how long a case must be settled through a judicial process. Not infrequently a criminal case requires three to six years to get a decision. The problem does not stop here, although the decision has been obtained, it is likely that the parties who are dissatisfied with the decision will submit other legal remedies such as appeal or reconsideration. When added up, the total time needed for a decision to have permanent legal force is fifteen to twenty years. Various technological advances were then anticipated with the birth of Law No. 11 of 2008 concerning Information and Electronic Transactions and subsequently written ITE Law. Information, Documents and Electronic Signature Arrangements are set forth in Articles 5 through 12 of the ITE Law. In general, it is said that Electronic Information, and/or Electronic Documents, and/or printouts, are valid legal evidence, which is an extension of legal evidence in accordance with the applicable Procedure Law in Indonesia. Likewise, Electronic Signatures have legal force and legal effect. However, the making of an electronic signature must meet the specified requirements. The threat of using information technology to encourage money laundering has been recognized by many. Professor of Information Technology at the University of Paramadina, Marsudi W. Kisworo stressed that currently the world is trying to fight money laundering through the Internet media, and even the biggest crime on the Internet is money laundering with a percentage of more than 30% of cybercrime.

Keywords: law enforcement, money laundering, cybercrime.

1. Introduction

The problem of money laundering has just been declared a criminal offense by Law No. 15 of 2002 concerning Criminal Acts of Money Laundering (TPPU) which was passed and enacted on 17 April 2002. With the TPPU Law, the legislators intend to criminalize[1] money laundering crimes (Money Laundering) into an act prohibited by law criminal.

[1] Criminalization is a rather new term in the science of law. Criminalization is part of criminal policy using the means of punishment. The definition of criminalization based on the Indonesian dictionary is: "A

Correspondence: Dr. H. Muhamad Rakhmat., SH., MH, Majalengka University, Faculty of Law, INDONESIA. E-mail: rakhmatmuhammad88@gmail.com.

As a new law, of course it contains new problems for the Republic of Indonesia (Indonesia). The issuance of Law No. 15 of 2002 this TPPU is to overcome the effects of Indonesia being blacklisted, which is categorized as a non-cooperative Country, or a Non-Cooperative Countries and Territories (NCCT's) country since 2001 by the Developed Countries group incorporated in the Financial Action Task Force (FATF) on Money Laundering.[2]

Increasing money laundering crimes, the State of Indonesia, which is a hotbed for money laundering, received enormous attention from governments, international organizations and those who carry out transnational business practices. The organization that first paid attention to money laundering was Task the Financial Action Force on Money Laundering (FATF). FATF has the function of developing and disseminating policies to eradicate money laundering, processing assets – assets from criminal acts in hiding their illegal origins.

One of the roles of the Financial Action Task Force on Money Laundering (FATF) is to determine the policies and steps needed in the form of recommended actions to prevent and eradicate money laundering. In Indonesia's input into the NCCT's based on the FATF decision due to the existing TPPU Law considered too weak, the government made efforts to amend the law with the birth of Law No. 25 of 2003 concerning Criminal Acts of Money Laundering, then precisely on 12 February 2005, Indonesia officially left the NCCT's list.

Why did the Republic of Indonesia twice make the TPPU Law?, the argument made by the makers of the TPPU Law was in the framework of preventing and eradicating TPPU, Indonesia already had Law No. 15 of 2002 concerning TPPU. However, it is felt that the provisions in the Act do not meet international standards and the development of judicial processes of money laundering, so it needs to be changed so that efforts to prevent and eradicate TPPU can run effectively.[3]

There is a reason why Indonesia immediately has an anti-money laundering law, even in a very fast time Indonesia changed it TTPU Law, and the most logical reason is because the practice of money laundering is very detrimental to society, why it harms the community. In this case Sutan Remy Sjahdeini,[4] said that:

> 1. Money laundering allows criminals or criminal organizations to expand their operations, this will increase the cost of law enforcement to eradicate it;
>
> 2. Money laundering activities have the potential to undermine the public to continue to commit these crimes;
>
> 3. As a result of money laundering, it is likely that corruption will increase along with the circulation of large amounts of illicit money;

process that shows the behavior was not initially considered a criminal event, but later classified as a criminal event by the community". According to Sudarto, what is meant by criminalization is as: "The process of determining an act of a person as an act that can be convicted, this process ends with the formation of a law where the act is threatened with a criminal sanction." Look in: Sudarto, *Hukum Dan Hukum Pidana*. PT. Alumni: Bandung, 1986: 31-32.

[2] Adrian Sutedi, *Tindak Pidana Pencucian Uang,* PT. Citra Aditya Bakti: Bandung, 2008: 175-176.

[3] Compare with Considering Law No. 25/2003 concerning Amendment to Law No. 15/2002 concerning TPPU, which states that in order to prevent and eradicate the TPPU effectively, the Law No. 15 of 2002 concerning TPPU needs to be adjusted to the development of criminal law regarding money laundering and international standards. So it is clear that Indonesia in changing Law No. 15 of 2002, only following the development of the international world, although during Law No. 15 of 2002 is valid until it is replaced, the case of Money Laundering has never been revealed by law enforcement officials in Indonesia.

[4] Sutan Remy Sjahdeini, *Pemberantasan Tindak Pidana Pencuciang Uang* (Makalah), Disampaikan pada Sosialisasi RUU-TPU, yang diselenggarankan leh Depkim dan HAM dari Tanggal 6-10 November 2000: 1.

4. Money laundering activities reduce government revenue from taxes and indirectly harm honest taxpayers and reduce legitimate employment opportunities;

5. Ease of money entering a country has attracted unwanted elements through the country's borders, lowered the level of quality of life, as well as raising concerns about the national security of the country concerned.

But in reality, even though Indonesia already has legal instruments to eradicate money laundering, why is Indonesia still labeled a "money laundering" paradise? There are still many legal instruments that have weaknesses. There are still many gaps that can be penetrated by the perpetrators of money laundering (Money laundering). As a result, this law remains powerless in the face of money laundering practices that are so sophisticated and almost perfect. These weaknesses must be overcome immediately and Indonesia revised with Law No. 25 of 2003 concerning Amendments to Law No. 15 of 2002 concerning Criminal Acts of Money Laundering.

Considering that this crime is a crime in a new and contemporary form, the law enforcement is not yet effective enough to be carried out. The problem that is the source of the trigger is not solely caused by factors that affect law enforcement not enough to be able to reach the problem of law enforcement in the field of money laundering crimes, but also born and sourced from the lack of willingness of law enforcement officials to reveal these crimes to surface.

In general, when talking about law enforcement, there are several factors that influence it, so that the law can be upheld, those factors are:[5]

1. The legal factor itself, in the present condition the legal factor itself, can be identified with the factor of the presence or absence of laws;

2. Law enforcement factors, namely those who form and apply the law;

3. Factors of facilities or facilities that support law enforcement;

4. Community factors, namely the environment in which the law applies or is applied;

5. Cultural factors, namely as a result of work, creativity, and taste based on human initiative in the association of life.

Talking about the legal factors (Law / Positive Law), Indonesia already has laws regarding money laundering, namely Law No. 15 of 2002; Law No. 25 of 2003. Regarding changes to Law No. 15 of 2002 concerning Criminal Acts of Money Laundering. With legal instruments like this, Indonesia is sufficient to combat money laundering.

There are several things, why money laundering crimes need to be fought and declared a criminal offense, so that Indonesia makes changes to Law No. 15 of 2002. In this case Guy Stessen,[6] stated that in general there are several reasons why the crime of money laundering needs to be fought and declared a criminal offense:

1. Money laundering can affect the financial and economic system which is believed to have a negative impact on the effectiveness of the use of resources and funds by money laundering resources and funds are widely used for illegal activities and can be detrimental to the community, in addition to that many funds are lacking used optimally;

2. Criminalizing money laundering as a crime will make it easier for law enforcement officials to confiscate the proceeds of crime which are sometimes

[5] Soerjono Soekanto, *Faktor - Faktor Yang Mempengaruhi Penegakan Hukum,* PT. Raja Grafindo Persada: Jakarta, 2004: 7-9.

[6] Guy Stessen, *Money laundering: A new international law enforcement model,* Cambridge Study in International and Comparative Law, Cambridge University Press, 2000, P-82-85.

difficult to confiscate, for example assets that are difficult to trace or have been transferred to third parties. In this way the escape from the proceeds of crime can be prevented. This means that eradicating money laundering has shifted its orientation from cracking down on perpetrators to confiscating "proceeds of crime". In many countries declaring money laundering as a criminal offense is the basis for law enforcement to criminalize third parties who are considered to obstruct law enforcement efforts;

3. Criminalization of money laundering as a criminal offense and with the fact that there are also a number of transaction reporting systems and a number of suspicious and suspicious transactions, this will make it easier for legal officials to investigate criminal cases up to the figures behind them.

Entering the current era of technology and information, crime is increasingly sophisticated to do and increasingly difficult for law enforcement officials to enforce the rules. Because the criminals are no longer conventional, but advancing towards the digital world by utilizing the Internet media.

With the existence of the Internet media, it is seen here that efforts to prevent money laundering (money laundering) seen from the mode of operation using cyber laundering is a problem that deserves to be discussed, bearing in mind the crime of money laundering will grow chalky if done using technology very sophisticated, this is what researchers mean that money laundering criminals make use of legal loopholes or the TPPU Law which is still empty and still has a very wide range of space for money laundering.

With the Internet, which has a new world or what is called "virtual word" or cyberspace, which is often referred to as "Cyberspace", money laundering starts with Cyber laundering techniques, even techniques like this are becoming more prevalent and becoming a trend for money laundering criminals.

Cyber laundering technique, one of which is by using electronic transfer (wire transfer), this technique allows criminal organizations and legitimate business people and legitimate banking customers to move funds quickly from their accounts (accounts) from one bank to another bank others throughout the world. So thus the practice of money laundering can be done by someone without having to go abroad, for example, this can be achieved by advancing information technology through the Internet, where dissemination through banks electronically can be done, as well as a money launderer can deposit dirty money to a bank without mentioning their identity.[7]

Moving on from the description above, which describes the phenomenon of money laundering crimes using Cyber laundering techniques, the authors identify the problem as follows: What forms of misuse of Cyber laundering for money laundering purposes?, What is the model of law enforcement in dealing with money laundering (Money laundering) with using Cyber laundering Technique?

2. Literature review

The basic theory used is, Law Enforcement Theory, what is called law (in the sense of positive law), must go through several stages, namely the making of law; law enforcement, justice and administration of justice. Law making is the beginning of the legal process. It is a momentum that separates the state without law from the state governed by law. It is also a separator between

[7] Through the digital world, money transfer can be made by not mentioning their identity, but by using or can be done anonymously, or with a pseudonym that the public does not know about.

the social world and the legal world.[8] After the making of the law is finished, the next step is that the law must be upheld.

The law enforcement process, as a complement to the next stage regarding the law-making process. This indicates that the law-making process must still be followed concretely in the implementation stage in people's daily lives. After this stage is still not finished, because there is still a judicial stage that must be carried out. The law will not be upheld, if without a judicial process,[9] because with this judicial process the law can be upheld.

The last legal process is the administration of justice stage, in this case what appears more prominent is the administrative approach compared to the legal approach. In this stage of performance, it is more dominant to think about the work efficiency of the institutions involved in the judicial process. This means that this process is closer to the bureaucratic process.[10]

Then what exactly is law enforcement, is it quite like what was meant above. In Indonesian terminology, law enforcement is known in several terms, *such as the application of law*;[11] *Implementation of law*,[12] *and the formation of law*. But it seems that the term law enforcement is the term most often used and thus in the future the term will be more established. In foreign languages the term law enforcement is known as rechtstoepassing; rechtshanhaving; (Netherlands); law enforcement; application (American).

Some of these terms, the meaning can be seen as follows: What is meant by the formation of law (Rechtsvorming) is:[13]

> *"Formulating general rules for everyone. Which is usually done by legislators. Judges are also possible to form law (judge made law) if the decision becomes*

[8] Satjipto Rahardjo, *Ilmu Hukum,* PT. Citra Aditya Bakti: Bandung, 2000: 176.

[9] It should be distinguished between the term "justice" with the term "court". The court comes from the word "Fair" obtaining the prefix "Pe" and the suffix "An". Look in the: Anton M. Moeliono**,** Dkk, *Kamus Besar Bahasa Indonesia,* Balai Pustaka, Jakarta, 1990: 6-7. The court of translation of the Court, designates a forum, body, institution, or institution. Whereas judicial translation from judiciary is used to show the function, process or method of providing justice. In this case Satjipto Rahardjo, means that "The judiciary shows the process of hearing, while the court is one of the institutions in the process of hearing. Other institutions involved in the judicial process are the Police, Attorney General's Office and Advocates. The final result of the judicial process is in the form of a court decision, or often referred to as a judge's decision, which is why the judge presides over the trial". Look inside: Satjipto Rahardjo, *Ilmu Hukum. Ibid.*: 182.

[10] La Patra said that the bureaucratic approach is closer and supported by a system analysis approach or a systems approach. See: J. W. La Patra, *Analzing the Criminal Justice System*. Lexington Mass; Lexington Books, 1987. See also in: Satjipto Rahardjo. *Ilmu Hukum. Ibid.*: 183. Just look at the application of this system approach in "criminal justice in system" for example we see the definition of the criminal justice system according to Romli Atmasasmita, the term Criminal justice system or criminal justice system (SPP) has now become a term that shows the mechanism of action in overcoming crime by using the basis system approach. The understanding put forward by Romli actually shows that the law is a system, and part of the system. The one whose performance is always to use bureaucracy. This can be seen from the following matters: (1) The emphasis is on the coordination and synchronization of the components of the criminal justice (Attorney Police, Courts, and Corrections); (2) Supervision and control over the use of power by the criminal justice component; (3) The effectiveness of the crime prevention system is more important than the efficiency of the settlement of the case; and (4) The use of law as an instrument to strengthen the administration of justice. Look in: Yesmil Anwar & Adang, *Sistem Peradilan Pidana: Konsep, Komponen, & Pelaksanaannya dalam Penegakan Hukum di Indonesia*, Widya Padjajaran: Bandung, 2009: 33-dst.

[11] Satjipto Rahardjo. *Ilmu Hukum. Op. cit.*: 181.

[12] Sudikno Mertokusumo. *Penemuan Hukum: Sebuah Pengantar*. Liberty: Yogyakarta, 2004: 36-37.

[13] Sudikno Metokusumo. *Penemuan Hukum Sebuah Pengantar. Ibid.*: 36.

permanent jurisprudence (vast jurisprudence) followed by the judges and is a guideline for the legal community in general."

Application of law (Rechtstoepassing)

"Applying abstract legal regulations to events, for that a concrete event must be made a legal event first so that the rule of law can be applied."

Law enforcement (Rechtshandhaving)

"Running the law whether there is a dispute or violation or without dispute. This includes the implementation of the law by every citizen every day which is often not realized by the citizen apparatus, such as a police officer standing at a crossroads to regulate the flow of traffic."

Creation of Law (Rechtshepping)

"That the law does not exist at all then created a new law, that is, from nothing to being."

From the various terms of law enforcement above, the writer can draw a conclusion that law enforcement is an attempt to realize abstract ideas in a reality. The process of realizing that abstract idea, according to the writer, is the essence of law enforcement. While the core of the process is to apply discretion that involves making decisions that are not strictly governed by the rule of law, but have an element of personal judgment.

The harmonization of values in law enforcement must be adjusted to the authority of the enforcers, because the law will run well if there is power to implement it. However, on the other hand, it is often the power that ravages the law, that is, if power is not strictly restricted by law. The destruction of the law because of power is also clearly seen in the implementation of the law. Then how can law and power be upheld. About this reminiscent of the views of Mochtar Kusumaatmadja who said that: "*Law without power is wishful thinking, while rule without law is tyranny"*,[14] to create fair order from the implementation of law,[15] or from law enforcement through power, then there must be something watch out for[16]

1. Modeling law enforcement by law enforcers;
2. A straightforward attitude (Zakelijk) from law enforcers;
3. Adjustment of applicable regulations with the latest technological developments;
4. Information and information about regulations that apply to the community;
5. Give enough time for the community to understand the new rules made.

From the applicable requirements above, the essence of law enforcement is increased, namely that law enforcement is not merely the implementation of the law, although in reality the tendency is in Indonesia. So, the notion of law enforcement is so popular. In addition, there is a strong tendency to interpret law enforcement as implementing judges' decisions. If this is only

[14] Mochtar Kusumaatmadja. *Konsep - Konsep Hukum Dalam Pembangunan*. Alumni: Bandung, 2002: 199.

[15] The term is taken from Budiono Kusumohamidjojo. He further said, that about what is fair and what is unjust becomes increasingly complex, this is in line with the increasing and also the increasingly complex patterns of human life needs and the increasingly limited resources needed to fulfill it. From this proposition, the writer can say this is "fair order". Furthermore, Budiono defines what is referred to as public order, according to him is: "the conditions concerning the implementation of human life as a life together". See in: Budiono Kusumohamidjojo, *Filsafat Hukum: Problematika Ketertiban Yang Adil.* PT. Grasindo: Jakarta, 2004: 166.

[16] Soerjono Soekanto, Penegakan Hukum Lalu Lintas Dan Kepatuhan Terhadapnya. *Majalah Hukum & Pembangunan*, No. 1, January 1978: Jakarta, FH-UI, Jakarta, 1978: 534.

limited to the implementation of judges' decisions, then law enforcement is biased, inconsistent because such opinions are too narrow in nature.

According to Soerjono Soekanto,[17] law enforcement actually lies in the factors that might influence it. These factors have a neutral meaning, so the positive or negative impact lies in the substance (content) of these factors. The intended factors are:

1. The legal factors themselves (Positive Law);
2. Law enforcement factors or parties who form or implement the law (Law enforcement);
3. Factors of facilities or facilities that support law enforcement;
4. Community factors, is the legal environment can be applied;
5. Cultural factors, namely as a result of work, creativity and taste based on human initiative in the association of life.

These five factors are closely related to each other, therefore, these factors are the essence of law enforcement, also a benchmark of law enforcement effectiveness.

Internet and crime or what is commonly called dentgan Cyber law. To arrive at a discussion on cyber law, it is first necessary to explain one term that is very closely related to cyber law, namely cyberspace (cyberspace), because cyberspace will be the object or concern of cyber law. The term cyberspace was first introduced by William Gibson, a science fiction writer in his novel *Neuromancer*. The same term was then repeated in another novel called Virtual Light.

According to W. Gibson, cyberspace is:

"*... was a consensual hallucination that felt and looked like a physical space but actually was a computer-generated construct representing abstract data.*"[18]

In subsequent developments along with the widespread use of computers this term is then used to designate an electronic space (electronic space), which is a virtual society that is formed through communication that is intertwined in a computer network (interconnected computer networks). At this time, cyberspace as stated by Cavazos and Morin is: ... "represents a vast array of computer systems accessible from remote physical locations".

Potential activities to do in cyberspace cannot be predicted with certainty given the rapid advancement of information technology and which may be difficult to predict. However, currently there are several main activities that have been carried out in cyberspace such as Commercial On-line Services, Bulletin Board Systems, Conferencing Systems, Internet Relay Chat, Usenet, Email lists, and entertainment.

A number of these activities can now be easily understood by most people as activities carried out via the Internet. Therefore it can be concluded that what is called cyberspace is nothing else but the Internet which is also often referred to as a *network of networks*. With characteristics like this then there is also a mention of cyber space with the term virtual community (virtual

[17] Soerjono Soekanto. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum. Op. cit.*: 8-9

[18] William Gibson, Neuromancer, Ace, New York, 1984: 51. See also William Gibson, Virtuallight, Viking, London, 1993. Gibson, in essence in both of his books, wants to say that cyberspace, is a hallucination experienced by millions of people every day, in the form of complex graphical representations of data in the human mind system abstracted from computer system data banks. For an initial understanding of William Gibson's theory, it is recommended to read Mark Slouka, War of the World; Cyberspace and the High-Tech Assault on Reality, which has been translated into Indonesian, *Ruang yang hilang: pandangan Humanis tentang budaya cyberspace yang merisaukan,*Mizan: Bandung, 1999. Atau dapat juga dibaca bukunya Jeff Zaleski, *Spritualitas Cyberspace,* Mizan: Bandung, 1999.

society) or virtual world (virtual world). Cyberspace will be called the Internet. Assuming that activities on the Internet cannot be separated from humans and the legal consequences are also on the community (humans) in the physical word (real world), then the thought arises about the need for legal rules to regulate these activities. However, given the characteristics of activities on the Internet that are different from those in the real world, then there are pros and cons about whether or not the traditional/conventional legal system (the existing law) regulates these activities. Thus, this polemic is actually not about the necessity of a legal rule regarding activities on the Internet, but rather questioning the existence of traditional legal systems in regulating activities on the Internet.

If we talk about the Internet (especially in Indonesia) (read: *Understanding the Internet by Indonesians*), in essence, the Internet is a computer network that is connected to each other through communication media, such as telephone cables, optical fibers, satellites or frequency waves. But sometimes, the rights possessed by each person are abused by some people who are not responsible, causing anxiety for some people who feel disadvantaged by the abuse of these rights.

Ahmad M. Ramli[19] said that:

> *"At this time a new legal regime has been born known as Cyber Law. The term "cyber law" is interpreted as the equivalent of the word Cyber Law, which is currently internationally used for legal terms related to the use of information technology."*

Other terms that are also used by Ahmad M. Ramli[20] are: Law of Information Technology, Law of the Virtual World and Mayantara Law. These terms were born in view of Internet activities and the use of virtual-based information technology. The term cyber law is based on the idea that cyber if identified with the "virtual world" will be sufficient to face problems when related to proof and law enforcement. Considering that law enforcers will face difficulties if they have to prove a problem that is assumed to be "virtual", something invisible and pseudo.

The legal world has long since broadened the interpretation of its principles and norms when confronting intangible issues, As Ahmad M. Ramli said:

> *"Electricity theft cases are initially difficult to categorize as theft crimes, but eventually they can be accepted as criminal acts."*

The current reality relating to cyber activities is no longer that simple, considering that their activities can no longer be limited by a country's territory, its access can easily be done from any part of the world, losses can occur both to Internet actors and other people who have never been connected even for example in the theft of credit card funds through Internet purchases.

According to Abu Bakar Munir[21] that:

> "*In addition, the issue of proof is a very important factor, considering that electronic data is not only not yet accommodated in the Indonesian procedural law system, but in reality the data referred to are also very vulnerable to be changed, tapped, falsified and sent to various parts of the world within seconds . So that the impact can be so fast, even very terrible.*"

Information technology has become an effective instrument in global trade. For example, banking transactions through Internet media are closely related to promotion issues. Where behind the convenience can occur problems regarding breaking into customer accounts

[19] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, *Ibid*.: 1-2.

[20] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, *Ibid*.: 1-2.

[21] Abu Bakar Munir, *Cyber Law Policies and Challenges*, Rajawali Pers, Jakarta, Cet.Pertama, 1999: 205.

through transactions via the Internet? Another example, is trading transactions through electronic media or also called electronic commerce which is currently often found.

Cyber activities, although virtual, can be categorized as real legal actions and actions. Juridical for cyber space is no longer in place to categorize something with the size and qualifications of conventional law to be used as objects and deeds, because if this method is taken there will be too many difficulties and things that escape from the snares of the law.

In the Draft Law on Information and Electronic Transactions it is said that:[22]

> *"Cyber activities are virtual activities that have a very real impact even though the evidence is electronic. Thus, the subject of the culprit must also qualify as someone who has committed a real legal act."*

According to Ahmad M. Ramli[23] there are three approaches to maintaining security in cyberspace:

1. *A technological approach;*
2. *Socio-cultural-ethical approach;*
3. *Legal approach.*

To overcome security problems, the technological approach is absolutely necessary, because without a network security it will be very easily infiltrated, intercepted, or accessed illegally and without rights. Technological and industrial progress which is the result of human culture in addition to having a positive impact, in the sense that it can be utilized for the benefit of humanity also has a negative impact on human development and civilization itself. The negative impact in question is related to the world of crime. It was stated by criminal law expert, Andi Hamzah,[24] that

> *"The development of technology is very influential on the attitude of action and mental attitude of every member of the community. Progress in technology will also affect changes in people's lives. Every society will always change from time to time. The greater the influence of the environment, the more rapid changes will occur within the community itself, both positive and negative changes."*

In cyberspace, perpetrators of violations often become difficult to prosecute because Indonesian law and courts do not have jurisdiction over perpetrators and legal actions that occur, bearing in mind that violations of the law are transnational but as a result have legal implications in Indonesia. Therefore, for cyber space a new law is needed which uses a different approach to the law made based on regional boundaries. As contained in the general explanation of the Draft Law on Information and Electronic Transactions (ITE) paragraph 8 which states:[25]

> *"Domain names used as addresses and identities on the Internet have their own problems. Domain naming has a close relationship with the name of the company, product or service (service) it has. Often these products or services are registered as trademarks or service marks. This domain name problem is quite complicated because in this world there are several independent domain name managers. There are more than two hundred domain-based domain managers (often referred to as country code Top Level Domains or ccTLDs). For example the domain manager for Indonesia (.id)."*

---

[22] Kementerian Komunikasi dan Informasi RI, *Rancangan Undang-undang tentang Informasi dan Transaksi Elektronik* (RUU ITE), Jakarta, 2004: 5.

[23] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, *Op. cit.*: 3.

[24] Andi Hamzah, *Hukum Acara Pidana Indonesia*, Sapta Artha Jaya, Jakarta, Cet.Pertama, 1992: 22.

[25] Kementerian Komunikasi dan Informasi RI, *Penjelasan Rancangan Undang-undang ITE*, *Op. cit.*: 19.

Why domain names are a problem because, anyone who can run the Internet can make his own domain name as an identity in cyberspace. However, sometimes there are some people who use other people's domain names for their own interests. The method used is by impersonating a domain name.

Understanding cyberspace is not limited to the world that is created when there is a relationship through the Internet. Bruce Sterling defines cyberspace as the "place" where a telephone conversation appears to occur. The Internet is also a good tool for people at work, at home and in other places of public service as stated by D. Beckers:[26]

> "*Information and communication technology has invaded all domains of our society: at work, at home and in public places. In modern culture is profoundly mediated. Current innovations in computers and telecommunications made new types of social interaction and cultural transmission possible across previously impossible distances. There is little doubt that these rapid advances in modern telecommunication and computers are changing the way we live our lives, but the direction of change is still uncertain*."[27]

Cyberspace whose reality is a virtual reality, is a world that transcends existing reality, a hyper-real, a virtual reality. This transcendent and artificial world of reality colonizes almost every reality that exists and will one day take over these realities. Reality itself is now engineered in such a way that it can no longer be distinguished between original and imitation realities (simulacra). Jean Baudrilard in Simulations defines that simulation as: "The creation of models of reality without origin and reality, or hyper-real".[28]

These models may seem cursory at first glance, but in fact do not describe the actual reality. Instead, it hides the true reality. Reality is covered by symbols of reality in such a way that between symbols and reality, between models and reality can no longer be distinguished. Simulation does not describe reality as it is, then the reality produced by simulation is reality that transcends or hyper-reality, meaning that reality can no longer be judged based on the measurements (rational-moral) that exist in the actual reality.

However, at this time we are trapped in a network of symbols that are so confusing that they lose their importance. These symbols come from many directions, and are so diverse, changing fast and contradictory, that the affirmation of the messages contained therein is dimmed. On the other hand, the recipients of these symbols are very creative, self-aware and reflective, so that the symbols are greeted with skepticism and one eye.

---

[26] Bruce Sterling, *The hacker crackdown, law and disorder on the electronic frontier*, Massmarket Paperback, electronic version available at http://www.lysator.liu.se/etexts/hacker. Assessed 10 October 2008.

[27] D. Beckers, *Research on virtual communities: An empirical approach*, and it can be find at http://www.swi.psy.nl/usr/beckers/publication/seattle.html. Assessed 10 October 2008.

[28] Jean Baudrillard, Simulation, Semiotext(e): New York, 1981, an initial understanding of his book can be read in Yasraf Amir Piliang, Posrealitas: *Cultural realities in the Postmetaphysical era*, Jalasutra: Yogyakarta, 2004. In the glossary, Simulation is defined as, the process of creating forms real through models that do not have the origin or reference to reality, so that it enables humans to make the supernatural, illusory, fantasy, fictional appear real. In a previous article, Yasraf A Piliang, said that what was meant by these models did at first glance seem real, but he actually did not describe the actual reality. He instead hides the true reality. Reality (real) is covered by the signs of reality (sign of the real) such that between signs and reality, between models and reality can no longer be distinguished. Look in: Yasraf Amir Piling. *Mesin-Mesin Kepalsuan,* Kompas, 14 June 2000; Agus Rahardjo, *Cybercrime: Pemahaman dan upaya pencegahan kejahatan Berteknologi.* PT. Citra Aditya Bakti: Bandung, 2002: 103.

By them the symbols were easily reversed, reinterpreted and distorted their original meaning. The symbols have lost their credibility.[29] In its development, the Internet turned out to bring a negative side, by opening up opportunities for the emergence of anti-social actions that had been considered impossible or could not have occurred. A theory says, crime is product society.

3. Findings and discussion

3.1 *Forms of misuse of cyber laundering*

Studying the development of cyber laundering crimes, is part of the study of computer crime in general, but cyber laundering is more focused on money laundering activities (money laundering). This kind of crime is actually a contemporary crime, a crime that combines science and technology. Speaking of contemporary crime, our study is entering a condition in which, the veil between reality and fantasy is getting thinner. Many things that were previously considered fantasy have now become a reality, and this will affect the culture and human life. An object can represent reality through its signifier, which has a specific meaning or signified. In this case, reality is a reference from the signifier. However, it can also happen that an object does not refer to a particular reference or reality at all, because it itself is a fantasy or hallucination that has become reality.

That is in the language of Jean Baudrillard and Umberto Eco[30] said to be hyper-reality. According to Baudrillard the "hyper-reality" era was marked by the disappearance of the signifier, and the metaphysics of representation; the collapse of ideology, and the collapse of reality itself which is taken over by the duplication of the world of nostalgia and fantasy or becomes a reality substitute for reality, the worship of the lost object is no longer the object of representation, but the ecstasy of denial and annihilation of its own ritual. The hyper-realistic world is a world that is filled with successive reproduction of simulacrum objects, objects that are purely "appearances", deprived of their past social reality, or have absolutely no social reality as a reference. In a world like this the subject as a consumer is herded into a hyper-real "space experience" the experience of alternating "appearances" in space, mingling and melting reality with fantasy, fiction, hallucinations and nostalgia, so differences between one another are hard to find, in this hyper-reality in Baudrillard's view emphasizes both nostalgia and science fiction.

The essence of the explanation, is the author wants to show that the first characteristic of computer crime (cybercrime), is that there is a shift from reality toward hyper-reality, its relation to cyber laundering, then the characteristics of the first cyber laundering are related to objects and subjects that are immaterial / unreal / intangible. So that's why cyber laundering activities, it is difficult to trace the surface or to the realm of reality. In addition to being difficult to track, cyber laundering is also difficult to prove and always develops by adapting to technological and system developments so that it is difficult to reach by positive law.

The launderer who are in this era are trapped in the condition of schizophrenia, remembering they do not need to reflect signs, messages, meanings or norms. Launderer was also treated to a reproduction of the appearance values but not the reproduction of ideological or mythological values. So, it can be said that cyber laundering techniques do not ignore the differences between manual systems and electronic systems that influence the form and nature of money-based crime-based technology.

---

[29] Soni Yuliar et al., *Memotret Telematika Indonesia Menyongsong Masyarakat Informasi Nusantara,* Pustaka Hidayah, Bandung, 2001: 64.

[30] Umberto Eco, *Tamasya Dalam Hiperealitas,* Jalasutra: Yogyakarta, 9-10

Then it can be said that cyber laundering is actually a conventional crime in money laundering that uses sophisticated technology as a means, so that after joining the sophisticated technology, money laundering crime can be called a cybercrime. At this point, the second characteristic emphasizes the different characteristics between conventional money laundering crimes based on manual systems and computerized / electronic / digitalized based cyber laundering crimes.[31] The difference in the characteristics of the crime begins with the difference in the process or procedure between the traditional money laundering system and cyber laundering (current money laundering).

The following is a display of the characteristics of money laundering and cyber laundering crimes.

Money laundering	Cyber laundering
1. It is obvious that money which is placed in a certain place and then exchanged it in the form of clothes, metal and horses (for example) is clearly visible and easy to trace; 2. It is easy to trace its tracks so that the launderers are easily caught by the kings.	1. Money invested in a bank is not easily seen because launderers break the money in digital, electronic form, making it difficult for officers to track it down, because the ability of launderers to use computers is already very advanced; 2. Not easy to trace, because of his traces in the digital world that are in computer chiefs connected to the Internet.

In the cyber laundering process, launderers are consumers who absorb material values, imaging / appearance values. This condition can be found when a person is in the Internet space unconsciously they have been trapped in the world of hyper-visual reality (media) with awareness, then he will realize that what he witnessed is nothing more than a fantasy, fiction or mirage. According to Baudrillard the world of reality and the world of hyper-reality media / television / Internet are difficult to distinguish, both are equally real.[32]

In fact, now many of the launderers have entered into the realm of the hyper-world, from the people who switch there to its negative impact on that world. One of them is the problem of cyber laundering activities which with this cyber media are rapidly evolving. If money laundering crime is only conventional in the real world. In this cybercrime has changed its form into a hyper-crime, in the view of postmodernism experts, this kind of crime is called a crime of hyper-criminality.[33]

The launderers so far, use technology in a very broad concept but with a meaning that is sometimes very limited. If technology is applied in a limited context where technology is only regarded as having technical, mechanical and knowledge matters, then cultural and organizational values will be an external factor and be set aside. However, if applied in a broader context then the technology is said to be impartial because it has an impact both directly and indirectly on cultural values, traditions and the environment.

Thus, from the description above can be taken the definition that the application of technology is the application of science and other sciences to the practice of cyber laundering in daily life by social systems involving people and organizations, living things and machines. Until

[31] The reader can compare the results of my research with those of Susan W. Brenner, Cybercrimes: New Crimes or Old Wine in New Bottles, in R. D. Clifford (Ed.), *Cybercrime: The investigation, prosecution and defense of a computer-related crime*, Durham-North Carolina Academic Press, pp. 12-15.

[32] Yasraf Amir Pilliang, *Dunia Yang Dilipat,* Bandung: Mizan, 1998: 330.

[33] Hyper-criminality means that crime has become a perfectly planned, organized and controlled discourse through high technology and towards the management of high-level politics, so that it bypasses legal authority, transcends common sense, and skips the reach of cultural values and morality.

now technology has often been made without considering cultural aspects, even though a technology should be designed in accordance with the pattern of community activities that have certain lifestyle and cultural values. From this it is clear that cultural aspects are often ignored. A technology that is intended for a community with certain values and culture, requires efforts that are not easy to be able to also be applied to other communities. The socio-cultural reality that exists in cyberspace is a counterpoint to the existing socio-cultural reality and the resulting boundary between the two eventually becomes blurred. Cyberspace as one form of communication network and global interaction has offered its own form of community, namely virtual community.

From the description above, the virtual community is the third characteristic of cyber laundering crime. In science and technology the idea of a virtual community has become a common view because virtual communication really exists. Cyberspace has interconnected many people, but this does not guarantee the community because the connection created by cyberspace is often one direction or in other words the flow of information is still broadcast. However, with the existence of interactive Internet facilities (online) people can exchange information and here there is a community in a broader sense. People in the virtual world do not present their physicality to communicate with other people, but instead use words on a computer screen. With the development of Voice of Internet Protocol (VoIP) and web cameras it allows the presence of voice and face in communication so that communication takes place in the form of computer conferencing. In virtual communities can communicate with any identity because real identity in the real world (real life) can be left behind, as Howard Rheingold said: "People in virtual communities do just about everything people do in real life, but we leave our bodies behind".[34]

In most countries, money laundering and financing of terrorism are significant issues in terms of prevention, eradication and prosecution.[35] The issue of money laundering in the last few years has always been raised and become a public concern especially in Indonesia or precisely since June 2001, namely the first time that Indonesia was included in the list of countries that were not cooperative in eradicating money laundering or Non Cooperative Countries and Territories (NCCTs) by FATF.[36]

Since this time academics, observers, and the public with the help of the mass media, paid great attention to the study of money laundering and its effects. Meanwhile, regulators such as Bank Indonesia, BAPEPAM and the Ministry of Finance have prepared themselves to make regulations for the development of an anti-money laundering regime in Indonesia.

Cyber laundering was created because of computer crimes in the current telecommunications era, computers that are united with the Internet, can indirectly be said to be cybercrime, as well as cyber laundering. If our study is directed to cyber laundering, then the use of banks will be more dominant as a form of cyber laundering itself. To find out some form of cyber laundering, we should first look at how the development of computer crime problems today.

If we follow the cases of computer and cybercrime that occur, and if it is examined using the criteria of conventional criminal law, then it turns out that in terms of law, computer and cybercrime is not a simple crime.[37] In connection with this matter, when viewed from conventional laws and regulations, the criminal acts that can be used in the computer and cyber fields are fraud, fraud, theft, and destruction, which are essentially carried out directly (using

---

[34] Howard Rheingold, *Virtual reality,* Mandarin, 1991, Versi elektronik dapat dijumpai dalam http://www.rheingold.com/vc/book/intro/html.

[35] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, The International Bank for Reconstruction/The World Bank*, 2003.

[36] Paul Allan Schott, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, The International Bank for Reconstruction/The World Bank*, 2003.

[37] Bainbridge David I, *Komputer & Hukum* Sinar Grafika: Jakarta, 1993: 161.

physical parts of the body and mind) by my slave. Meanwhile, if this is done through cyber facilities, then computer and cybercrime may take the following forms:[38]

1. *Computer fraud (computer fraud);*
2. *Acts of embezzlement;*
3. *Hacking;*
4. *Criminal deeds of communication;*
5. *The criminal act of damaging a computer system;*
6. *Criminal conduct relating to intellectual property, copyrights and patents.*

The development of the use of computer technology, telecommunications and information in daily activities has encouraged the development of transactions via the Internet in the business world, or what people often call E-Commerce.[39] The link with cyber laundering as already mentioned is that universal money laundering is classified as a crime. Even because the modus operandi is generally cross country, money laundering has been considered an international crime. Because the crime of money laundering is also regulated internationally. As seen in article 3 of the UN convention which was ratified since 19 December 1988, and came into force since November 1990. Indonesia has ratified this convention since 31 January 1997 with Law No. 8 of 1996. Until the birth of this UN convention, UN member states (including Indonesia) have held several meetings to prepare a convention that replaces the old convention on narcotics. The meeting was a follow-up step and the consequences of the adoption of UN resolution 39/41 of 1984 consensus. If the 1961 convention emphasizes more on efforts to increase the legal force of each UN member, including confiscating the results of the illicit trade.

In ASEAN countries, activities to eradicate money laundering are also intensively carried out. Even the Philippines is one step ahead of other ASEAN member countries, because the first Philippines had special laws governing the confiscation of assets illegally obtained from drug trafficking traffic.

Money laundering arrangements in Indonesia according to Law Number 25 Year 2003 are in Article 44 which according to that article is in the framework of preventing and eradicating money laundering (money laundering) conducted in accordance with statutory provisions. What is meant by "statutory regulations" is this law, the law regarding criminal procedure law, the law on foreign relations and the law on international treaties.

3.2 *Law enforcement model*

Recognizing the threat of TPPU as a serious crime that can disrupt the stability of the financial system and economic system and have a wide impact on the lives of the people and nation, efforts to prevent and eradicate must be carried out through conceptual, sporadic, and comprehensive measures. Considering that money laundering crimes are mostly committed by transnational organized crimes that cross national borders, international cooperation between PPATK and law enforcement agencies and institutions similar to PPATK abroad is needed. The role of PPATK as Indonesia's Financial Intelligence Unit (FIU) is expected to contribute to the public in handling TPPU cases, especially after the rampant cases of money laundering. The

[38] Compare with Niniek Suparni, *Cyberspace problems and anticipating its arrangements*, Sinar Grafika: Jakarta, 2009, pp. 4-6.

[39] According to statistical data on E-Commerse Transactions between companies (business to business), according to estimates, it rose to US $ 145 billion in 1999 to US $ 7.29 trillion in 2004 or 7% of total worldwide sales transactions estimated at US $ 105 trillion. Kompas, 21 July 2000.

existence of the PPATK institution in providing input for the benefit of the investigation process on TPPU cases is the spearhead for law enforcement officials, PPATK acts as an informant who is considered to have access to the research focus. Good cooperation between law enforcers (Polri) and PPATK is very much needed in handling money laundering cases, because these two agencies are part of the anti-money laundering regime in Indonesia in addition to the Prosecutor's Office, Justice, and the PJK and Bank Indonesia as regulators.

In our criminal justice system, the police and prosecutors are entitled to carry out investigations and prosecutions of crimes, this is based on the provisions in the Criminal Procedure Code, as well as on the TPPU, as stated in Article 30 of Law No. 25 of 2003 concerning TPPU which states:

> *"Investigations, prosecutions, and hearings in court hearings against criminal offenses referred to in this law, are carried out based on the provisions in the Criminal Procedure Code, unless otherwise stipulated in this law."*

Based on this, Yunus Husein argues:

> *"The authority of investigations is not owned by PPATK, even investigations are not clearly mentioned in the law, so the authority of PPATK is limited to the authority of investigators or before the examination is conducted."*

The advantage of the PPATK institution is that in addition to receiving reports from the PJK and the community which are then analyzed and then handed over to the police and prosecutors, the PPATK can work to use the database for the authorities if law enforcement officials require it. Then PPATK can seek cooperation with other countries if information from other countries is needed, this is as stated in Article 25 paragraph 3 of Law No. 25 of 2003 concerning TPPU which states that:

> *"PPATK in conducting prevention and eradication of TPPU, can cooperate with related parties, both national and international."*

PPATK's contribution in providing input to the interests of the investigation process for investigators is very large, especially in supporting financial investigations and the flow of funds transactions of actors who are not the expertise of police investigators, and the role of PPATK is very helpful in terms of coordination with the PJK in terms of finding evidence in the form of evidence bank products relating to suspects' accounts to prove suspicious transactions, so it is unfortunate if this institution is limited to pre-investigation and not an investigative institution.

Problems that often arise since the formation and operation of PPATK in 2002, Polri has received 252 STR (Suspicious Transaction Reports) from the new PPATK as many as 181 cases carried out by investigations by the remaining Polri as many as 73 cases cannot be followed up because of reasons for insufficient evidence. Of the 181 cases investigated by the National Police 47 have been completed, while 134 cases are still under investigation.

Many cases reported by PPATK to the National Police have not reached 50% of these cases, even maybe only 20% of reports submitted by PPATK. Researchers see obstacles in handling cases that indicate TPPU because there are insufficient investigators, limited investigators in the field of money laundering have resulted in obstacles that have been reported by PPATK.

Limited human resources in the Criminal Investigation Body of the Police, especially on investigators against the TPPU resulting in the STR-STR being transferred to the Regional Police, sometimes because the TPPU investigator is lacking then it is combined by other investigators so that the investigation process can be completed quickly. Things like this should be of concern to various groups, especially the government, to take even more wise steps, that in the TPPU problem, people cannot deal with it arbitrarily because TPPU is a special crime, the

people or institutions that accompany it must be specialized institutions also, in the sense of people or institutions who understand and understand correctly about this crime

The PPATK Institution was established as a FIU in Indonesia, as one of the institutions dealing with money laundering issues, therefore this institution should be able to directly deal with money laundering problems that occur in Indonesia. Aside from being an informant institution PPATK can contribute even more if given the trust to carry out its function as an investigator. Considering that investigators lacking in the National Police force the investigation process to be protracted.

Therefore, the PPATK needs to be given more authority, namely the authority as a TPPU investigator to assist police investigators if there are suspicious financial transaction reports and the search for financial evidence in the form of funds. So that cases that have not been resolved will not accumulate and can be resolved.

PPATK is not part of the criminal justice system, but the existence of PPATK can complement the criminal justice system in Indonesia, especially in assisting police agencies and prosecutors in conducting investigations, investigations and prosecutions of TPPU. It is time for PPATK to also expand the criteria for parties who must report suspicious financial transactions, it is better for those who must report not only PJK but also other professions such as public accountants, lawyers, notaries, and property agents, because the professions This enables closeness to the process of money laundering.

In the example of the Adrian Herling Waworuntu PPATK case in collaboration with the National Police, the two institutions were able to complete and submit their case files to the public prosecutor. PPATK assisted the National Police in the process of investigating money laundering cases conducted by Adrian Herling Waworuntu, so it was revealed that Adrian had conducted a TPPU. Compared to other countries, institutions such as PPATK are also owned by the Philippines, Thailand, and Malaysia, these institutions together function as FIUs with the aim of handling and responsible in preventing and eradicating TPPU. But there are differences between PPATK and FIU institutions from each of the countries above, it is due to the different conditions of each country. One of the differences between PPATK and FIU in the Philippines, Thailand and Malaysia in terms of the criteria of the parties who are obliged to report suspicious financial transactions can be seen from:

1. Philippines, the name of the institution that handles or is responsible for preventing and eradicating TPPU is Anti Money Laundering Council (AMLC). There are parties who are obliged to submit suspicious financial transaction reports, namely:

   a. Securities companies, salesmen, and investment institutions;

   b. Companies engaged in the field of commodities and other monetary instruments.

The difference between PPATK and AMLC in terms of duties and authority is that AMLC can investigate all suspicious financial transactions and all deviations of the law, and carry out an action needed to eradicate TPPU, whereas PPATK cannot conduct investigations only until pre-investigation only and the pre-investigation is only a matter of suspicious financial transactions, the deviation of the law is not the duty and authority of the PPATK to conduct an investigation.

2. Thailand, the name of the institution that handles or is responsible for preventing and eradicating TPPU is the Anti Money Laundering Office (AMLO) of those who are obliged to submit suspicious financial statements, namely:

   a. Credit distributor;

   b. Saving and loan cooperative.

In terms of the authority of AMLO and PPATK differences, AMLO has the authority to provide educational programs to disseminate information, educate, and provide training or help the public and private sectors to spread the program, while PPATK only issues guidelines and publications to PJK regarding its obligation to assist in detecting the behavior of customers suspicious.

> 3. Malaysia, the institution tasked with preventing and eradicating money laundering is the Money Inserting Unit. The parties that are obliged to submit suspicious financial statements are:
>
> a. Housing business and electronic funds transfer;
>
> b. Business development financing and factory business.

In terms of tasks, this institution provides training to reporting institutions related to reporting obligations and suspicious transactions, while PPATK is limited to issuing guidelines and publications and information to reporting institutions relating to suspicious transaction reporting obligations, the form of socializing is not in the form of training.

When compared to FIU from other countries, PPATK still has shortcomings in carrying out its duties and authority. Compared to AMLC FIU from the Philippines, AMLC can conduct an investigation of all suspicious financial transactions and can carry out an action necessary to eradicate TPPU while PPATK cannot. Expansion of the criteria for parties must report the above countries have run it, while in Indonesia it is still fixed on the PJK only. Indonesia, especially the PPATK, needs to emulate the systems of the Philippines, Thailand and Malaysia so that this Indonesian-owned institution (PPATK) is clearer in its existence and is equal to the FIU institutions of other countries.

4. Conclusions

Cyber laundering crimes are created because of computer crimes in the current era of telecommunications, computers that are united with the Internet, so it can indirectly be said to be cybercrime, as well as cyber laundering. If our study is directed to cyber laundering, then the use of banks will be more dominant as a form of cyber laundering itself. To find out the mode of cyber laundering, we first know the modus operandi that is often used in committing money laundering, itself. The modes of money laundering itself are: Investment Cooperation; Swiss Bank Credit Collateral; Overseas Transfer; Disguised in Gambling; Disguising Documents; Foreign Loans; Foreign Loan Engineering. Based on the results of the author's library research on the use of banks in cyber laundering, obtained a number of banking activities that support the occurrence of cyber laundering for money laundering crimes, namely as follows Saving money from criminal acts under false names (identification); Keep money in the bank in the form of deposits / savings / accounts / demand deposits in some accounts so as to avoid suspicion; Exchange bills of crime-related money with other large or small bills; The bank in question may be asked to provide credit to customers who hold deposits with a guarantee of money deposited at the bank concerned; Using transfer facilities or EFT (Electronic Fund Transfer) with very high technology; Carry out fictitious export and import transactions using L/C (letter of credit) facilities by falsifying documents carried out in collaboration with relevant officials; Establishment or use of illegal banks. From a number of banking activities and the banking financial system that launched the cyber laundering, there are several forms of cyber laundering activities in money laundering activities, which include cybersquatting; E-Commerce; and the Illegal banking business.

The model of law enforcement in dealing with cyber laundering crimes, namely the model of law enforcement in a progressive manner, namely in its enforcement, the police, prosecutors, and judges not only involve elements that are factual in nature, but also the judge must be able to present the spiritual in society, meaning judges must act in accordance with the

wishes and care of the community. Even though the ITE and Anti Money Laundering Laws do not specifically regulate cyber laundering, on the basis of the demands of the community the judge must have the courage to open a progressive model of law enforcement, which is not based on existing laws alone, but must be based on the conscience of the community. Of course, judges are needed who understand the sociological problems of the community, why because the main goal is law enforcement in the broadest sense, namely law enforcement involving elements of society in it.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The author declares no competing interests.

References

Albrow, M. (1970). *Bureaucracy*. University College, Cardiff. Tt.

Ali, Ch. (1999). *Badan Hukum*. Bandung: Alumni.

Ancel, M. (1965). *Social defence: A modern approach to criminal problems*. London: Routledge & Kegan Paul.

Arief, B. N. (2006). *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia,* Jakarta: RajaGrafindo Persada.

Arief, B. N. (2003). *Kapita Selekta Hukum Pidana*. Bandung: Citra Aditya Bakti.

Atherton, C. R., & Klemmack, D. L. (1982). *Reseach methods in social work: An intoduction*. Lexington: Massachusetts: D.C. Heath & Co.

Bainbridge, D. I. (1993). *Komputer & Hukum*. Jakarta: Sinar Grafika.

Baudrillard, J. (1981). *Simulation*. New York: Semiotext(e).

Brenner, S. W. (2011). *Cybercrimes: New crimes or old wine in new boottles*. In R. D. Clifford (Ed.), *Cybercrime: The investigation, prosecution and defese of a computer-related crime*. Durham-North Carolina Academic Press.

Dias, R. W. M. (1976). *Jurisprudence*. London: Butterworths.

Dikdik, M. Manur, A., & Gultom, E. (2005). *Cyberlaw: Aspek Hukum Teknologi Informasi*. Bandung: PT. Refka Aditama.

Dirdjosisworo, S. (2002). *Respon Terhadap Kejahatan*, *Intoduksi Hukum Penanggulangan Kejahatan* [*Introduction to the law of crime prevention*]. Bandung: STHB Press.

Djumhana, M. (2000). *Hukum Pidana Di Indonesia*. Bandung: PT Citra Aditya Bhakti.

Duadji, S. (2008). *Selayang Pandang Praktik Pencucian Uang dan Kejahatan Asal*. Bandung: Books Terrace & Library.

Eco, U. (2008). *Tamasya Dalam Hiperealitas*. Jalasutra: Yogyakarta, tt.

Epping, A. et al. (1983). *Filsafat ENSIE*. Bandung: Jenmars.

Fajar, M., & Achmad, Y. (2010). *Dualisme Penelitian Hukum Normatif & Empiris*. Yogyakarta: Pustaka.

Fuady, M. (2006). *Bisnis Kotor Anatomi Kejahatan Kerah Putih*. Bandung: PT. Citra Aditya Bakti.

Ganarsih, Y. (2004). Pencucian Uang dan Permasalahan Penegakannya di Indonesia, *News Letter Kajian Hukum Ekonomi dan Bisnis*, No. 58.

Galanter, M. (1998). *Hukum Hindu dan Perkembangan sistem Hukum India Moderen,* Dalam A.A.G Peters & Koesriani Siswosoebroto (*ed*) *Hukum Dan Perkembangan Sosial*. Buku Teks Sosiologi Hukum Buku II. Jakarta: Pustaka Sinar Harapan.

Hamzah, A. (1992). *Hukum Acara Pidana Indonesia*, Sapta Artha Jaya. Jakarta: Cet.Pertama.

Hart, H. L. A. (1981). *The concept of law*. London: Oxford at the Clarendon Press.

Hasanuddin, A. F. et al. (2004). *Pengantar Ilmu Hukum*. Jakarta: Pustaka Al-Husna Baru.

Irman S., T. B. (2006). *Hukum Pembuktian Pencucian uang*. Bandung: MQS Publishing.

Irman S., T. B. (2006). *Anatomi Kejahatan Perbankan*. Bandung-Jakarta: MQS Publishing & AYYCCS Group.

Kartohadiprodjo, S. (1977). *Pengantar Tata Hukum Indonesia*. Jakarta: Ghalia Indonesia.

Kelsen, H. (2006). *Teori Umum Tentang Hukum Dan Negara*. Bandung: Nusamedia.

Kusumaatmadja, M. (2002). *Konsep-Konsep Hukum Dalam Pembangunan*. Bandung: Alumni.

Kusumohamidjojo, B. (2004). *Filsafat Hukum: Problematika Ketertiban Yang Adil*. PT. Jakarta: Grasindo.

Lamintang (1997). *Dasar-Dasar Hukum Pidana Indonesia*. Bandung: Citra Aditya Bakti.

La Patra, J. W. (1987). *Analzing the criminal justice system*. Lexington Mass; Lexington Books.

Lubis, S. (1989). *Landasan & Teknik Perundang-undangan*. Bandung: Mandar Maju

Machmudin, D. D. (2002). *Pengantar Ilmu Hukum: Sebuah sketsa*. Bandung: PT. Refika Aditama.

Madinger, J., & Zalopany, S. A. (1999). *Money laundering, a guide for criminal investigation*. Ploridfa, USA: CRS Press LLC.

Mahayana, D. (2000). *Menjemput Masa Depan, Futuristik dan Rekayasa Masyarakat Menuju Era Global*. Bandung: Rosda.

Makarim, E. (2005). *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Persada: PT RajaGrafindo Persada.

Manthovani, S. d. R. (2004). *Pemberantasan Tindak Pidana Pencucian Uang di Indonesia*. Jakarta: CV. Malibu.

Meleong, L. J. (2002). *Metodologi Penelitian Kualitatif,* PT. Bandung: Remaja Rosdakarya.

Mertokusumo, S. (2004). *Penemuan Hukum: Sebuah Pengantar*. Yogyakarta: Liberty.

Mertokusumo, S. (1993). *Bab-Bab Tentang Penemuan Hukum*. Bandung: PT. Citra Aditya Baktu.

Mertokusumo, S. (1996). *Mengenal Hukum: Suatu Pengantar*. Yogyakarta: Liberty.

Moeliono, A. M. (1990). Dkk, *Kamus Besar Bahasa Indonesia*. Jakarta: Balai Pustaka.

Muladi, & Arief, B. N. (1984). *Teori-Teori & Kebijakan Hukum Pidana*. Bandung: Alumni.

Munir, A. B. (1999). *Cyber law policies and challenges*. Rajawali Pers, Jakarta, Cet.Pertama.

Nasibitt, J. (2001). Nana Naisbitt dan Douglas Philips, *High Tech, High Touch, Pencarian Makna di Tengah Perkembangan Pesat Teknologi*. Mizan, Bandung.

Naisibit, J. (1994). *Global paradox*. New York: Wiliam Morrow and Comapany, Inc.

Naisibit, J. (1990). *Megatrend 2000,* Pan Paradox: Published in Great Britain: Sidgwick & Jackson Ltd.

Ohame, K. (1990). *Borderless world*. Harper Business: Printed In USA-Maknisey Company Inc.

Parsons, T. (1951). *The social system*. New York: The Free Press.

Piliang, Y. A. (2004). *Posrealitas: realitas Kebudayaan dalam era Posmetafisika*. Yogyakarta: Jalasutra.

Piliang, Y. A. (1999). *Sebuah Jagat Raya Maya: Imprealisme Fantasi dan matinya Realitas,* Pengantar Dalam Mark Slouka, *Ruang Yang Hilang: pandangan Humanis Tentang budaya Scberspace Yang Merisaukan*. Bandung: Mizan.

Piliang, Y. A. (1998). *Dunia Yang Dilipat*. Bandung: Mizan.

Prakoso, D. (1988). *Alat Bukti dan Kekuatan Pembuktian di dalam Proses Pidana*. Yogyakarta: Liberty.

Purbacaraka, P., & Soekanto, S. (1979). *Perundang-undangan & Yurisprudensi*. Bandung: Alumni.

Rahardjo, S. (2009). *Hukum Progresif: Sebuah Sintesa Hukum Indonesia*. Yogyakarta: Genta Publishing.

Rahardjo, S. (2000). *Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti.

Rahardjo, S. (1986). *Masalah Penegakan Hukum: Suatu Tinjauan Sosiologis*. Jakarta: BPHN, tt.

Raharjo, A. (2006). *Cybercrime, pemahaman dan upaya pencegahan kejahatan berteknologi*. Bandung: P.T Citra aditya Bakti.

Ramli, A. R. (2004). *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Refka Aditama, Bandung, Cet.Kesatu.

Remmelink, J. (2003). *Hukum Pidana: Komentar Atas Pasal_Pasal Terpenting dari Kitab Undang-Undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-Undang Hukum Pidana Indonesia*. Jakarta: PT. Gramedia Pustaka Utama.

Ranggawidjaja, R. (1998). *Pengantar Ilmu Perundang-Undasngan Indonesia*. Bandung: CV Mandar Maju.

Sabadan, D., & Kunarto (1999). *Kejahatan Berdimensi Baru*. Jakarta: Cipta Manunggal.

Salim, A. (2002). *Perubahan Sosial: Sketsa Teori dan Refleksi Metodologi Kasus Di Indonesia*. Yogyakarta: Tiara Wacana.

Sanusi, A. (1991). *Pengantar Ilmu Hukum & Pengantar Tata Hukum Indonesia*. Bandung: Tarsito.

Seidman, R. B. (1972). Law and development: A general model. Majalah *Law and Society Review*.

Siahaan, N. H. T. (2000). *Money Laundering dan Kejahatan Perbankan*. Jakarta: Pustaka Sinar Harapan.

Sjahdeini, S. R. (2004). *Seluk Beluk Tindak Pidana Pencucian Uang & Pembiayaan Terorisme*. Jakarta: PT. UTama Grafiti.

Slouka, M. (1999). *War of the World; Cyberspace and the high-tech assault on reality* (translated into Indonesian). "*Ruang yang hilang: pandangan Humanis tentang budaya cyberspace yang merisaukan*. Bandung: Mizan.

Soedarto (1990). *Hukum Pidana I*. Semarang: Yayasan Sudarto: Fakultas Hukum Undip.

Soedarto (1983). *Hukum Pidana Dan Perkembangan Masyarakat: Kajian terhadap Pembaharuan Hukum Pidana*. Bandung: CV. Sinar Baru.

Soedarto (1981). *Kapita Selekta Hukum pidana*. Alumni: Bandung, p. 35.

Soehartono, I. (1995). *Metode Penelitain sosial: Suatu Teknik Penelitian Bidang Kesejahteraan Sosial & Ilmu Sosial Budaya*. Bandung: *I* PT. Remja Rosdakarya.

Soekanto, S. (1983). *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: PT. Raja Grafindi Persada.

Soekanto, S. (1981). *Pengantar Penelitian Hukum*. Jakarta: UII Press.

Soekanto, S. (1980). *Pokok-pokok Sosiologi Hukum*. Jakarta: Rajawali Pers, Cet.kesatu.

Soemitro, R. H. (1990). *Metodologi Penelitian Hukum dan Jurimetri*. Jakarta: Ghalia Indonesia.

Stone, J. (1966). *Program and moment in the borderlands of law and social science*. Dalam *Law in Social Science*. The Second Half Century, Minneapolis: University of Minneasota Press.

Sumadikara, T. S. (2010). *Penegakan Hukum: Sebuah Pendekatan Politik Hukum dan Politik Kriminal*. Bandung: Kencana Utama.

Sumarjono, M. S. W. (1996). *Pedoman Pembuatan Usulan Penelitian, Sebuah Panduan Dasar*. Jakarta: Gramedia.

Sumbayak, R. F. S. (1985). *Beberapa Pemikiran Kearah Pemantapan Penegakan Hukum*. Jakarta: INDH-HIIL, Co.

Susantha, G. (1984). *Aborted creativity: science & creativity in the Third World*. London: Zed Book Ltd.

Suseno, F. M. (2003). *Etika Politik: Prinsip-Prinsip Moral Dasar Kenegaraan Modern*. Jakarta: PT. Gramedia Pustaka Utama.

Sutendi, A. (2008). *Tindak Pidana Pencucian Uang*. Bandung: PT. Citra Aditya Bakti.

van Apeldoorn, L. J. (1993). *Pengantar Ilmu Hukum*. Jakarta: PT. Pradnya Paramita.

Wahid, A. (2002). *Kriminologi & Kejahatan Kontemporer*. Malang: Lembaga Penerbit Fakultas Hukum Unisma.

Warasih, E. (2005). *Pranata Hukum: Sebuah Telaah Sosiologis*. Semarang: PT Suryandaru Utama.

Wignjosoebroto, S. (2002). *Hukum: Paradigma, Metode Dan Dinamika Masalah*. Jakarta: Elsam-Huma.

Yuliar, S. et al. (2001). *Memotret Telematika Indonesia Menyongsong Masyarakat Informasi Nusantara*. Bandung: Pustaka Hidayah.

Yuliar, S. et al. (2001). *Memotret Telematika Indonesia Menyongsong Masyarakat*.

Zaleski, J. (1999). *Spiritual cyberspace*. Bandung: Mizan.


C O A S