

THE ROLE OF BANKING IN PREVENTION ONLINE GAMBLING CRIME

Efendi Gunawan Sidiki¹, Barbalina Matulesy²
efendigunawansidiki@gmail.com¹, bmatulesy542@gmail.com²,

Fakultas Hukum Universitas Doktor Husni Ingratubun Tual^{1,2}

Articles Info

Received: 2021-06-07

Revised: 2021-10-10

Accepted: 2022-12-10

Keywords:

*The Role of Banking,
Prevention, Online
Gambling.*

Abstract

This research aims to obtain data and information regarding the role of banking institutions in preventing criminal acts of online gambling as well as factors that become obstacles to implementing the role of banking institutions in preventing criminal acts of online gambling. In this research, the methods used are normative juridical research methods and empirical juridical research methods, supported by data collection techniques in the form of direct observation and interviews in the field in order to obtain valid and accountable data. The results of the research show that the implementation of the role of banking institutions in preventing criminal acts of online gambling has not been implemented according to the aims and objectives of implementing the know your customer principle and/or the customer due diligence principle, as a result of the lack of clarity in the legal regulations as regulated in the Law. -Law Number 10 of 1998 concerning Banking, as well as those regulated in the Financial Services Authority Regulation Number: 12/POJK.01/2017 concerning the Implementation of Anti-Money Laundering and Terrorism Financing Prevention Programs in the Financial Services Sector. Namely, the bank is only passive, and reports suspicious transactions on a request basis. Meanwhile, the factors that become obstacles are, firstly, the bank ratio factor, secondly, advances in technology and electronic transactions and thirdly, the regulation of the nominal amount of money that can be carried out by EDD as regulated in Article 15 of the Financial Services Authority Regulation Number: 12/POJK.01/2017.

I. Introduction

Gambling from various points of view is a bad act, and is not in accordance with the norms that exist in society because of its negative nature. Gambling is one of the ills of society and is categorized as a crime and/or criminal act. Gambling or gambling is a game that involves betting on property, money, where the losing party must pay a certain amount of money or property to the winning party, usually this can result in a short time to get the same result "win" or "lose".

In Indonesian society, gambling is not a new phenomenon. Gambling has existed since ancient times along with the development of world civilization. The oldest evidence of gambling is thought to have existed since 3000 BC in Ancient Egypt with gambling using "dice". Then, in 2300 BC, namely a type of gambling found in Ancient Chinese civilization, called "lottery", then in 800 AD the game "card gambling" appeared in China, in the 14th century card games began to be known in Europe, until they entered Indonesia. by VOC traders. "Cockfighting", "card gambling" and "dice" or also called "po" were already known at this time. During the VOC era, the highest tax income was obtained from gambling houses, which were managed by the Chinese Kapitan (Chinese) in 1620. Meanwhile, European or Dutch-style "lottery" games only entered the Dutch East Indies in the mid-19th century.

In line with the development of information technology, this mode of crime has developed. In the beginning, gambling or better known as "gambling", "betting" such as "guessing numbers", "lottery", "card gambling", "skill gambling", "cockfighting", or "cockfighting", etc., known as conventional crimes. However, nowadays with various technological advances, especially the use of the internet (inter connection network), it is easier for people to commit this crime through virtual spaces or cyber spaces where and at any time they can play modified types of gambling. using technological advances or better known as "online gambling". Such as "online soccer gambling", "online soccer gambling", "online casino gambling", "online poker gambling" via the internet, which only rely on the luck factor and are activities where the final result cannot be known for certain.¹

The phenomenon of online gambling from day to day is increasingly widespread in various levels of society, from the lower classes to the upper classes. This gambling does not look at a person's age, gender, social status or

¹ Edmon Makarim, 2005, *Kompilasi Hukum Telematika*, PT Raja Grafindo Persada, Jakarta, hal 10.

occupation, it is carried out from small scale to large scale gambling. Online gambling can be done in markets, terminals, hotels, offices, homes, boarding houses, social gathering activities and even gambling has developed and can occur in the morning, afternoon and evening. In other words, online gambling activities do not know space, place, time and who does it.

Online gambling games in the context of criminal law constitute a crime and/or criminal act. This is based on the regulations regulated in Law Number 7 of 1974 concerning the Control of Gambling, the regulation of criminal acts of gambling which are regulated by the provisions of Articles 303 and 303bis of the Criminal Code (KUHP) and criminal acts of gambling which use regulated electronic transaction facilities. Article 27 paragraph (2) along with Article 45, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE).

In the provisions of Article 1 of Law Number 7 of 1974, it is stated that all criminal acts of gambling are crimes. Meanwhile, Article 303 paragraph (1) paragraph (2) carries a maximum prison sentence of ten years or a maximum fine of twenty-five million rupiah, and Article 303bis, which carries a maximum prison sentence of four years or a maximum fine of ten million rupiah.

Meanwhile, the provisions of Article 27 paragraph (2) along with Article 45 of the ITE Law, states that every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain gambling content. Threatened with criminal threats as regulated in Article 45, namely imprisonment for a maximum of 6 years and/or a fine of a maximum of IDR 1,000,000,000.00 (one billion rupiah).²

This crime is committed through online transactions, with services provided by providers through websites or pages and applications provided. Examples of online gambling, which can be accessed easily, are: 25-in Casino, Big Fish Game, Roulette, Online Poker, Blackjack 21 HD, Sic bo, Baccarat, Works Series of Poker, and Domino QiuQiu.³

According to the Director of Economic Crimes, the National Police's Special Criminal Investigation Agency, in carrying out cyber patrols, found 360 sites that carried out online gambling games, and detected 460 bank

² Budi Suhariyanto. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime)*. Raja Grafindo Persada. hlm 12

³ <https://www.todayline.me/id/v2/article/I217r3> Game Judi Online Paling Marak di Android, Iseng Berhadiah. Diakses 07 April 2024.

accounts.⁴ Aswin Sasongko, the value of online gambling transactions in Indonesia in one day can exceed billions of rupiah. The problem is that this practice is difficult to eradicate considering the network problem of Internet Access Provider (NAP) access providers is not only in Indonesia but is owned globally, which can include Internet Service Providers (ISP) that have received permission from the Ministry of Communication and Information and there are hundreds of them.

This is where the role of a banking institution is required, which is not only looking for economic profit. Although the main function of Indonesian banking is as a collector and distributor of public funds. Banking institutions must also play an active role in addressing and preventing online gambling practices. Because gambling will be very dangerous for the livelihood and lives of Indonesian people. By gambling, people will be determined to sell their possessions and wealth, which can even give rise to criminal cases or other crimes. This is certainly not in line with the aim of establishing banking institutions in Indonesia as regulated in Article 4 of Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, namely supporting the implementation of national development, in the context of increasing equality, economic growth and national stability towards increasing people's welfare.

Banking, as a financial institution that plays an important role in the country's economic system, should play an active role in efforts to assist government policy, in the framework of preventing and eradicating criminal acts of online gambling in Indonesia.

The phenomenon that occurs is that banking institutions are considered to have not played an active role in efforts to prevent criminal acts of online gambling, by only adhering to the principles or principles of bank secrecy (confidential principle). The principle of confidentiality is indeed important, but this principle or principle is not the only principle or principle adhered to in banking law. There are still other principles that also need to be considered, namely the principles or principles of economic democracy, the principle of prudence (prudential principle), the principle of trust (fiduciary principle), and the principle or principle of knowing your customer (know your customer principle).

In relation to the role of banking institutions in preventing criminal acts of gambling, banks must pay attention to the meaning of the know your customer principle, namely monitoring transaction activities including

⁴ Telusuri Judi Online, Polri temukan 360 situs dan 460 rekening Bank, lihat <https://www.nasional.kompas.com/read/11310001/> diakses 07 April 2024.

reporting any suspicious transaction activities. This principle is regulated in Bank Indonesia Regulation Number: 3/10/PBI/2001 as amended by 5/21/PBI/2003 concerning the Implementation of Know Your Customer Principles.

In recent developments, the use of the term Know Your Customer Principles has been replaced with the term "Customers Due Diligence (CDD)", in the customer identification, verification and monitoring process. For high-risk customers, they are required to carry out "Enhanced Due Diligence (EDD)", namely more in-depth CDD actions when conducting business relationships with high-risk customers. This principle must be strictly observed by staff, especially tellers, customer service and the digital banking transaction analysis section.

The objectives to be achieved in implementing the know your customer principle or CDD and EDD are: first, increasing the role of financial institutions with various policies in supporting the practices of financial institutions, especially banking institutions; secondly, avoiding the various possibilities of financial institutions becoming a venue for crimes and illegal activities carried out by customers; and thirdly protecting the good name and reputation of banking institutions. Based on the descriptions above, the author presents this article with the title "The Role of Banking in Preventing Online Gambling Crimes"

2. Research Method

The approach method used in this research is the Normative Juridical research method, starting from examining library data or secondary data, (primary legal materials and secondary legal materials), especially statutory provisions that are related to the title and formulation of the problem, namely the Criminal Code, Law Number 7 of 1974 concerning Controlling Gambling, Law Number 10 of 1998 concerning Banking and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, as well as other laws and regulations relating to crimes or crimes and online gambling, based on and supported by legal principles or principles, doctrines or theories of legal science.

Apart from the normative juridical research method, this research also used the Empirical Juridical research method, namely research carried out by looking directly at the facts and data relating to the problem of preventing criminal acts of online gambling by banking institutions, by conducting observations and interviews with relevant respondents. directly related to what is being researched.

3. Results And Discussion

A. The Role of Banking in Preventing Online Gambling Crimes

The use of telecommunication, information and communication (telematics) technology via internet networks today is not only used as a means of seeking information, communicating and interacting between fellow humans through various kinds of networks or social media applications (social media) such as Facebook, Twitter, Instagram, etc. telegram and so on. However, advances in telematics through the use of the internet are also used as a means of creating criminal acts or crimes in virtual space or cyberspace, known as computer crime, cyber crime, cyber space crime, with various shapes and types. One of them is "online gambling" or "online gambling", such as online poker, black jack, slot machines, lottery (white coupons, lottery), up to the games ludo, dominoes, halma using applications or information systems and electronic transactions using money as a bet.⁵

Therefore, gambling in any form is prohibited by law in Indonesia, and is categorized as a criminal act of gambling as regulated in Article 303 of the Criminal Code, as well as the provisions of Article 45 paragraph (2) along with Article 27 paragraph (2) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU

⁵ Sulisty H., & Ardjayeng L. (2020). Tinjauan Yuridis Tentang Perjudian Online Ditinjau Dari Undang-Undang No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Dinamika Hukum & Masyarakat*, 1(1)

ITE).

The provisions of this article are legal rules that are used as the basis for eradicating criminal acts of online gambling in Indonesia (*lex specialist de lege generalis*). However, in practice, there seems to be no end to eradicating criminal acts of online gambling. For this reason, various efforts are needed by the relevant agencies to prevent and deal with criminal acts of online gambling, including the Ministry and/or Communication and Informatics Service, the National Police of the Republic of Indonesia, including banking institutions.⁶

Banking as the largest financial institution in Indonesia certainly has a strategic role in preventing online gambling crimes. Banking institutions as intermediary institutions and institutions of public trust in saving and managing their finances are guided by the principle of prudence. The application of the principle of prudence in the banking world is intended to maintain the trust of the public who save funds and create healthy banking. One way to implement the precautionary principle is to apply the know your customer principle, which is also known as the "know your customer principle". Implementing the principle of knowing your customer is considered important as a way to protect the health of the bank.

The Know Your Customer Principle requires banking institutions to monitor customer transaction activities and report suspicious transactions. This principle needs to be considered by banking institutions to minimize various risks, such as operational risk, legal risk, concentration risk and reputational risk. In addition, by applying this principle, it is hoped that banks will not only know customers literally, but can get to know them more comprehensively, not only knowing the customer's identity but also regarding the profile and character of customer transactions, which are carried out through banking services. This includes transactions related to online gambling.

Based on research data obtained by the author at the Jayapura City Communication and Information Office, the results showed that from 2018 to August 2022, Kominfo has cut off access to 566,332 content in digital spaces that contain elements of gambling, digital platforms and sites that share related content. online gambling activities, with details of handling per year can be seen in table 1 below:

⁶ HS Manalu, (2019), *Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online*.

Jurnal of Education, Humaniora and Social Sciences (JEHSS). 2, (2), 428-446.

Table : 1
Number of Digital Content / Online Gambling Sites Taken Down
(disconnected) 2018 – August 2022

No	Year	Number of Digital Content / Sites / Online Gambling Applications Taken Down (Disconnected)
1	2018	84.484 Digital Content/App/Site
2	2019	78.306 Digital Content/App/Site
3	2020	80.305 Digital Content/App/Site
4	2021	204.917 Digital Content/App/Site
5	August 2022	118.320 Digital Content/App/Site
Total		566.332 Digital Content/App/Site

From table 1 above, it is clear how much content, applications and online gambling sites have been removed by the Indonesian Ministry of Communication and Information because they are illegal content and violate positive law in Indonesia.

Removal of unregistered content can be done in two ways. First, Kominfo can decide on the content on a site. Second, Kominfo can terminate the domain name of a site that violates specified regulations. Apart from that, access termination can also be done through third parties in terms of content on platforms, for example social media in the form of accounts, narratives or content related to products in the marketplace. For this reason, Kominfo can do this by collaborating with social media platforms. In the technical aspects of this cooperation, Kominfo, through special communication facilities, asks social media platforms to immediately handle accounts/content that are deemed to violate statutory regulations, especially online gambling crimes.

However, during the last five years the Papua Regional Police through the Directorate of Special Crimes, Subdit V Cyber have only succeeded in handling 1 online gambling case and that has been happening since 2017. From 2018 to 2021 there was not a single online gambling case handled. by the Papuan Police. This can be proven from the results of research conducted by the author at the Papua Police Cyber Sub-Directorate V.⁷

Based on data obtained by the author from the Directorate of Special Crimes, Sub-Directorate V for Cyber, Papua Police, between 2017 and 2021, there was only one online gambling criminal case handled by the Papua Police Cyber sector. Where handling and/or examination of online gambling cases is carried out on the basis of:

⁷ Maria Margareta, dkk. 2014. Kebijakan Kriminal Dalam Penanggulangan Tindak Pidana Judi Online Yang Dilakukan Markas Besar Kepolisian Republik Indonesia (Mabes POLRI). *USU Law Journal*, 2(2), 187-188.

1. Police Report Number: PL/38/III/2017/SKPT Polda Papua, dated 16 March 2017;
2. Investigation Order Number: Sp.Sidik/69/III/2017, dated March 18 2017;
3. Order to Commence Investigation Number: SPDP/III/2017 Ditreskrimsus, dated March 23 2017.

One effort to prevent criminal acts of online gambling can be done through implementing the roles and functions of banking institutions. Because the practice of online gambling cannot be separated from transactions that use the services of banking institutions, as for example the criminal case of online lottery gambling which was handled by Subdit V Cyber Polda Papua, the evidence confiscated, both accounts and ATMs and proof of transfers, involved almost all institutions. banks operating in Papua.

As bank products, activities and information technology develop increasingly complex, opportunities for irresponsible parties to use banking institutions' products or services to assist criminal acts in the form of money laundering from the proceeds of crime or online gambling crimes can be minimized. and banking institutions in carrying out their business can avoid various risks as mentioned above.

Within the above framework, Bank Indonesia in 2012 issued Bank Indonesia Regulation Number: 14/27/PBI/2012 concerning Guidelines for Anti-Money Laundering and Preventing Funding for Terrorist Activities for Commercial Banks. With the enactment of Bank Indonesia Regulation Number: 14/27/PBI/2012, the term know your customer principle has been changed to the term customer due diligence (CDD), namely activities in the form of identification, verification and monitoring carried out by the Bank to ensure that the transaction is in accordance with the profile. prospective customers, customers and Walk In Customers.

Since the establishment of the Financial Services Authority (OJK) by the Indonesian government Law Number: 21 of 2011, the function of regulating and supervising financial institutions, which at that time was under the authority of Bank Indonesia, was delegated to the duties and functions of the OJK. Therefore, within the framework of supervision and regulation of financial institutions and services (banks and non-banks), regarding the implementation of the principle of customer due diligence, the OJK issued OJK Regulation Number: 12/POJK.01/2017 concerning the Implementation of the Anti-Money Laundering Program and Prevention of Terrorism Financing in the Financial Services Sector.

The Financial Services Authority regulations mentioned above require every financial institution to apply the principles of Customer Due Care in its

business activities, namely:

1. Establish business relationships with prospective customers;
2. There are financial transactions in rupiah and/or foreign currency whose value is at least or equivalent to IDR 100,000,000.00 (one hundred million Rupiah);
3. There are Fund Transfer transactions as intended in OJK Regulations regarding the Implementation of Anti-Money Laundering Programs and Prevention of Terrorism Financing in the Financial Services Sector;
4. There are indications of Suspicious Financial Transactions related to Money Laundering and/or Terrorism Financing; or
5. PJK doubts the veracity of the information provided by prospective customers, customers, proxy recipients and/or beneficial owners.

Apart from that, identifying potential customers or customers through requests for data and information which at least includes:

1. Self-Identity. PJK will submit a request for personal identity information of potential individual customers which includes their full name including aliases (if any), identity document number, residential address according to the identity document and other residential addresses (if any), place and date of birth, nationality, occupation, gender, marital status. If the prospective customer is already working, he must complete data in the form of employment information, office address and telephone number where he works. In this case, as a prospective customer, you will be asked to attach documents such as personal identity card (KTP/SIM/Passport), NPWP, and attach a signature specimen.
2. Identity of the Beneficial Owner, if any. If there is another party who is the beneficial owner of the financial product that you are proposing, then the prospective customer must attach data from the beneficial owner.
3. Information on sources of funds and average annual income. In this case, you will be asked to write down the source of funds and income per year, for example funds come from work, business, or gifts from parents.
4. The aims and objectives of the business relationship or transaction that the prospective customer will carry out.

The implementation of Customer Due Diligence is expected to reduce the risk of being used as a means of money laundering, including money from

gambling. With information obtained through the Customer Due Diligence process, Banking Institutions can identify transactions that are considered suspicious, such as financial transactions that do not match the customer's profile, and financial transaction traffic whose source is suspected to be assets resulting from criminal acts.

The following are several parameters used in assessing fraudulent transactions, the source of which is assets resulting from criminal acts through the services of banking financial institutions in Indonesia.

Table: 2
Parameters of Suspicious Transactions from Criminal Proceeds

No	Skenario	Parameter
1	Judi Online	1. Frekuensi Kredit > 100, dalam satu bulan dan transaksi tidak bulat (2 digit terakhir ber-kode unik 1-99). 2. Nominal transaksi Kredit/Debit > 100 juta (dlm 1 bulan) dengan selisih kredit dan debit kurang dari 20jt. 3. User menerima transaksi dari > 20 cabang berbeda.
2	Narkoba - CMS	1. Tidak sesuai profil, nasabah individu dengan profil minimal mengelola dana untuk individu diatas 500 juta dan badan usaha diatas 1 M. 2. Frekuensi kredit 50 <x<100 dalam satu bulan. 3. Melaksanakan transaksi CMS (Uker CMS 00397) transaksi > 1 M dalam jangka waktu 1 bulan.
3	Narkoba - Remark	1. Tidak sesuai profil, nasabah individu dengan profil minimal mengelola dana untuk individu diatas 500 juta dan badan usaha diatas 1 M. 2. Frekuensi kredit 50 <x<100 dalam satu bulan. 3. Transaksi yang mengandung remaks atau kata-kata sebagai berikut: bong, insul, spidol, kertim, amplop, BB, afo, cimeng, gelek, ikan, bedak, atep putih, tepung, boat, boti, lexo, kuncian, nipam, dum, coke, junkies, bd, birong, bokul, jokul, tu, selinting, baw, stengky, setangki, sesut, relaps, papir, sprempi, pokemon, anjing.
4	Korupsi - General	1. Tidak sesuai profil, nasabah individu dengan profil minimal mengelola dana untuk individu diatas 500 juta dan badan usaha diatas 1 M. 2. Transaksi CTR. 3. Kenaikan saldo > 50 juta setelah pembukaan rekening.
5	Korupsi - Kartu Kredit	1. Tidak sesuai profil, nasabah individu dengan profil minimal mengelola dana untuk individu diatas 500 juta dan badan usaha diatas 1 M. 2. Nasabah flag PEP. 3. Nominal total transaksi debit dan credit > 1 M. 4. Membayar kartu kredit > 50jt, berdasarkan transcode kartu kredit (check payment, non direct payment, cash payment, dan retail payment). 5. Kartu kredit bersaldo kredit (2x lipat dari plafond).
6	Korupsi- Pinjaman	1. Tidak sesuai profil, nasabah individu dengan profil minimal mengelola dana untuk individu diatas 500 juta dan badan usaha diatas 1 M. 2. Nominal total transaksi debit dan credit > 1 M. 3. Membayar pinjaman bukan namanya (berbeda CIF debit simpanan kredit pinjaman). 4. Pelunasan maju pinjaman < 6 bulan. 5. Pinjaman bersaldo kredit > 1M.
7	Korupsi - Valas	1. Nasabah flag PEP. 2. Transaksi valas > 100.000 USD.
8	Terorisme	1. Transaksi IFTI kenegara-negara red flag (afganistan, iraq, syria, somalia, yemen, pakistan, filipina). 2. Yayasan yang menerima donasi > 100 juta. 3. Lokasi transaksi kartu di luar negeri dan zona negara high risk. 4. Masuk ke dalam list DTTOT.
9	Perpajakan	1. Tidak sesuai profil, nasabah individu dengan profil minimal mengelola dana untuk individu diatas 500 juta dan badan usaha diatas 1 M. 2. Transaksi CTR, frekuensi transaksi > 5 dalam 1 bulan.
10	Pinjaman	1. Pelunasan maju pinjaman < 6 bulan. 2. Pinjaman bersaldo kredit > 1M.
11	Kustodian	Nominal rekening giro escrow nasabah yang meningkat tajam (signifikan), individu nominal > Milyar masuk ke rekening giro escrow, non individu nominal > Milyar.
12	Kartu Kredit- Merchant	1. Frekuensi merchant kartu kredit yang transaksi kredit > 100 (Bulanan dan Dikecualikan untuk yang Patnership Ecommerce). 2. Pinjaman bersaldo kredit untuk kartu kredit > 20 juta.

The table above provides an overview of the measures or parameters that can be used by financial institutions, especially banking institutions, to prevent criminal practices, especially online gambling at number one.

Data from research results that the author obtained from the Supervision and Audit section of Bank Rakyat Indonesia Jayapura Branch, there was one suspicious transaction related to online gambling crimes from January to March 2019, by one of the BRILink agents who used the EDC (Electronic Data Capture)

B. Factors That Become Obstacles for Banks in Implementing Actions to Prevent Online Gambling Crimes

The negative impact of gambling is a real threat to social norms so that it affects the continuity of social life, gambling games can create dependency and cause material and non-material losses not only for the players but also for their families, gambling can cause household destruction, and can encouraging perpetrators to commit crimes or other criminal acts, for example, stealing, robbing, and other acts of violence.

Therefore, gambling, both conventional and online, in the context of criminal law is a criminal act, because it is an act that is prohibited, threatened with sanctions and/or punishment in criminal law regulations, both in general as regulated in the provisions of the Code of Law. Criminal Code (KUHP), Law Number: 7 of 1974 concerning Controlling Gambling, as well as specifically regarding Online Gambling in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2001 concerning Information and Electronic Transactions.⁸

Even though this gambling game has been prohibited or is an act that is categorized as a criminal act, as regulated in the legal regulations mentioned above, it still exists in people's lives, even with the development of communication and information technology, contemporary types of gambling games have emerged in virtual spaces, known as online gambling games.

Therefore, questions arise in society as to why or what factors cause gambling and/or online gambling to be difficult to prevent, overcome and eradicate by law enforcement officials in Indonesia. To answer this question, of course we have to look again at the practice or empirical life of society, so that at least we know what factors are obstacles in prevention and control of gambling games, and if this is related to the title of the research that the author has adopted, it is worth asking what factors hinder banking institutions from preventing the occurrence of criminal acts of online gambling in society.

In general, based on the author's observations, the factors that hinder and/or become obstacles in terms of preventing and overcoming gambling in society are greatly influenced by several general factors, namely the hedonistic lifestyle, socio-economic factors of society (employment, high levels of poverty), community behavior. who want to seek instant and quick profits from their wealth without going through a process, even this gambling game is often linked to the habits,

⁸ Maskun. 2013. *Kejahatan Siber (Cyber Crime)*: Suatu Pengantar. Jakarta: Kencana.

customs or culture of Indonesian society and what is most problematic is law enforcement.

From the literature study that the author obtained, according to Johanes Papu in his article entitled Gambling Behavior, there are factors that greatly influence a person's life when playing gambling, namely what is known as a pathological gambler, namely a person's ability to escape from the urge to gamble.⁹ They are very obsessed with gambling and there is a continuous increase in the frequency of gambling and the number of bets without being able to consider the negative consequences caused by this behavior, both on themselves, their families, careers, social relationships and the surrounding environment. The criteria that can be classified as a pathological gambler according to the DSM-IVScreen (a tool used to measure the level of gambler) are if the individual has more than five factors, including:

- a. Preoccupation, obsession with gambling (e.g. obsession with repeating past gambling experiences, difficulty diverting attention to things other than gambling or specifically thinking about ways to earn money through gambling)
- b. Tolerance, the need to gamble with a tendency to increase money (bet) in order to achieve a desired pleasure or satisfaction.
- c. Withdrawal, becoming easily restless and irritable every time you try to gamble.
- d. Escape, using gambling as a way to escape from various life problems or unpleasant feelings (for example, guilt, helplessness, anxiety, depression or sadness)
- e. Chassing, after losing at gambling, tends to return to gambling again to chase wins in order to break even.
- f. Lying, lying to family members, counselors or others about one's involvement in gambling.
- g. Loss of Control, always failing in efforts to control, reduce or stop gambling behavior.
- h. Risked Significant Relationship, endangering or causing friendship relationships with people who play a big role in life, loss of job, dropping out of school or breaking up the family or losing career opportunities.
- i. Bailout, controlling other people to give money to themselves or their families in order to reduce the financial burden caused by gambling.

⁹ Johanes Papu, Prilaku Berjudi, lihat <https://www.e-psikologi.com/sosial.asp>, 20 September 2023.

Looking at the impact and factors that trigger it as well as the obstacles faced by the government, it is necessary to make more intensive efforts by all Indonesian people. In particular, the role of financial institutions in this case is banking institutions. Because in reality, the practice of online gambling games will always use banking products and services in carrying out financial transactions.

1. Bank Secrecy Settings.

Banks are trusted financial institutions (trust banks). It is said this because customers trust the bank as a place to store and manage their money. As a form of bank appreciation for customers, the bank will provide the best service, use and manage customer money as best as possible and safeguard all data and information related to its customers. Considering the importance of customer data/information and their savings, in Law no. 10 of 1998 concerning Banking, this is clearly regulated in Chapter VII concerning Bank Secrecy. Article 40 of the Banking Law states that 'banks are obliged to keep confidential information about deposit customers and their deposits except in cases as intended in Article 41, Article 41A, Article 42, Article 44 and Article 44A. In line with provisions regarding bank secrecy, the Financial Services Authority (OJK) also issued Circular Letter No. 14/SEOJK.07/2014 concerning Confidentiality and Security of Consumer Data and/or Personal Information.

This circular letter was issued in connection with the implementation of Financial Services Authority Regulation no. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. In principle, the OJK and POJK Circulars above regulate that Financial Services Business Actors (PUJK), including banks, are obliged to protect consumers' personal data and/or information and prohibit in any way providing such consumers' personal data and/or information to third parties.

Below we will briefly explain several conditions under which banks are required to disclose customer data:

First, for tax purposes. For this purpose, banks are required to provide written information and evidence as well as letters regarding the financial condition of certain depositors to tax officials. This can be done based on a written order from the Financial Services Authority - OJK, to the bank based on a request from the Minister of Finance. With the enactment of Law Number 9 of 2017 concerning Stipulation of Regulations in Lieu of Law Number 1 of 2017 concerning Access to Financial Information for Tax Purposes into Law, to make it easier for tax authorities to receive and obtain customer financial information for tax purposes without going through procedures in accordance with stipulated in Article 41 of the Banking Law.

Second, for the purposes of settling bank receivables which have been submitted to the State Receivables and Auctions Agency/State Receivables Affairs Committee. The process is, the Head of the State Receivables and

Auctions Agency/State Receivables Affairs Committee submits a written request to the Financial Services Authority Bank - OJK, to obtain information from the bank regarding debtor customer deposits. The permit application is accompanied by the name and position of the official of the State Receivables and Auctions Agency/State Receivables Affairs Committee. Then, OJK will provide permission in writing.

Third, for purposes in criminal cases. In the context of criminal law purposes, the police, prosecutors and judges can obtain information from the bank regarding the suspect's or defendant's deposits with the bank. Similar to the process above, the police, prosecutors and judges must apply for permission in writing to the OJK, stating their name and position clearly. Based on this letter, OJK will issue a permit.

Fourth, in civil cases between banks and their customers. In this case, bank directors can provide information to the Court about the financial condition of the customer concerned and other information relevant to the case without requiring permission from the OJK.

Fifth, related to the exchange of information between banks. Based on the explanation of Article 44 of the Banking Law, the exchange of information between banks is permitted with the aim of "facilitating and securing bank business activities, among other things to prevent duplicate credit and to know the condition and status of another bank." "In this way, banks can assess the level of risk they face before carrying out a transaction with a customer or with another bank."

Sixth, at the request, approval or power of attorney from the Saving Customer made in writing and at the request of the legal heirs of the saving customer who has died. In this case, the bank is obliged to provide information regarding the customer's savings. Further regulations regarding the disclosure of confidential customer data are further regulated in PBI No. 2/19/2000 concerning Requirements and Procedures for Giving Written Orders or Permission to Reveal Bank Secrets.

Based on the explanation above, it can be stated that banks are, in principle, institutions of trust, obliged to maintain the trust of their customers by keeping confidential all information relating to customers and their deposits with the bank. However, under certain conditions as explained above, banks are permitted to provide information regarding data on customer depositors and their deposits in accordance with the regulated mechanisms.

The problem is, when it comes to the role of banking institutions in preventing criminal acts of online gambling, the provisions regulated in both the Banking Law and OJK Regulations, the role of banking institutions is only passive, where to disclose banking secrets is only based on request, it is not

an obligation and/or the obligation for banking institutions to actively disclose bank secrets regarding their customers' financial transactions.

In other words, even though the principle of knowing the customer and/or Customer Due Diligence has been implemented, based on the bank's internal analysis, suspicious transactions were found. Banking institutions will not immediately report the case to the police, considering the various risks that will be faced, as for example cases of misuse of BRILink products used by customers for online gambling transactions.

2. Technological Development Factors and Electronic Transactions.

Factors in the development of communication and information technology generally have two impacts on human life, namely negative and positive impacts. Likewise with the practice of banking institutions in Indonesia, with the emergence of various applications and electronic transactions, which has greatly influenced the application of the Customer Due Diligence principle, which was initially carried out face to face, so that between customer service and prospective customers or clients and walk in see and Affiliated parties can meet directly.

The positive impact felt by banking institutions in the application of technology and electronic transactions aims not only to facilitate internal banking operations, but also to further facilitate service to customers or customers and clients. Moreover, currently, in the banking world, almost all products offered to customers are similar, so the competition that occurs in the banking world is how to provide products that are easy and fast, which is very much determined by the technology used and applied.

This is a demand for banks because like it or not, banking institutions that have a wide scope of work plus a lot of operations must be supported by technology to facilitate, streamline and make this performance more effective. Moreover, in the banking world, up to date information is needed for middle and upper management to predict business steps that will be taken so that various obstacles that may arise can be overcome.

Apart from that, real time operations between banks have also become a demand for the banking world, because this is one of the materials for services that compete in marketing banking products. Sending money between bank transfers, Automated Teller Machine (ATM) outlets, Point of Sales (POS), Electronic Fund Transfers (EFT), Electronic Data Capture (EDC), various types of credit cards, clearing automation, online banking, making the system easier financial reporting, becomes a benchmark for assessment for customers in general when carrying out transactions in terms of service.¹⁰

¹⁰ Shilvia Amanda. 2022. Penegakan Hukum Terhadap Praktik Money Game dengan Skema Ponzi dalam Investasi Ilegal Tiktok E-Cash di Indonesia. *Res Nullius Law Journal*. 4(1), 64-65.

Thus, like it or not, the banking business must be supported by operational efficiency if it wants to compete in the world, and this must be supported by an integrated system contained in information technology. Apart from the positive impacts mentioned above, there are also negative impacts, including the risk faced by banks of hacking into the banking system, banks have to incur additional costs in using an application system which will experience changes from time to time, besides that, another negative impact is with people. - people who are not responsible for carrying out transactions that do not match their personal profile as well as transactions resulting from criminal acts, or money laundering, including online gambling proceeds.

3. Setting the Nominal Amount in Implementing the Principles of Customer Due Diligence.

The implementation of Customer Due Diligence is expected to reduce the risk of misuse of banking institution products and facilities, especially fraudulent transactions involving the proceeds of criminal acts. With information obtained through the Customer Due Diligence process, Banking Institutions can identify transactions that are considered suspicious, such as: financial transactions that do not match the customer's profile, and financial transaction traffic whose source is suspected to be assets resulting from criminal acts.

Bank Rakyat Indonesia actually has a system as mandated in the Financial Services Authority Regulation Number: 12/POJK.01/2017 concerning the Implementation of Anti-Money Laundering and Terrorism Financing Prevention Programs in the Financial Services Sector. However, regarding the implementation procedure, it is only carried out on transactions in rupiah and/or foreign currency whose value is at least or equivalent to IDR 100,000,000 (one hundred million rupiah)

With settings like the above, it will be difficult for banking institutions to detect transaction values with a value below one hundred million rupiah. Although in the explanation of article 15 it is stated that what is meant by "financial transactions in rupiah and/or foreign currency whose value is at least or equivalent to IDR 100,000,000.00 (one hundred million rupiah)", includes transactions carried out in one transaction. or carried out in several transactions that are reasonably suspected to be related to each other.

The regulation of the article above, in itself, opens up opportunities for irresponsible people to practice criminal acts of online gambling, by opening more than one bank account and using the names of different people.

4. . Conclusion

Based on the descriptions in the previous chapters, as well as the research data obtained, the conclusions that can be put forward in this writing are in practice, the role of banking in preventing criminal acts of online gambling has not been carried out as the aim and objective of implementing the know your customer principle and/or the principle of Customer Due Deligence, as well as the principle of Exchange Due Deligence. As a result of the lack of clarity in legal regulations which place banking institutions in a passive position in disclosing bank secrets, as regulated in Law Number 10 of 1998 concerning Banking and Financial Services Authority Regulation Number: 12/POJK.01/2017 concerning Implementation of the Anti-Money Laundering Program and Prevention of Terrorism Financing in the Financial Services Sector.

Factors that become obstacles to implementing the banking role in preventing criminal acts of online gambling consist of three factors, namely the first is bank secrecy, the second is the development of technology and electronic transactions, and the third is the determination of the nominal amount or transaction value as regulated in the Financial Services Authority Regulations. Number: 12/POJK.01/2017

References

Buku:

- Budi Suhariyanto. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime)*. Raja Grafindo Persada.
- Edmon Makarim, (2005). *Kompilasi Hukum Telematika*, PT Raja Grafindo Persada, Jakarta.
- Maskun. (2013). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana.

Artikel Jurnal:

- HS Manalu, (2019), Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. *Jurnal of Education, Humaniora and Social Sciences (JEHSS)*. 2, (2), 428-446.
- Maria Margareta, dkk. 2014. Kebijakan Kriminal Dalam Penanggulangan Tindak Pidana Judi Online Yang Dilakukan Markas Besar Kepolisian Republik Indonesia (Mabes POLRI). *USU Law Journal*, 2(2), 187-188.
- Shilvia Amanda. 2022. Penegakan Hukum Terhadap Praktik Money Game dengan Skema Ponzi dalam Investasi Ilegal Tiktok E-Cash di Indonesia. *Res Nullius Law Journal*. 4(1), 64-65.
- Sulistyo H., & Ardjayeng L. (2020). Tinjauan Yuridis Tentang Perjudian Online Ditinjau Dari Undang-Undang No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Dinamika Hukum & Masyarakat*, 1(1)

Website:

Johanes Papu, *Prilaku Berjudi*, lihat <https://www.e-psikologi.com/sosial.asp>, 20 September 2023.

<https://www.todayline.me/id/v2/article/I217r3> Game Judi Online Paling Marak di Androit, Iseng Berhadiah. Diakses 07 April 2024.

Telusuri Judi Online, Polri temukan 360 situs dan 460 rekening Bank, lihat <https://www.nasional.kompas.com/read/11310001/> diakses 07 April 2024.