Proceeding of 1st Ahmad Dahlan International Conference on Law and Social Justice

ISBN: 2962-4460
pp. 85-102

Prevention of Financial Crime after Covid 19

Nikmah Mentari[1*], Nurul Hudi[2]

1. *Faculty of Law, Universitas Hang Tuan, Indonesia*
   Corresponding e-mail: nikmah.mentari@hangtuah.ac.id
2. *Faculty of Law, Universitas Hang Tuan, Indonesia*
   nurul.hudi@hangtuah.ac.id

ARTICLE INFO

Keywords
Financial Crime; Development; Cyber; Covid 19, Prevention

ABSTRACT

The Covid-19 pandemic throughout 2020 was categorized as an extraordinary situation. The existence of large-scale social restrictions to lockdowns has resulted in changes in people's daily lives than they are very dependent on the internet and online digital transactions. The huge number on the use of online transactions and its transition cannot be separated from the increase of cybercrimes. The research aims at analyses prevention of financial crime after covid-19 which depends on sophistication of digital technology transaction. This research is normative juridical research with a conceptual approach and statute approach. The regulation related to cybercrime in financial had accommodated by ITE Law, OJK Regulations, supervision by PPATK and other institutions. The results show that, the prevention should accommodate for people use non-penal method which consist of three parts. There is prevention by online service providers, prevention by users of online services, and prevention by the government.

Introduction

Since the advent of Coronavirus Diseases on 2019 (Covid-19) until June 1, 2021, countless cases of positive confirmation number 170 426 245 and the confirmation of death reached 3,548,628 worldwide (Nanthini & Nair, 2020). Covid-19 cases in Indonesia reached 1,826,527 and 50,723 deaths, but 1,674,479 patients were confirmed to have recovered. Covid-19 has not only impacted the health and mental safety sector, however, but it has also become a worldwide pandemic and affects all important sectors in human life. Until now, the major impact caused by a pandemic of a disease on a country is very complex. This is because, unlike a localized and brief tragedy, a pandemic will spread throughout the globe over months or years, most likely in waves, and will affect populations of different sizes and composition. In terms of scale, a severe pandemic's impact may be outweighed by war or a widespread economic catastrophe rather than a hurricane, earthquake, or terrorist attack (Homeland Security Council, 2006).

This is evidenced by the mutation of new variants of Covid-19 in the form of B.1.1.7, B.1.3.5.1, and B.1.6.1.7 which has increased the number of confirmed Covid-19 patients in mid-June 2021. Pandemic Covid-19, which has similarities with the influenza pandemic is

a serious threat not only to the world population but also to the economy. The impact of economic losses can lead to economic instability. The impact is through direct costs, long-term expenses, and indirect costs. This pandemic is a worldwide concern that deserves a global response. Given the speed in which the virus spreads and the susceptibility of the human population as a whole

In addition to the economic and social impact, the Covid-19 pandemic also affects the type and level of crime that occurs in a country. During the lockdown or Large-Scale Social Restriction applied, some countries experience the uniqueness of the level of crime. For example, in Sweden, crime rates that have decreased are molestation, sexual crimes, and traffic offenses. Meanwhile, fraud and robbery did not change significantly. In global area, when the number of other crimes decreased, cybercrimes actually increased, especially hoaxes, hate crimes, and online transaction fraud. Cyber activity is an activity that has a global dimension coupled with very rapid advances in information technology so that it is very difficult for legal experts to give a firm definition of this crime.

One of the cybercrimes, namely online transaction fraud, is rife throughout 2020- 2021, with an estimated loss due to cybercrime of around USD 171 billion (detik.com, 2020). In addition, scams in the name of banks, and phishing have become commonplace during the pandemic. In the United States, the Federal Trade Commission (FTC) recorded fraud that cost consumers more than $469 million with an average loss of $360 through June 14, 2021. Fraudsters use a full suite of fraudulent tools including emails, phishing texts, fake social media posts, robot calls (robocalls), impostor schemes, and so on. Fraudsters follow the headlines, adapting messages and current issues during the Covid-19 pandemic.
The FBI's Internet Crime Complain Center received reports that phishing, smishing and similar scams had more than doubled in 2020. Additionally, cybercriminals (cybercrooks) registered tens of thousands of fake web domains related to Covid at the start of the pandemic. If people are not careful and visit these malicious domains, fraudsters will share phishing emails to directly hack personal data information. Fraudsters will also plant malware that digs into personal files on individuals' computers, hacking passwords and other personal data for identity theft.

The economy affected by the pandemic raises concerns for the public, thus providing an opportunity for fraudsters to imitate the banking industry and online loan providers. Scammers offer loans or assistance either by calling a phone, text message, or email. In addition, fraudsters also commit investment fraud, by offering investments both on the stock exchange and outside the stock exchange. In Indonesia itself, many cases of fraudulent investment were reported during the Covid-19 pandemic. The mode is in the form of offering high-interest rates above the Bank Indonesia rate.

The existence of crime in the financial sector during the pandemic definitely worsens the condition of countries that are struggling against Covid-19. This is considering that the community has been harmed due to the Covid-19 pandemic, then as a victim of crime and the emergence of unrest for the wider community. Especially now, as of June 2021, Covid-19 cases have experienced a spike and new variants have emerged due to the Covid-19 mutation. When the Covid-19 vaccine has been completed and vaccinations have begun, it is hoped that people's lives can run normally. Although it cannot return to its daily routine

before the Covid-19 pandemic. For example, the implementation of health protocols that are still in effect, micro-scale social restrictions that have an impact on life patterns that are all online and remotely. Therefore, the prevention of financial crime in cybercrime is deemed necessary so that it does not recur during the Covid-19 pandemic which is still in waves until the implementation of the new normal era.

Methodology

This research is juridical-normative research with a conceptual approach and statute approach. The juridical-normative research means that research would be focused in depth regarding the existence of Law and Regulations to analyze the legal issues. The Law and Regulations would be differed not only in the certain law but also law which contains of common rules to harmonize the explanation in research. Conceptual approach used to analyze specific or common theoretical about prevention and nonpenal policy. Statute approach used to analyze the regulation related to prevention of cybercrime before the Covid-19 pandemic.

Results and Discussion

Financial Crimes During the Covid-19 Pandemic

Cybercrime in Finance

According to Black Law's Dictionary of divine crimes, "*An act that the law makes punishable; the breach of a legal duty treated as the subject matter of a criminal proceeding. – Also termed criminal wrong* (Campbell, 2004). According to the Bill of Code Penal (RKUHP), crime (*rechtsdelict*) and offense (*wetsdelict*) are not distinguished but became one of the terminologies that is a crime. Moreover, the Code Penal (KUHP) itself is also not described the crime. Myriam Quéméner, who is examining French and European Union cybercrime legislation, describes cybercrime as criminal activity carried out in cyberspace using Internet technology. These offenses are divided into two categories: 1) unlawful access to data and systems for criminal purposes, and 2) fraud, falsification, diversion of funds, accessing illicit content, or defamation through internet services. The introduction of viruses into a computer system, external and internal computer intrusion, data manipulation, information theft, and fraud are identified as the most common types of cybercrime in a report by the Swedish National Council for Crime Prevention on the rise of information technology–related crime (Division, 2009).

The phrase "cybercrime" refers to illegal activities in which a digital device or information system is used as a tool, a target, or a combination of the two. Computer crime, electronic crime, e-crime, high-tech crime, information age crime, cybernetic crime, computer-related crime, and digital crime are all terms that can be used interchangeably when referring to cybercrime (Sabilon, et al, 2016). While cybercrime is a crime committed online. This crime knows no time and is not picky about its targets. It can happen to individuals or companies wherever they are. The goals of cybercrime are varied. It can be just a fad, to a serious crime that harms the victim financially. In practice, cybercrime can be carried outs alone or organized by a group of people. The perpetrators of cybercrime of course are people who

are experts in various hacking techniques. It is not uncommon for *cybercrime to be* carried out from different places at the same time (Suwiknyo et al., 2021)

The essence of the existence of cyberspace is a virtual construction created by a *computer* that contains abstract data that functions as follows: self-actualization; a forum for exchanging ideas; and means of strengthening democratic principles (Budhijanto,2019). People can enter the data system and computer network and then get a feeling that they really have entered a space that has no attachment at all to physical realities. Therefore, all of its activities in the cyber world have characters, namely: easy; its spread is very fast and widespread which can be accessed by anyone and anywhere; and can be destructive from loading insulting and/or defamatory material using electronic media, which is extraordinary because it has unlimited victimization patterns (Budhijanto, 2019).

Cybercrime, on the other hand, is a more particular definition of illicit action involving the internet and information technology. However, as cybercrime has evolved in everyday life, it has taken on many different shapes and manifestations. The direct effects of cyberattacks resulting from unlawful access to information resources and successful technical manipulation methods determine the unfavorable impact on business. The process of primary identification, recovery, and detection of later cybercrime attacks, on the other hand, necessitates a thorough examination as a managerial strategy, taking into account the fundamental position of authority (Antonescu & Birău, 2015).

Cybercrime is becoming a bigger problem, especially in underdeveloped countries. International cyber terrorism aims to steal classified information in order to gain complete control and hence large revenues. Furthermore, due to their inherent vulnerabilities, underdeveloped countries are particularly vulnerable to cybercrime. Due to these catastrophic occurrences, the global environment, which encompasses both financial and non-financial components, has changed dramatically. Modern technology allows for incredibly sophisticated tracking methods that appear to be untraceable and invisible. Cyber-attacks, in a metaphorical sense, are based on security system flaws, and their strategy is determined through tracking. The economic and corporate targets are severely harmed as a result of this illicit behavior (Antonescu & Birău, 2015).

Further, related to financial crimes. Internationally, there is no patent definitionrelated to the definition of financial crime (Hairi, 2015). Financial crime is one of the most widespread forms of criminality in any society. However, there has been no consensus on the definition of financial crime until today. It is impossible to recognize and respond to the newest sorts of financial crimes without correct classification and conceptualization of financial crimes. As a result, it's critical to comprehend the nature and characteristics of today's financial crime (Jung & Lee, 2017)

Financial crime is frequently defined as a crime against property, involving the illicit conversion of another's property for personal advantage. Financial crime is defined as "any non-violent crime that often ends in financial loss," according to the International Monetary Fund in 2001. Meanwhile, in the UK, the Financial Services and Markets Act 2000 (FSMA) states that financial crimes include 'any offense involving fraud or dishonesty; errors in, or misuse of information relating to, financial markets; or dealing with the proceeds of crime.

Pickett and Pickett (2002) use the phrases financial crime, white-collar crime, and fraud, financial crime is defined as "the employment of fraud for illegal gain, usually involving a violation of trust and some concealing of the true nature of the action." consecutively. Financial crimes, on the other hand, are often referred to as white-collar crimes, according to Interpol, which were initially described by Sutherland (1939) as "perpetrated by persons of respectable and high social status in the course of their employment". White-collar crimes are equivalent to occupational crimes under this concept. Financial crimes are classified as white-collar crimes, which are committed by people or organisations regardless of their vocation. Money laundering, insider dealing, fraud, and market manipulation are examples of white-collar crimes that financial crimes can catch (Jung & Lee, 2017).

Financial crimes, according to Interpol, are typically global and include the use of networks such as the internet. Transnational crime and cybercrime are inextricably linked to financial crime, posing a threat to financial institutions and individuals all over the world. According to Gottschalk, Victims range from individuals to institutions, companies, thus affecting all walks of life. At the micro-level, individual citizens and corporations suffer the consequences of serious financial crimes. Several market scams have claimed thousands of people, with many losing their savings, security and also affecting their emotional well-being, physical health, and relationships (Australian Crime Commission). At the macro level, financial crimes harm the entire economic and social system through substantial financial losses.

Financial crime in the sense of fraud is defined as a series of unlawful acts that are carried out intentionally and harm other parties. These harmful actions can take the form of corruption, collusion, and nepotism (KKN), fraud, theft, bribes, manipulation, embezzlement, looting, fraud, smuggling, misstatements. The act as a whole is an act that deviates from ethics and propriety/abuse (Sutrisno, 2013). Fraud, on the other hand, refers to a variety of criminal offences the deception of financial persons or services in order to conduct theft, including as forgery, credit scams, and insider threats. Financial organizations have always treated fraud as a loss problem, but in recent years, powerful analytics have been used to detect and even prevent fraud in real time. Financial institutions must utilize many of the same techniques to protect assets from all three types of crime, as the distinction between them has become less important (Hasham et al., 2019). Cyberattacks against financial companies are increasingly sophisticated and diverse. They use website attacks (DDoS), fake transfers, ATM hacks, and crypto theft. 40%of the dark web is financial fraud and leaked data is stolen. Brian Krebs, journalist and investigative reporter stated that expropriated accounts pose a less challenging threat than fake accounts and synthetic identity fraud, where stolen data is attached to fake accounts and identities. Financial firms invest in AI forces that uncover criminal behavior and hunt down fraudsters. Organizations will need a quantum strategy to stay safe incyberspace. Quantum computers are very fast and use the principles of quantum mechanics .

The act of acquiring financial benefit through profit-driven criminal activities, such as identity fraud, ransomware attacks, email and internet fraud, and attempts to steal financial accounts, credit cards, or other payment card information, is referred to as financial cybercrime. To put it another way, financial cybercrime includes things like obtaining

payment card information, gaining access to bank accounts to make unlawful transactions, extortion, and identity fraud to apply for financial products, among other things (visma.com, n.d.). That financial crimes use electronic devices. So, it is very closely related to cybercrime or in other words, financial crime is part of cybercrime. Cyber, used to commit financial crimes. For example (Suwiknyo et al., 2021)

a. Phishing, a phishing technique used by perpetrators to trick or manipulate bank account owners so that they provide data and information that can be used to access customer banking accounts. Deception is carried out to obtain confidential information such as passwords by impersonating a trusted person or business in an electronic communication. Channels are used as email, instant messaging services (SMS), or spreading fake links on the internet to direct victims to websites that have been designed to deceive.
b. Impersonation, which is an attempt by fraudsters to pretend to be someone else to obtain confidential information.
c. Internet banking fraud and online transactions using credit/debit cards, where the perpetrator claims to be a bank employee who informs him of changes in SMS/internet banking service fees, giving credit bonuses, distribution of invitation gifts, and others. The perpetrators also commit fraudulent online loan offers with low-interest rates.
d. Bank contact centers, namely fraudsters manipulate ATMs so that victims fail to make transactions and swallow cards in the machine. At the same time, members of the fraud team standby around the ATM to direct the victim to call a fake call center number. The team pretending to be a fake call center informed that the ATM had been blocked, then asked the victim to provide personal identity including the ATM PIN. The perpetrators who were around the victim then took the victim's ATM card which was swallowed in the machine.
e. Fraud SMS fraud, victims receive SMS content containing the lure of gifts, discounts, credit bonuses, tour packages, online loans, and others. Under the pretext of withdrawing the prize, the victim will be lured into an ATM and directed to follow instructions given by the perpetrator, such as transferring funds or top- up e-commerce balances.
f. Customer identity theft through open banking. Open banking is a service provider system for interaction between customers and financial institutions. This system can be read by the perpetrators of theft by 'skimming' or tapping customer profile data.
g. Skimming, this technique is carried out by the perpetrators by cloning the customer's ATM card into an empty ATM card. The trick is to install a pocket wifi router with a camera that is modified to resemble a PIN cover on ATMs to steal customer PINs before they are duplicated.
h. Malware, which stands for malicious software, means unwanted software in a computer system. Malware can include any software that is used to measure, manipulate or even spy on a system. Malware is a term used to describe malicious software. Malware can be spread through several methods. Most of it is via the internet, email, private messages, or web pages.40 Malware is very difficult for computer systems to detect. Because there are two (2) paths that cause the computer

system to be affected by malware, namely through a USB Drive and through the internet. Until now, malware is still a serious threat to cyberspace globally.

i. Hacking is a fairly common cybercrime term. This action is carried out by accessing the victim's computer system without rights. Hackers will use their skills to carry out various public crimes. Hacking is not always aimed at getting financial gain. Many hackers just want to show off their skills. For example, hacking actions that often occur are password breaches. This step is the starting point for hackers to commit further crimes. Some time ago, two major media in Indonesia were victims of hacking. The hackers managed to penetrate the security system of the media website and managed to make some of the news that was published.

Financial Crimes During the Covid-19 Pandemic

Even before the pandemic, it was seen that the development of e-commerce crimes or buying and selling online had shown a sharp increase. It is easy to predict that the pandemic period will provide more opportunities for cybercriminals to act. The limitations of movement during the pandemic have forced people not to leave their homes or restricted people from leaving their homes, thus making more people dependent on digital platforms to live their daily lives. This is because, during the pandemic period with the existence of work from home, online studies, and everything based on online transactions, Indonesian people have increased their use of the internet and digital technology. According to a survey by the Indonesian Internet Service Providers Association (APJII) from 2019 to the second quarter of 2020, the number of internet users in Indonesia was 196.7 million, equivalent to 73.7% of the population in Indonesia (BSSN, 2020).

Description of digital transactions and cybercrimes according to the White Paper on Mitigation of Cyber Incidents during the COVID-19 Pandemic compiled by BSSN. Massive distribution of *malware* and leveraging public curiosity about COVID-19 has the potential to cause unauthorized intrusion of an organization's IT infrastructure, leak of sensitive data, *malware infection* (ransomware, *virus*, etc.), or other cyber incidents. Inaddition, the majority of employees who currently work from home (WFH) are potentially exposed to this risk because they are not connected to a secure network as in the organization's corporate network (Syafrina & Irwansyah, 2018). It is not surprising that this period is a *window of opportunity* for criminals who make users of digital platforms – bothsellers and buyers – easy targets. Building fake websites to make shoppers believe they are dealing with the official website of a legal business entity, offering low-quality goods as genuine, are some of the more common online scams. This condition increasingly demands people to be more digitally literate, so it is not easy to fall into the trap of online criminals.

According to the general description of the Financial Action Task Force (FATF), there is an increasing trend and the emergence of financial crime risks due to the pandemic, namely financial fraud, one of which is fake investment offers and phishing. It's also a virtual scam (ojk.go.id, 2020). Report of Interpol related to typology of crimes that appear during Covid-19 (crime Typologies emerging from covid-19) based on the modus operandi was reported from the member states during pandemic era that is (Khweiled et al., 2021)

a. Advanced payment fraud
b. Donation fraud/charity fraud
c. Telephone fraud/phishing
d. Vaccine & testing kit fraud
e. Business email compromise fraud

The crime of fraud using electronic transactions is in principle the same as conventional fraud or fraud that occurs in society. The only difference is in the means of action, namely using an electronic system or by using a computer that is connected directly to the internet network. Therefore, as legal as fraud using electronic transactions can be treated the same as conventional fraud and can be charged with the legal rules contained in Law Number 11 of 2008 concerning Information and Electronic Transactions in conjunction with the Criminal Code (Sumadi, 2016).

In addition to cyber-attacks, criminals have taken advantage of the current crisis to recruit money mules under the premise of combating the virus's spread. From an infrastructure standpoint, there has been a dramatic surge in the registration of domain names with a reference to or containing the words 'corona' or 'covid' since the start of the pandemic. A large percentage of these registrations have been identified as malicious and linked to other sorts of criminality, such as organizing spam campaigns, hosting malware, or setting up scam sites (*How Covid-19 Related Crime Infected Europe During 2020*, 2020)

INTERPOL has received reports of monetary losses in the hundreds of thousands of dollars in a single occurrence, and these crimes are occurring across international borders. INTERPOL's Financial Crimes Unit receives information about fraud cases and requests to help stop fraudulent transfers on a near-daily basis from member countries. The thieves have largely targeted victims in Asia, but they have also utilized bank accounts in other parts of the world, such as Europe, to imitate real accounts tied to the impersonated organization (INTERPOL, 2020). In one case, a victim in Asia transferred payments to many bank accounts in Europe that were inadvertently controlled by criminals. National authorities were able to restrict some of the payments with the help of INTERPOL, but others were promptly transferred by the criminals to second and third bank accounts before being traced and banned. INTERPOL has aided in the investigation of more than 30 COVID-19-related fraud scam cases with ties to Asia and Europe, resulting in the freezing of 18 bank accounts and more than USD 730,000 in alleged fraudulent transactions. In addition, INTERPOL has issued a Purple Notice alerting authorities in all 194 of its member nations of this new sort of fraud.

Here are some known fraud schemes related to the Corona Virus pandemic as quoted from the US Department of Justice website (Saiful, 2020).

a. Counterfeit Drugs: A fraudster advertises fake drugs, fake vaccines, and so- called "immunity pills" and includes claims of the product's healing powers without any scientific or medical basis.
b. Counterfeit Testing: A fraudster sells fake testing kits in-house or performs door-to-door fake testing in exchange for money.

c. Health Care Scams: Fraudsters offer free (and fake) coronavirus testing to obtain Medicare or other health insurance information that they use to make false claims for benefits.
d. Counterfeit protection and equipment: Fraudsters advertise fake or untested personal protective equipment (including respiratory masks) through websites, social media, and robots. Fraudsters may not have real equipment to sell or provide equipment that has not been proven to work as advertised.
e. Phishing: A fraudster masquerades as representatives of well-known agencies such as the World Health Organization (WHO) and the Centers for Disease Prevention and Control (CDC) to trick victims into downloading malware or providing personal and financial information.
f. Fake Healthcare Providers: Fraudsters pretend to be doctors or hospital employees and call the individual by phone or email. They make false claims that they are treating a relative or friend for the coronavirus and ask for money for the purported treatment.
g. Identity theft: A fraudster uses social media to fraudulently search for donors or provide stimulus funds. The victim provides her bank account number or other personally identifiable information. A fraudster uses information entered by the victim to impersonate the victim and steal money from the victim's bank account.
h. Securities Fraud: The fraudster promotes securities in a public company that falsely claims that he has found the cure.
i. Fake Charity: A fraudster asks for charitable donations which he deems to be beneficial to the person affected by this virus and has the money for himself.

On another side, the economic crisis caused by COVID-19 has resulted in an upsurge in investment frauds, such as advertisements erroneously stating that publicly traded firms' products or services can prevent, detect, or cure COVID-19. Microcap stocks, which are often issued by the smallest companies, are particularly vulnerable to fraudulent investment schemes, according to FATF members, because they are low-priced equities with less publicly available information.

The *Corona Virus Disease* 2019 (COVID-19) outbreak that occurs in most areas of the world is currently being used by *threat actors* to spread *malware* (*viruses, ransomware*, etc.) and *email spam* to many parties. Based on information released by security service provider TrendMicro*, at least more than 200,000 *malware* and *spam* spread campaigns were detected worldwide in Q1 2020. In Indonesia alone, at least 4800 similar campaign activities were detected during that time span.

In research entitled 'Future-proofing Fraud Prevention in Digital Channels: An Indonesian FI Study', GBG collaborated with The Asian Banker to conduct a survey in more than 300 financial institutions in 6 countries in the Asia Pacific region. Managing Director of APAC GBG June Lee said the type of crime with the money mule model is predicted to increase drastically in 2020-2021 which has an impact on consumers in the banking and financial sectors. In 2019, more than 50 percent of respondents saw an increase in fraud, the most prominent of which was the synthetic ID of more than 60 percent. While in 2020, there is an increase in first-party fraud, but the most prominent is the money mule. Research

conducted by GBG also found that 55% of identity theft and 53% of identity theft were entered with money mules.

It is estimated that the loss due to cybercrime is around USD 171 billion because cyberattacks are increasingly complex, organized, and coordinated. Based on data from the National Cyber and Crypto Agency (BSSN), from January to August 2020, there were nearly 190 million cyber-attack attempts in Indonesia, an increase of more than four times compared to the same period last year which was recorded at around 39 million. The highest number was recorded in August 2020, where BSSN recorded the number of cyberattacks in the range of 63 million, much higher than August 2019 which was only in the range of 5 million. According to the Head of Sub-Directorate for Vulnerability Identification and Risk Assessment of National Critical Information Infrastructure III BSSN, Sigit Kurniawan, the sharp increase in the number of cyberattacks in Indonesia is directly influenced by changes in people's lifestyles during the pandemic (kompas.com, 2021). This is due to the increasing use of the internet and digital transactions during work from home and Large Scale Restritions.

Pusopskamsinas 2020 detected the occurrence of *phishing emails* in as many as 2549 cases with an increase in the number of cases of *phishing emails* occurring in March-May 2020. A total of 55.53% of *phishing emails were* sent during working hours (09.00 - 17.00) and 44.37% were sent outside working hours (BSSN. *Email Phishing is* a technique of Social *Engineering that* is widely used by hackers to trick victims. The hacker sends an *email* with an attractive title for the victim to open, usually financial or advertising-related (gifts, *vouchers*, discounts, etc.). *The email* usually contains *a file* insertion (*attachment*) or a *link* that leads to the download of a malicious program. This program can automatically work on the victim's computer and steal credentials, *passwords*, accounts, credit card information, and more. Phishing is becoming a popular choice among hackers because it is cheap, and its ease and effectiveness are quite high. Although many organizations have implemented security systems to block *phishing* attacks, attackers are also increasingly having more sophisticated *phishing* tools.

Phishing is the practice of sending fraudulent communications that appear to come from a trusted source and is usually done via e-mail. The purpose of phishing is to steal sensitive data such as personal data (name, age, address), account data (username and password), and financial data (credit card information, accounts) belonging to the victim, even to install malware on the victim's device.

Prevention of Financial Crimes in the New Normal Era

The Legislation Regarding Financial Crime Prevention

At the statutory level, to address cybercrime-based financial crimes, namely through the ITE Law. This was followed by OJK regulations and Bank Indonesia regulations to provide legal protection as well as prevention of crimes in the financial sector. The ITE Law departs from the fact that the use of information technology should contribute to the improvement of socio-economic welfare and encourage the achievement of the goals of the state. But not present any bit also initiate a complexity problem from the technical side, the spread of development, economics, law, and culture in the community. Based on these

considerations, in 2008 the ITE Law was issued (Law Number 11 of 2008 which is the first Law in the field of Information Technology and Electronic Transactions as a legislative product that became a pioneer in laying the basis for regulation and protection in the field of utilization of Information Technology and Electronic Transactions) Electronic Transactions (Budhijanto, 2019).

The Indonesian government's policy with the promulgation of the ITE Law is the first legal umbrella that regulates the cyber world (cyberlaw), because of its broad content and scope in discussing regulations in cyberspace such as the expansion of electronic evidence to the same as evidence that has been known so far, admits electronic signatures as a means of verification, and valid authentication of an electronic document, as well as regulation of acts committed in cyberspace as a crime. The formulation policy for regulating information technology crimes in Indonesia is regulated by the ITE Law which is special in nature (Sumadi, 2015).

Article 26 of the ITE Law Number 11 of 2008 states that unless otherwise stipulated by the laws and regulations, the use of any information through electronic media concerning a person's data must be carried out with the consent of the person concerned. In addition, any person whose rights are violated can file a lawsuit for the losses incurred under the law. The provisions in the article explicitly provide protection and prevent acts of data theft (theft) which are usually also misused for account break-ins, fraud to third parties with the mode of borrowing money, and other forms of crime that have implications for material losses.

The ITE Law also accommodates protection against hackers late either directly or indirectly through Article 30 which states that: (1) Every person intentionally and without right or against the law to access Computers and/or Electronic Systems belonging to other people in any way. Furthermore, in paragraph (2) Any Person intentionally and without rights or against the law accesses a computer and/or Electronic System in any way to obtain Electronic Information and/or Electronic Documents. Finally, paragraph (3) Any person intentionally and without rights or against the law accesses a computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking into the security system.

The sanctions imposed are contained in Article 46 of the ITE Law for actions in Article 30 paragraph (1) in the form of, being punished with imprisonment for a maximum of six years and/or a fine of a maximum of Rp. 600,000,000.00. Sanctions in paragraph (2) Anyone who fulfills the elements as referred to in Article 30 paragraph (2) shall be sentenced to a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiahs). And in paragraph (3) Anyone who fulfills the elements as referred to in Article 30 paragraph (3) shall be sentenced to a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp.800,000,000.00 (eight hundred million rupiahs).

Article 32 (1) Any person intentionally and without rights or against the law in any way alters, adds, reduces, transmits, damages remove, transfers, hides an Electronic Information and/or Electronic Document belonging to another person or the public. (2) Any person

intentionally and without rights or against the law in any way transfers or transfers Electronic Information and/or Electronic Documents to the Electronic System of another person who is not entitled. This activity is also often used in hacking social media accounts to commit fraud, for example asking for funds or making loans.

Sanctions for violators of Article 32 are contained in Article 48 (1) Anyone who meets the elements as referred to in Article 32 paragraph 1 shall be sentenced to a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp. 2,000,000,000.00 (two billion rupiah). (2) Everyone who fulfills the elements as referred to in Article 32 paragraph 2 shall be sentenced to a maximum imprisonment of 9 (nine) years and/or a maximum fine of Rp. 3,000,000,000.00 (three billion rupiah). (3) Everyonewho fulfills the elements as referred to in Article 32 paragraph (3) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 5,000,000,000.00.

Recently, there have been several cases of buying and selling personal data online. Previously, data leaks also occurred in BPJS Kesehatan. This is certainly very worrying because in the end it will be misused, for example for online loan applications. The ITE Law has warned in Article 34 that, (1) Any person intentionally and without rights or against the law produces, sells, procures for use, imports distribute, provides, or possesses:

a. Computer hardware or software designed or specifically developed to facilitate the actions as referred to in Article 27 to Article 33;
b. password via a Computer, Access Code, or something similar that is intended to make the Electronic System accessible

Sanctions for violating Article 34 are contained in Article 50 that any person who fulfills the elements as referred to in Article 34 paragraph (1) shall be sentenced to a maximum imprisonment of 10 years and/or a maximum fine of Rp. 10,000,000,000.00 (ten billion rupiah). Article 35 Any person intentionally and without rights or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if the data is authentic.

Article 51 (1) Anyone who fulfills the elements as referred to in Article 35 shall be sentenced to a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp. 12,000,000,000.00. (2) Everyone who fulfills the elements as referred to in Article 36 shall be sentenced to a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp. 12,000,000,000.00.

The ITE Law provides flexibility to investigators outside the Police environment so that other institutions with investigative authority can enforce cybercrime eradication following their fields. This is contained in Article 43 paragraph (1) In addition to Investigators of the Indonesian State Police, certain Civil Servants in the environment. The government whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions is given special authority as an investigator as referred to in the Law on Criminal Procedure Law to investigate criminal acts in the field of Information Technology and Electronic Transactions.

The implementer of law enforcement of the ITE Law to prevent penal crimes is the Indonesian National Police. The Police, through the Directorate of Cyber Crime (Direktorat Tindak Pidana Siber also known as Dittipidsiber), Bareskrim Polri, is a work unit under the Bareskrim Polri and is tasked with enforcing the law against cybercrimes. In general, Dittipidsiber handles two groups of crimes, namely computer crime and computer-related crime. Computer crime is a group of cybercrimes that use computers as the main tool. The forms of crime are hacking of electronic systems (hacking), illegal interception (illegal interception), changing the appearance of websites (web defacement), system interference (system interference), data manipulation (data manipulation) (patrolisiber.id, n.d.).

Computer-related crime is a cybercrime that uses computers as a tool, such as online pornography, online gambling, online defamation, online extortion, and online fraud. (Online fraud), hate speech, threats in the network (online threat), illegal access (illegal access), data theft (data theft). To support cybercrime evidence, Dittipidsiber is equipped with various capabilities and supporting facilities, one of which is a digital forensic laboratory. Therefore, Dittipidsiber also serves the examination of digital evidence from various work units, from the Headquarters to the Polsek level. In addition, Dittipidsiber also cooperates with various institutions, both at home and abroad, to facilitate coordination in the disclosure of transnational and organized cybercrimes (patrolisiber.id, n.d.)

Dittipidsiber also provides complaint services for victims of cybercrime through the cyber patrol website, as an effort to prevent and at the same time eradicate financial crime through cybercrime. According to Sudarto, police patrol activities that are carried out continuously include non-penal measures that have a preventive effect on potential criminals (Arief, 2011). In this regard, raids or operations carried out by the police in certain places and activities oriented towards community service or educative communicative activities with the community can also be seen as an effective non-penal effort (Arief, 2011). However, the National Police as law enforcers in preventing financial crimes in the cyber world does not work alone. There is another institution called Center for Indonesian Financial Transaction Reports and Analysis Center (PPATK), as an independent agency established to prevent and combat money laundering (Article 1 paragraph 2 of Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering). The role of the PPATK institution is to supervise if a suspicious transaction occurs which is the result of a criminal act. One of them is criminal acts in the financial sector such as banking, capital markets, insurance, fraud, and others. In other words, the crime can also be suspected or originated from cybercrime in the financial sector.

The presence of PPATK is to prevent the occurrence of financial crimes, which even though they do not have the authority to investigate and investigate, prevent *predicate crimes*. This is based on the PPATK's functions, namely preventing and eradicating money laundering offenses, managing data and information, monitoring the compliance of the Reporting Party, and analyzing or examining reports and information on financial transactions with indications of money laundering and other criminal acts. Thus, PPATK also has an important role to monitor the flow of funds for financial crime actors which can then be used as evidence for law enforcement.

In the practice of providing financial services, the OJK, based on the mandate of the OJK Law, also has an important role in preventing financial crimes, especially by financial service providers. H al this is a kind of prevention that is specifically regulated in the field of financial services. As for the legitimacy of the OJK as an authorized institution in law enforcement to prevent financial crimes, namely based on article 1 number 1 of Law Number 21 of 2011 concerning the Financial Services Authority (OJK Law), which is an independent institution and free from interference from other parties, which has functions, duties, and authorities of regulation, supervision, examination, and investigation.

In addition, it is emphasized in CHAPTER XI of the OJK Law concerning Investigations that certain Civil Servant Officials whose scope of duties and responsibilities include supervision of the financial services sector within the OJK are given special powers as investigators as stipulated in the Criminal Procedure Code. In the implementing regulations, OJK Regulation Number 22/POJK.01/2015 concerning Criminal Acts in the Financial Services Sector confirms the technical implementation of OJK investigators as law enforcement for crimes in the financial services sector. Article 1 Number 2 explains that a criminal act in the Financial Services sector is an act/event that is punishable by a crime regulated in several laws.

For example, the laws governing OJK, Banking, Sharia Banking, Capital Markets, Pension Funds, Microfinance Institutions, Insurance, Indonesian Export Financing Institutions, Social Security Administering Bodies, Bank Indonesia as long as it relates to interference with the implementation of OJK duties in regulating and bank supervision, as well as the Law on other Financial Services Institutions, as referred to in the OJK Law. The above mandate also gives legitimacy to the OJK to monitor and carry out investigations into any financial crimes, whether carried out conventionally or in cyber.

Regarding cyber-based financial crimes, OJK focuses on implementing digital financial innovations and digital-based investment services and implementing anti-money laundry. Digital financial innovation is regulated in OJK Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector. OJK requires digital-based financial service providers to apply the principles of independent monitoring at least including:

a. the principles of information and communication technology governance following thelaws and regulations;
b. consumer protection under the provisions of this Financial Services AuthorityRegulation;
c. education and socialization to consumers;
d. confidentiality of consumer data and/or information including transaction dataand/or information;
e. the principles of risk management and prudence;
f. the principle of anti-money laundering and the prevention of terrorism financing inaccordance with the provisions of the legislation; and
g. inclusiveness and the principle of information disclosure.

In accordance with Article 18 paragraph (1) POJK 13/POJK.02/2018. OJK also requires to provide data protection and confidentiality for digital-based financial service providers following Article 30. As well as the prohibition in Article 38 to provide data and/or information regarding consumers to third parties. OJK Regulation Number 12/POJK.01/2017 concerning Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs in the Financial Services Sector. The POJK anti-money Laundry is a form of prevention to prevent financial crimes, especially the type of money laundry and funding for terrorism. OJK requires financial service providers (PJK) to implement anti-money laundry programs and prevent terrorism financing. The output of the regulation is the internal policy of the PJK company.

Prevention of Financial Crime in The New Normal Era

Criminal policy includes employing criminal law to combat crime. The purpose of preventing these crimes is to fulfill the criminal policy's ultimate goal, which is to provide community protection in order to create community prosperity. The employment of criminal law is one of the methods to prevent and overcome the problem of crime (penal policy). The problem of criminal law policy is not only limited to making or creating a statutory regulation that regulates certain things (Setiyawan et al., 2019). More than that, criminal law policy requires a comprehensive approach that involves various legal disciplines other than criminal law and the reality in society so that the criminal law policy used does not come out of the broader concept of social policy and national development plans in the context of realizing prosperity. Public. However, in this case, there is an approach that is used in the context of efforts to prevent crime through a criminal approach that can use 2 (two) facilities, namely penal and non-penal ways.

The prevention of crime is non-penal, which focuses on the preventive nature before the crime occurs. Efforts to overcome crime need to be taken with a policy approach, in the sense of (Arief, 2011).

a. There is an integration between criminal politics and social politics.
b. There is integration (integrality) between efforts to overcome crime with penal andnon-penal.

Non-penal efforts are more preventive for the occurrence of crime, so the main target is to deal with the conducive factors that cause crime These factors, among others, focus on problems or social conditions that can directly or indirectly lead to or foster. One of the non-penal ways to overcome social problems in the GP Hoefnagels scheme is social policy that goes into the "prevention without punishment" route. Social policy is a policy or rational effort to achieve public welfare. so that it is identical to the national development policy or planning which covers various fairly broad aspects of development.

Likewise, with the reality of the development of information technology, cybercrime is present as a negative existence and is dangerous for the development itself, because its presence is not wanted. However, it cannot be denied because it has become part of the currency side. Denying cybercrime means denying the development of information technology. This is quite reasonable with the adage above, "where there is society, it is evil (Saputra et al., 2021) Therefore, crime prevention efforts are a continuous and continuous

effort. The moreadvanced human civilization, as an implication of the development of science and technology, emerging various types of crime with a new dimension, which includes cybercrime. In line with this, countermeasures are needed to ensure order in society. From a legal perspective, this effort is realized through criminal law. Criminal law is expected to be able to fulfill public order.

In responding to cyber financial crimes in the new normal era, non -penal based, among others:

1. Prevention by Online Service Providers

In addition to being required to improve technical security on portal services and ensure the confidentiality of personal data, online service providers (e-commerce, mobile and internet banking, fintech, etc.) need to have risk mitigation for the possibility of crime or fraud in their product services. What's more, currently most transactions made by customers are digital online. referring to the pandemic condition that shows dependence and the shift in people's habits from conventional to online transactions, must be a major concern for online transaction providers. Mitigation of these risks is an internal policy and a guideline for the company in protecting customers. In addition, online service providers must provide security education for customers in conducting transactions on their portals.

2. Prevention by Online Service Users

One of the best preventions of financial crimes is from the perspective of the potential victims themselves. In this case, of course, users of online services. not without reason, the opening of opportunities for financial crime through cybercrime is also much 'supported' by the lack of vigilance of online service users. For the user community, an active role is also needed in preventing the occurrence of financial crimes and cyber-attacks that cause losses, including:

a. Changing account passwords at affected services and periodically changing passwords.
b. Avoid using the same password on all online services.
c. Enable 2-factor or multi-factor authentication
d. Avoid using public wifi when making online transactions
e. Avoid payment information such as credit cards automatically in online service systems.
f. Do not share personal data information on social media.
g. Ignore messages detected as spam
h. Do a double-check if there are parties who contact to ask/borrow money.
i. Avoid sites or websites that are not credible.
j. Do not reveal any code, pin number, credit card number, etc. that goes into messages or emails.
k. Avoid downloading malicious apps.
l. Make payments and transfers through official sites and be more aware of who is receiving and the reason for sending money.
m. Checking the credibility and status of financial service providers on the OJK portal before investing.

3. Prevention by the Government

So far, the National Cyber and Crypto Agency has even issued a White Paper on Mitigation of Cyber Incidents During the Covid-19 Pandemic as a response to the increasing and increasingly vulnerable cybercrime in Indonesia. The White Paper serves as an internal guide in dealing with cyber threats during the Covid-19 pandemic. The internal scale guidelines are a preventive measure in preventing cyber-based financial crimes. The government through BSSN and Kominfo can work together to educate the public about the risk of financial crime through cyberspace. The government, which has full authority in managing the internet in Indonesia, must be more proactive in blocking and deleting accounts or sites that are indicated to cause financial crimes. So far, during the 2020 pandemic, Kominfo has blocked telegram accounts related to the piracy of circulating films. However, there are still many Telegrams group accounts that gather large numbers of people to offer fraudulent investments.

In addition, it is necessary to immediately ratify the Personal Data Protection Bill. The urgency of the Personal Data Protection Law is a basic need in the new normal era, especially now that people have depended on and are getting used to using digital technology access. Because so many forms of cybercrime (cybercrime) which forms the crimes were committed by people who are expert in the use of computers or better known by the *hacker*, then the government should embrace the *hackers* is that they use his skills to ward off cybercrime.

Conclusion

In fact, the pattern of community activity during the pandemic has shifted due to physical and social distancing policies. This has led to changes in remote-based activities or using more interactions with online media. Work from home, online study, and transaction services even in terms of buying and selling and delivery have increased internet usage. The increasing use of the internet also increases the threat and attacks of cybercrime. One of the cybercrime attacks is related to financial crimes. Prior to the pandemic, the state through several laws and regulations had accommodated penal and non-penal-based prevention, namely through the ITE Law, OJK Regulations, supervision by PPATK, and the establishment of a special division within the National Police Agency related to cybercrime. However, referring to the pandemic which is an extraordinary condition, and the increasing use of online transactions, more adaptive prevention efforts are needed. That in the future, when there is a disease pandemic after society has completely depended on online transactions, as well as the increasingly sophisticated online digital technology, prevention efforts from three parties are needed. This three-party prevention is the implementation of non-penal prevention, which includes prevention by online service providers; prevention by users of online services, and prevention by the government.

References

Antonescu, M., & Birău, R. (2015). inancial and Non-Financial Implications of Cybercrimes in Emerging Countries. *Procedia Economics and Finance*, *32*, 618–621.

Arief, B. N. (2011). *Bunga Rampai Kebijakan Hukum Pidana : Perkembangan Penyusunan Konsep*

KUHP Baru. Kencana Prenada Media Group.

BSSN. (2020). *Laporan Hasil Monitoring Keamanan Siber Tahun 2020*.

Budhijanto, D. (2019). *Cyber Law dan Revolution Industri 4.0*. Logoz.

How Covid-19 Related Crime Infected Europe During 2020, (2020). https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

Hairi, P. J. (2015). A Systematic Review of Criminal Recidivism Rates Worldwide: Current Difficulties and Recommendations For Best Practice. *PLoS ONE*, *10*(6), 199–216. https://doi.org/10.1371/journal.pone.0130390

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial Crime and Fraud in The Age of Cybersecurity. In *McKinsey & Company* (Issue October).

Homeland Security Council. (2006). *National Strategy for Pandemic Influenza: Implementation Plan*. The White House.

Jung, J., & Lee, J. (2017). Contemporary Financial Crime. *Journal of Public Administration and Governance*, *7*(2), 88–97.

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID -19 Pandemic. *International Journal of Information Engineering and Electronic Business*, *13*(2), 1–10. https://doi.org/10.5815/ijieeb.2021.02.01

Nanthini, S., & Nair, T. (2020). COVID-19 and the Impacts on Women. *NTS Insight*, *July*, 1–11. https://www.who.int/news-room/detail/29-06-2020-covidtimeline

Saiful, H. B. (2020). Covid-19 and its Relevant Crimes: Financial Intelligence Role. *Majalah IFII*.

Saputra, M. B. B., Heniyatun, H., Hakim, H. A., & Praja, C. B. E. (2021). The Roles of Local Governments in Accommodating the Registration of SME's Product Trademarks. *Amnesti Jurnal Hukum*, *3*(1), 53–59. https://doi.org/10.37729/amnesti.v3i1.1227

Setiyawan, W. B. M., Utara, T. H., & Wulandari, F. D. (2019). Pembentukan Small Claim Court (SCC) sebagai Upaya Mewujudkan Asas Peradilan Sederhana, Cepat dan Biaya Ringan. *Citizenship Jurnal Pancasila Dan Kewarganegaraan*, *7*(2), 72–81.

Sumadi, H. (2016). Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia. *Jurnal Wawasan Yuridika*, *33*(2), 175. https://doi.org/10.25072/jwy.v33i2.102

Sutrisno, C. R. (2013). Audit Forensik : Membongkar Dan Mencegah Kejahatan Keuangan. *Prosiding Seminar Nasional Audit Forensik*, 54–65.

Suwiknyo, F. B., Tonny Rompi, & Muaja, H. S. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *IX*(4), 183–192. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33358

Syafrina, A. E., & Irwansyah. (2018). Ancaman Privasi Dalam Big Data. *Jurnal Penelitian Komunikasi Dan Opini Publik*, *22*(2), 132–143.