Advances in Social Science, Education and Humanities Research, volume 529
Proceedings of the International Conference on Engineering, Technology and Social Science (ICONETOS 2020)

Potential Criminal Action in Shadow Banking Practice

Iffaty Nasyiah[1*]

[1]*Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia*
[*]*Corresponding author. Email: iffaty.nasyiah@syariah.uin-malang.ac.id*

ABSTRACT
The industrial revolution 4.0 has a lot of influence, both socially, culturally, aspects of technology-information and others. Examples, in the information and technology aspects, such as trends in automation and data exchange. This includes cyber-physical systems, internet of things (IoT), cloud computing, and cognitive computing. In case, for examples are computational data storage, digital money, virtual money, ride-sharing transportation systems such as Go-Jek and Grab, shadow banking which includes financial technology and others. These benefits are also accompanied by negative aspects that urge to make clearer, firm and comprehensive rules. The most phenomenal thing in this industrial revolution is financial technology through shadow banking. The practice of shadow banking is felt to be strong enough that several parties have urged the government to enact regulations and legislation on shadow banking practices. Apart from the potential for an economic crisis, the practice of shadow banking can also lead to the potential for several criminal acts. This further strengthens the reasons for the formation of regulations regarding shadow banking, including its criminal aspect. The purpose of this paper is to describe the potential for criminal acts that occur due to the spread of shadow banking, especially illegal ones. This type of research is normative juridical with a statutory approach. The results of the study found the potential for criminal acts in banking, money laundering, double pledge, opening personal data (crackers), extortion and threats via the internet and insulting and defamation through the internet**.**

Keywords: *shadow banking, criminal acts in banking, money laundering, crackers, hacker, ITE.*

1. INTRODUCTION

Advances in technology and information are irresistible, even the economic progress of a nation depends on technological progress. European countries became the pioneers of developed countries due to technological advances which at that time began with the industrial revolution 1.0.

If the industrial revolution 1.0 in the 18th century was marked by the discovery of the steam engine, then the industrial revolution 4.0 in this century was marked by combining automation technology with cyber technology. The term industry 4.0 comes from a project in the German Government's advanced technology strategy that prioritizes factory computerization [1].

This industrial revolution had a lot of influence both socially, culturally, as well as in the aspects of information and technology. Information and technology aspects such as trends in automation and data exchange. This includes cyber-physical systems, internet of things (IoT), cloud computing, and cognitive computing. Concrete examples are computational data storage, digital money, virtual money, ride-sharing transportation systems such as Go-Jek and Grab, financial technology which includes shadow banking.

On the one hand, the development of financial technology has proven beneficial for consumers, business actors, and the national economy, but on the other hand it has potential risks which, if not properly mitigated, could disrupt the financial system. This new risk comes from shadow banking activities in lending and borrowing services based on financial technology. In a series of Staff Reports issued by the Federal Reserve Bank of New York (FRB), "shadow banks" act as "financial intermediaries that transform maturity, credit, and liquidity without explicit access to central bank liquidity or public service credit guarantees.*"* [2]

Shadow banking activities are the same as banking, namely collecting and channeling funds, providing loans

with high interest rates but the requirements are easier to fulfill than the requirements required by banks. It is feared that the existence of shadow banking will disrupt economic stability because high interest rates have the potential to cause non-performing loans (NPL) or bad credit [3].

Based on data from the Financial Services Authority as of September 30, 2019, there are 127 registered financial technology service providers. Meanwhile, the number of licensed financial technology service providers was 13 entities. There were only 7 previously licensed financial technology service providers then as of September 2019 there were 6 entities that increased their status from registered to licensed. These entities include Modalku, KTA Filat, Kredit Pintar, Mau Cash, Finmas and Klik ACC.

In contrast, the number of illegal service providers based on records from the Financial Services Authority has reached 1,230 entities. That number consists of 404 entities registered in 2018 and 826 entities throughout 2019. Of these, 42% of servers are not found in Indonesia, but use foreign servers. Only 22% of servers run from Indonesia, while the remaining 15% of servers come from the United States and other countries[3]. This illegal shadow banking practice has clearly caused unrest because it often harms society, financial institutions and or even the country's economy globally.

The negative sides of shadow banking include, *first*, it creates a greater potential risk in the financial system. This is because Shadow banking operates like a bank but with minimal supervision. They increase systemic risk because they have links with the traditional banking system through the credit intermediation chain. If a problem occurs in the shadow banking system, the risk can easily spread to the traditional banking system. *Second*, loose regulation. Monitoring shadow banking activities is often difficult because of the lack of information disclosure. *Third*, do not have deposit insurance. Unlike commercial banks, funds from capital suppliers do not have credit guarantees. So, if the confidence of the suppliers of capital falls, they can withdraw their funds at once. It disrupts shadow banking operations and forces them to sell assets. This causes shocks that can destroy the financial system. *Fourth*, high liquidity risk. Shadow banking raises short-term funds and uses them to invest in long-term assets. As a result, during periods of illiquid markets, they can go bankrupt and fail to meet their short-term obligations. [4]

The negative side is correlated and intertwined with potential criminal acts that can be detected from the rampant illegal shadow banking.

1.1. Criminalization of Shadow Banking

Criminalization means turning an act into a criminal act (a criminal act). There are various considerations and provisions that must be considered when criminalizing an act. These considerations are dealt with in a "criminal policy". Sudarto put forward a brief definition of criminal policy as: "a rational effort by society in tackling crime"[5]. Penal and non-penal efforts are part of criminal policy, and criminal policy is an integral part of social policy, namely policies or efforts to achieve social welfare[6]. From the meaning conveyed by Sudarto, the penal policy is a rational effort by society in overcoming crimes by using penal means.

Soetandyo Wignjosoebroto argues that criminalization is a statement that a certain act must be assessed as a criminal act which is the result of normative considerations (judgments) which in the end are decisions. Criminalization can also be interpreted as the process of determining a person's actions as punishable. This process ends with the formation of a law in which the act is punishable by a criminal sanction [7].

In connection with the issue of criminalization, Muladi reminded several measures that must be considered as a doctrinal guideline, namely: Criminalization should not appear to cause overcriminalization which is categorized as the misuse of criminal sanction; Criminalization must not be ad hoc; Criminalization must contain elements of victimizing both actual and potential victims; Criminalization must take into account the analysis of costs and results and the principle of ultimum remedium [8]; Criminalization must produce enforceable regulations; Criminalization must be able to get public support; Criminalization must contain elements of subsociality causing harm to society, even if it is very small; Criminalization must pay attention to the warning that every criminal regulation limits people's freedoms and gives law enforcement officials the possibility to curb that freedom.

The rise of shadow banking has met several guidelines stated by Muladi above, especially the existence of victims, does not cause over-criminalization, and has received public support. However, in terms of criminal sanctions as ultimum remidium, the authors do not agree because in certain conditions, in case, the mushrooming of shadow banking which is disturbing should be controlled by criminal sanctions as premium remidium.

2. POTENTIAL CRIMINAL ACTION IN SHADOW BANKING PRACTICE

2.1. Money Laundering Crime

Money laundering or what is known in English as money laundering is a term used for criminal acts in the financial sector. The use of the term money laundering was first written in newspapers, namely news about watergate in the United States in 1973. While the use of the term money laundering in the context of court or law

appeared for the first time in 1982 in a case of US v $ 4,255,625.39 (1982) 551 F Supp. 314. Since then the term has been widely accepted and used throughout the world [9]

In Article 3 of Law Number 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering (PPTPPU/ Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang) it is stated that money laundering is:

> *"Anyone who places, transfers, transfers, spends, pays, donates, entrusts, takes abroad, changes forms, exchanges currency or securities or other actions on assets which he knows or should reasonably suspect are the result of a crime as referred to in Article 2 paragraph (1) with the aim of concealing or disguising the origin of Assets shall be punished for the crime of Money Laundering with a maximum imprisonment of 20 (twenty) years and a maximum fine of Rp. 10,000,000,000.00 (ten billion rupiah)."*

Money laundering includes what is stipulated in Article 4 of the PPTPPU Law, namely :

> *"Anyone who conceals or disguises the origin, source, location, designation, transfer of rights, or actual ownership of Assets which he knows or should suspect is the result of a crime as referred to in Article 2 paragraph (1) shall be sentenced for laundering. Money with a maximum imprisonment of 20 (twenty) years and a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah)."*

Money laundering crime which will be abbreviated as TPPU has a special character, namely that this TPPU cannot stand alone as a complete criminal act even though it has fulfilled all the elements in a criminal act. Therefore, this TPPU is called a "subsidiary crime" or it can be said as an additional crime. As an additional criminal act, TPPU has a main criminal act or in the PPTPPU Law it is said to be a predicate crime or often referred to as a "predicate crime".

TPPU is intended so that the money generated from this "predicate crime" becomes clean money or as if it is lawful or legal money. There are 3 stages in ML: placement, layering, and integration. At the placement stage, money is placed in a legal financial system, such as a bank, insurance, mutual funds, etc. or placed in a company that has high cash flow. Then, at the layering stage, the money that has been placed is separated or sorted or made in layers to make tracking difficult. The point is that the perpetrator wants to create a complicated financial system so that dirty money is not detected. For example, the ML conducted by Nazarudin. How complicated the financial system was created by Nazarudin. Nazarudin committed a criminal act of corruption and gratification. The proceeds from this crime were then bought shares in several companies under the name of the company created by Nazarudin, namely the Permai Group.

Various ways can be done at this stage, for example: funds are allocated as capital for fictitious companies, purchases of anonymous goods (such as gold, stocks, foreign exchange, etc.).

Shadow banking, which is mostly on behalf of cooperatives, has the potential as a place for money laundering. Based on Sectoral Risk Assessment data compiled by PPATK and a number of related institutions, there are no less than 67,891 Sharia Savings and Loans Cooperatives / Savings and Loans Financing Cooperatives / Savings and Loans Units / Savings and Loans and Sharia Financing Units. "Of this number, only 501 KSPs have registered and submitted 297 Suspicious Financial Transaction Reports (SFTR) and 2,451 Cash Financial Transaction Reports (CFTR) during the period 2010 to June 2020."[10]

Thus, shadow banking becomes an easy target for mafia or criminals to deposit their dirty money with illegal business entities that are not affiliated with the legal financial system. They carry out the layering stages freely in this shadow bank.

2.2. Banking Crime

In banking law, there are two terms of criminal offense, namely: "Banking Crime" and "Banking Field Crime". Banking crime "is defined as a criminal act committed by a bank or a bank person, while a crime in the banking sector has a broader meaning because it can include criminal acts committed by people outside and inside the bank [11][12]. The term "banking field crime" is intended to cover all types of illegal acts related to activities in conducting bank business. There is no formal definition of a crime in the banking sector. There is a popular definition, that a banking crime is a crime that makes a bank a means (crimes through the bank) and a target of this crime (crimes against the bank).

In Act Number 7 of 1992 as amended by Act Number 10 of 1998 concerning Banking (hereinafter referred to as the Banking Law), there are thirteen types of criminal offenses that are regulated from Article 46 to Article 50A. The thirteen criminal acts can be classified into four types :

1. Criminal acts related to bank business licensing / bank legality. Regulated in article 46 paragraph (1) and (2);

2. Criminal acts relating to bank secrecy are regulated in Article 47 paragraph (1) and paragraph (2) as well as Article 47 A;

3. Criminal acts related to bank supervision and development are regulated in Article 48 paragraph (1) and paragraph (2).;

4. Criminal acts related to bank business are regulated in Article 49 paragraph (1) letters a, b and c, paragraph (2) letters a and b, Article 50 and Article 50A.[13]

Shadow banking practice can be categorized as a violation of article 46 paragraph (1) and if it is carried out by a business entity or legal entity (such as: Limited Liability Companies, unions, foundations or cooperatives), it may be subject to Article 46 paragraph (2). This article regulates criminal acts related to bank business licensing / bank legality and is often referred to as "Dark Bank". Basically, there are no applicable laws and regulations in Indonesia that specifically regulate the definition of "Dark Bank". Based on best knowledge and best practice, "Dark Bank" is an individual or entity carrying out banking business activities, without a business license to carry out these activities from the Management of Bank Indonesia (now the head of the OJK).[14]

Included in the violation of this article are; a) Running a bank-like business; Running a bank business or like a bank includes businesses both as a financial institution (attracting or collecting money from the public, channeling money back to the community or running a bank-like main business such as providing credit, providing services in payment traffic and money circulation[15]; b) Running a bank business; Running a bank business that is carried out by individuals or legal entities (corporations) is conducting banking business activities without permission from the OJK. The requirements that are required by this provision are to fulfill the elements of the offense in question having carried out banking operations, but do not have an official operating license; c) Running a bank business within a bank; Emphasis on fulfilling the offense element of this provision is running a bank business within a bank, a person who carries out business activities to collect funds from the public as well as channel them, whereby the collection and distribution of such funds is through an account he opens, so that he automatically takes refuge in an official bank business. For example, an official or a bank employee or a customer deposits funds that use his account to raise funds and simultaneously distributes these funds to the public with interest rates and certain conditions, which are usually different and / or save from the provisions of banking practice[13]; d) Establishing a bank without a business license from the management of Bank Indonesia (now OJK); Committing a criminal offense under Article 46 is punishable by imprisonment of at least 5 years and a maximum of 15 years, as well as a fine of at least 10 billion and a maximum of 200 billion..

Shadow bank raises public funds. Like conventional banks, they only act as facilitators who channel funds from investors to those in need or debtors. They offer investors high returns if they want to invest their funds in the *shadow bank.* The interest offered reaches 10 percent of the given capital. With this high interest rate, the shadow bank will indirectly attract high interest to the debtor.

Shadow bank is not shaped like a traditional bank, mostly in the form of Multi Level Marketing (MLM) or cooperatives. The Head of the Investment Alert Task Force, Tongam L. Tobing, said that the fraud under the guise of a cooperative has characteristics. First, offers through various media such as SMS short messages, websites, social media, Google Play Store, or Apps Store. Second, use the cooperative name. However, it does not have legal entity approval and / or business license from the competent ministry. Third, there is also the writing of the name of a licensed or well-known cooperative so as to generate trust. There are also those who claim to have been registered or supervised, as if they have been under the supervision of an authorized agency [16]

2.3. Opening Personal Data

One of the positive impacts of the 4.0 industrial revolution is the digitization of data into one complete and interconnected device. This impact will make it easier to find one's personal data and the things needed from that personal data. A simple example of this personal data interconnection is the existence of E-KTP, BI Checking, and others. BI checking, for example, through BI checking, a person will be able to know his credit history and credibility in the credit as long as this history is connected to the financial system. This makes it easier for financial institutions, both banks and non-banks, to analyze credit (financing) applications that will be submitted by prospective borrowers.

Apart from these positive impacts, there are also negative impacts. If there is a system error in the data center, the impact will be very large and massive. This error can be due to intentional or hacking or cracking as well as accidental bugging due to deficiencies or errors in writing program code.

Hacking or crackers are becoming a hot thing lately. The forgery of FB, Whatsapp accounts reaches the data center and uses the data for illegal purposes such as account theft, defamation for political purposes and the spread of “hoax” news for certain purposes. The personal data in question is your full name or real name, KTP, complete address, emergency contact, mother's name, KK and a selfie for authorization, account number and salary slip.

The rise of shadow banking can be used as an easy target for crackers. They steal data to get loans from shadow banks that do not require the bank to meet with prospective debtors. If this happens, the data owner will be the loser because he has to pay a sum borrowed by the crackers using fake data.

It has repeatedly happened that shadow bank customer data is stolen and then published, the most prohibited

thing in the traditional banking system is disclosing customer secrets.

Thus, the regulation regarding personal data protection (PDP regulation) becomes something that is urgent to be ratified with an applicable criminal sanction tool, not just a patch and inconsistency of norms.

The PDP Law is being finalized in the national legislation program (prolegnas). However, in fact there have been various legal instruments regulating this PDP, for example Law Number 23 of 2006 concerning Population Administration, Law Number 7 of 1992 concerning Banking and Law Number 11 of 2008 concerning Electronic Information and Transactions.

2.4. Information and Electronic Transaction Law violations

Revolution 4.0 can be said to have created a new regime in the field of law known as hukum telematika / hukum siber, hukum teknologi informasi (law of information technology) / hukum mayantara / virtual word law. In this regime, new criminal acts committed through the cyber world are also known as "cyber crime" or "mayantara crime".

Cyber crime is also commonly defined as computer fraud or computer crime because it is always done by means of a computer [17]. According to Mendell [18], there are two activities in computer crime, namely:1) Use of computers to carry out fraudulent, theft, or concealment acts intended to obtain financial gain, business advantage, wealth or services; 2) Threats to the computer itself, such as theft of hardware or software, sabotage and extortion.

There are two terms that are common in the world of cyber crime, namely hackers and crackers. Many interpret the same and both have negative connotations. However, both have different meanings. hacker is a term for someone who studies, modifies, analyzes and gets into a computer network. The goal of hackers is for profit or it could be just a challenge. Crackers can also be interpreted as people who have the ability in programming and can open computer network systems but with a negative purpose, while "cracking" is a term for activities carried out by crackers. For example for crime, data theft is important to sell it to certain parties, and the like [18].

A Hacker is a skilled computer expert who uses their technical knowledge to solve problems. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with his technical knowledge, uses a "bug" or "exploit" to break into a computer system. Thus it can be concluded that hackers have a positive connotation (white hat hackers) and crackers have a negative connotation (black hat hackers), but in Indonesia, they both mean “peretas”.

How is the relationship between borders and the rise of shadow banking? in technology finance, we knew peer to peer lending (P2P lending). P2P lending is what operates like a bank, and which is not licensed or illegal which we called shadow banks. As we discussed earlier, the rise of p2p lending is due to the computing system or digitization in the era of the 4.0 revolution. Therefore, it becomes normal if everything is done digitally or computationally, including when committing a crime.

Like TPPU, this ITE crime is also a criminal act that is "subsidized", meaning that crimes committed through information technology are included in ITE violations or crimes. For example, someone who creates or produces pornographic images and then posts them in a public place is said to have violated Article 4 of the Pornography regulation. However, if the image is then photographed and distributed via social media, it will also be subject to Article 27 of the ITE regulation.

Regarding opening and using personal data, it is regulated in article 26 of the ITE Law. The article says: "Any information via electronic media relating to a person's personal data, must be done with the consent of the person concerned". This article can be used as a basis if a shadow bank (P2P lending) opens and uses the personal data of its customers without permission. In paragraph 2 it is said that if this is done and causes a loss to the customer, then the customer can demand compensation.

3. CONCLUSION

The government must immediately handle shadow banking practice. Criminal sanctions as ultimum remidium must be applied seriously considering that this case has seriously disturbed the stability of the national banking economy. Delayed handling will increase several crimes related to shadow banking, including the practice of money laundering, disclosing customer personal data, practicing bank inside the bank and information and electronic crimes. *Otoritas jasa keuangan* must also carry out transparency regarding registered and unregistered financial technology to protect prospective customers so that losses do not occur.

REFERENCES

[1] N. Rahayu, Mengenal revolusi industri dari 1.0 hingga 4.0, in: Warta Ekonomi.co.id, 2020, https://www.wartaekonomi.co.id/read226785/ mengenal-revolusi-industri-dari-10-hingga-40

[2] R. J. Girasa, Shadow banking: the rise, risks, and rewards of non-bank financial services, Pace University, New York, 2016

[3] D. Fidhayanti, "Urgensi pembentukan regulasi shadow banking pada layanan pinjam meminjam berbasis teknologi finansial di Indonesia", Jurnal IUS kajian hukum dan keadilan, 8(2) (2020), 381-404, DOI: http://dx.doi.org/10.29303/ius.v8i2.722

[4] Shadow Banking: Definisi, Cara Kerja, Pro dan Kontra, 2020 in: https://cerdasco.com/sistem-shadow-banking/

[5] Sudarto, Hukum dan Hukum Pidana, p. 150

[6] B. N. Arief, Bunga rampai kebijakan hukum pidana, Bandung: PT. Citra Aditya Bakti, 1996

[7] S. Luthan, "Asas dan kriteria kriminalisasi", Ius Quia Iustum Law Journal of Islamic University of Indonesia, 16(1) (2009) 1-17, DOI: https://doi.org/10.20885/iustum.vol16.iss1.art1

[8] Muladi, Kapita selekta hukum pidana, Semarang: Badan Penerbit Universitas Diponegoro, 1995

[9] S. R. Sjahdeini, Seluk Beluk Tindak Pidana Pencucian Uang dan Pembayaran Terorisme, Jakarta: Pustaka Utama Grafika, 2004.

[10] Y. S. Vendy, "PPATK beberkan fakta, koperasi dipakai sebagai sarana pencucian uang kejahatan", in: Kontan.co.id, https://keuangan.kontan.co.id/news/ppatk-beberkan-fakta-koperasi-dipakai-sebagai-sarana-pencucian-uang-kejahatan

[11] HAK Moch Anwar, *Tindak Pidana di Bidang Perbankan*, Bandung: Alumni, 1986.

[12] M. Reksodiputro, Kemajuan Pembangunan Ekonomi dan Kejahatan, Kumpulan Karangan Buku Kesatu, Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum, 1994

[13] M. Sholehuddin, Tindak Pidana Perbankan, Jakarta: PT. Raja Grafindo Persada, 1997.

[14] Direktori institusi perbankan terdapat pada website Direktori Perbankan Indonesia, declared by Bank Indonesia, in: website resminya, http:// www.bi.go.id/id/publikasi/dpi/default.aspx

[15] M. H.A.K. Anwar, Tindak Pidana di Bidang Perbankan, Bandung: Alumni, 1982.

[16] M. Walfajri, Polisi Menyisir Koperasi Berpraktik Shadow Bank-ing, Businessinsight, 2020, retrieve from https://insight.kontan.co.id/news/polisi-menyisir-koperasi-berpraktik-shadow-banking

[17] B. Suhariyanto, Tindak Pidana Teknologi Informasi (cybercrime), Jakarta: PT. RajaGrafindo Persada, cetakan ke-3, 2014.

[18] Andi, "Mengenal Perbedaan Hacker dan Cracker Lebih Dalam", Qwords, 2020, retrieve from https://qwords.com/blog/perbedaan-hacker-dan-cracker/