East Asian Journal of Multidisciplinary Research (EAJMR)
Vol. 2, No. 7, 2023: 2895-2906

The Urgency of Reforming Regulations for Money Laundering in the Digital Era

Mashuril Anwar
Program Studi Hukum Bisnis Institut Informatika dan Bisnis Darmajaya
Corresponding Author: Mashuril Anwar mashuril@darmajaya.ac.id

A R T I C L E I N F O

Keywords: The Digital Era, Regulation Renewal, Cyber Laundering

Received : 20, May
Revised : 15, June
Accepted: 16, July

A B S T R A C T

This article aims to examine the politics of criminal law in dealing with cyber-based money laundering and the urgency of updating regulations to combat money laundering in the digital era. The type of research used in writing this article is normative with a statutory approach. The collection of legal materials in this study was also supported by literature studies and analyzed qualitatively and deductively. Based on the discussion, at the normative level, it is still partial and has not been specifically regulated. Currently, cyber laundering crimes are only accommodated by several separate legal regimes that have not been able to reach the perpetrators of cyber laundering crimes. Countermeasures against money laundering in the digital era, like cyber laundering, are still governed by conventional regulations. Therefore, it is urgent to update regulations on dealing with cyber laundering crimes that can accommodate the complexity of the problem.

DOI: https://doi.org/10.55927/eajmr.v2i7.5009
ISSN-E: 2828-1517
https://journal.formosapublisher.org/index.php/eajmr

INTRODUCTION

The digital era is like a double-edged sword; one side allows humans to make transactions in a sophisticated, easy and fast way. Then on the other hand, the digital era also has contributed to the development of crime. One of the impacts of digitalization is the development of a modus operandi for money laundering. The criminal act of money laundering is an act of hiding or disguising the origin of the money obtained from the proceeds of the crime (Harahap, 2020). The main offense was "hiding and disguising the proceeds of crime as stipulated in Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (from now on referred to as the TPPU Law). Money laundering is not a crime that stands alone but rather a continuation of previous crimes, including corruption, narcotics trafficking, illegal arms trade, trafficking in persons, etc (Sari, 2022).

The crime of money laundering is carried out in various stages, including placement, layering and integration. Placement is the conversion of proceeds from crime into securities or transfers and exchanges into foreign currency. Layering is a transaction made to make it difficult to trace the proceeds of crime. Integration is the stage of merging the proceeds of crime with lawful money so that it appears as if the proceeds of crime appear legal (Nuryanto, 2019).

The modus operandi of money laundering in the digital era is increasingly complex and complicated because it uses cyber media in conducting financial transactions. Cybermedia allows financial transactions to be done easily and quickly anytime and anywhere. Money laundering in the digital era is carried out using various cyber media, including e-commerce, e-banking, online gambling, online games and other cyber means so that conventional money laundering shifts to contemporary money laundering called cyber laundering.

Cyber laundering through e-commerce is increasingly open, along with the increasing popularity of e-commerce on various Indonesian digital platforms. Using e-commerce, financial transactions can be carried out via e-money and e-cash (digital cash), making tracking difficult. According to the records of the Central Bank of the UAE, the limitations due to the lockdown during the Covid-19 pandemic caused the use of e-commerce as a means of money laundering to increase (Sidik, 2021). The modus operandi of cyber laundering through e-commerce includes the perpetrator selling goods or services on the marketplace and then the perpetrator combining the proceeds of crime with the proceeds of the sale so that the proceeds of crime appear legal. In addition, e-commerce can also be used as a means of money laundering by selling illicit, illegal and pirated goods under disguise and transferring illicit money to other accounts to be withdrawn by taking a commission on the transaction (Indiraphasa, 2021). Another modus operandi can occur through the purchase of goods or services of high value in e-commerce, but there is no delivery of goods but only for the transfer of money (Iskandar, 2022).

Cyber laundering can also be done through e-banking, where financial transactions can be done online without coming to the bank. The modus

operandi of cyber laundering through e-banking includes perpetrators taking over other people's accounts and then using these accounts to practice buying and selling crime syndicates (Sidik, 2021). Another modus operandi of cyber laundering is through the use of smart cards. Through peer-to-peer payment systems and e-banking, criminals can move e-money from one card to another in the possession of others in conspiracy with the perpetrators (Leslie, 2010).

Online gambling has also become the modus operandi of cyber laundering with two main scenarios. First, perpetrators or cyber launderers can exploit very legitimate web-based online gambling services for laundering purposes or can create online gambling services to clean "dirty money (Bumeter, 2001)." The second scenario involves the establishment of an online casino, the modus operandi that is generally practiced (Leslie, 2010). According to the Financial Transaction Reports and Analysis Center (PPATK) records, money laundering resulting from online gambling has reached Rp. 57 Trillion in 2021 and Rp. 81 Trillion in 2022 (Merdeka, 2022). Unfortunately, the TPPU Law does not regulate the relationship between money laundering and online gambling (Alda Satrya, 2022).

The next modus operandi of cyber laundering is through online games. Transactions in online games are carried out by transferring several funds to buy various items known as RMT Real Money Trading). This activity can be found in the online games Mobile Legend, RF, Dragon Nest and Mobile Legend. Through online games, money launderers divert money from the proceeds of crime by buying RMT and receiving money that can be easily withdrawn (Artha, 2019).

Money laundering through cyber media or cyber laundering has occurred in Indonesia through Bitcoin transactions. Since 2015, efforts have been detected to hide proceeds of crime through Bitcoin transactions in Indonesia. Then the findings of the Attorney General's Office showed that the three suspects in the PT. Asabri hid the proceeds of its corruption in bitcoins. Not only corruption cyber laundering also occurs in cases of financing terrorism and narcotics activities (Aditya, 2021).

Regulations related to preventing and eradicating money laundering as per the TPPU Law have yet to accommodate the development of money laundering in the global era or cyber laundering. The TPPU Law does not specifically regulate cyber laundering. The TPPU Law can only prosecute conventional money laundering actors. In addition, developing the modus operandi of money laundering through cyber media poses its challenges. Law enforcement against cyber laundering actors requires the readiness of law enforcement officials, law enforcement jurisdiction, international cooperation, and infrastructure. Law enforcement against cyber laundering requires expertise in the fields of computers, banking and needs to involve multi-agency collaboration and even international cooperation.

As technology develops, the modus operandi of money laundering through cyber media will become increasingly complex. Indonesia does have legal instruments to deal with money laundering crimes. However, this legal instrument was born long before digitization, so it has yet to follow the

development of the modus operandi of money laundering. The absence of any TPPU Law updates has created law enforcement complications. Therefore, existing regulations need to be updated to accommodate the development of money laundering crimes through cyber media or cyber laundering. Therefore, the problems analyzed in this article include the politics of criminal law in dealing with cyber-based money laundering. And what is the urgency of updating regulations on money laundering in the digital era?

THEORETICAL REVIEW

In general, there is no universally agreed definition of money laundering (Garnasih, 2015). This occurs because each country has a different approach to viewing money laundering as a crime, resulting in different classifications in considering the criminalization of money laundering, including the qualifications of predicate crimes. Pamela H. Bucy defines money laundering as concealing the existence of something originating from an illegal source so that the funds appear to have come from a legitimate source (Sutedi, 2008).

According to Romli Atmasasmita, there is a very close correlation between predicate crimes and money laundering crimes, but that does not mean they have similarities in malicious intent or mens rea. This is because there is a difference between the intention to commit predicate crimes that are manifested in their actions and the will to commit money laundering as stipulated in Article 3, Article 4 and Article 5 of the TPPU Law so that it can be concluded that ML is not included in continuing criminal acts (Atmasasmita, 2016). Based on the several definitions of money laundering presented previously, at least there is a fundamental element of money laundering, namely the predicate of crime, which is the background to the emergence of money laundering (proceeds of crimes) (Garnasih, 2015).

Article 1 point 1 of the TPPU Law states that "money laundering is any act that fulfills the elements of a criminal act in accordance with the provisions of this law." The elements of the crime referred to in Article 1 point 1 of the TPPU Law are further regulated in Article 3, Article 4 and Article 5 of the TPPU Law. According to Hanafi Amrani, in examining the elements of the article in Article 3, Article 4 and Article 5, it uses "known or reasonably suspected" as mens rea. This is a form of anticipation of developments and, at the same time, a shift in the meaning of men's rea from actual knowledge to constructive knowledge, where money laundering can be carried out when the perpetrator knows or reasonably suspects that the assets in question originate from certain crimes which in criminal law is known as property. dolus proparte culpa (Amrani, 2015).

In the current era of technology and information, money laundering behavior is increasingly complex and difficult to track because perpetrators use cyberspace to carry out financial transactions without coming to the bank but simply use e-banking facilities and other cyber facilities. Cyber laundering was coined as a result of the ease that these digital financial instruments offer and how they affect money laundering offences (TPPU).

Cyber laundering is essentially the penetration of technology (cyber) which manifests as a means of crime. In particular, this cybercrime is exploited to carry out money laundering activities. Cyber laundering is also widely referred to as electronic money laundering, which today refers to the development of digitalization related to the emergence of digital assets, cryptocurrencies, virtual currencies, financial technology and several other things specifically intended to carry out money laundering activities (Irina, 2018).

Cyber laundering utilizes online financial services and media available on the Internet that use virtual money. Money laundering via the Internet is believed to be the newest and most up-to-date technique in money laundering methods (Reuter, 2006). With cyber laundering, the money laundering process becomes faster. Because of the anonymity that exists, the lack of physical contact, the speed of transactions, and the wider coverage in Indonesia, it is more likely that many perpetrators will switch from traditional money laundering to cyber laundering given the state of the Internet which is still not fulfilled by the rule of law. services offered online (Filipkowski, 2008).

METHODOLOGY

To answer research problems, normative/dogmatic research methods are used. This means that this research examined the laws and regulations in money laundering about developing the modus operandi of money laundering in the current digital era. Apart from that, the collection of legal material in this study was also supported by a literature study analyzing some of the relevant literature. The legal material obtained is then classified and analyzed qualitatively deductively so that the current regulation on countering money laundering and the urgency of its reform are known.

RESULTS AND DISCUSSION

1. The Politics of Criminal Law in Combating Cyber-Based Money Laundering Crimes

Criminal law politics, also known as "criminal law policy," is a policy to determine the formulation and implementation of criminal provisions per the objectives to be achieved (Bunga, 2019). Political enforcement of criminal law generally includes three stages, namely the formulation stage, the application stage and the execution stage. The formulation stage is enforcing criminal law in abstracto by the legislature. At this stage, the legislature formulates criminal laws and regulations by current and future needs.

In connection with the prevention of cyber-based money laundering, at the formulation level, it has been regulated in several legal instruments, among others, "Law Number 15 of 2002 *jo.* Law Number 25 of 2003, which was revoked by Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (from now on referred to as the TPPU Law), Law Number 11 of 2008 concerning Information and Electronic Transactions as amended with Law Number 19 of 2016 (from now on referred to as the ITE Law) and Law Number 1 of 2023 concerning the Criminal Code (from now on referred to as the National Criminal Code)".

According to the TPPU Law, money laundering is generally categorized into two types: active money laundering, regulated in Article 3 and Article 4, and passive money laundering, regulated in Article 5, paragraph (1) (Sudarti, 2021). Active money laundering actors are parties to money laundering and perpetrators of predicate crimes, while passive money laundering perpetrators are parties who enjoy the results or benefits of money laundering and disguise the origin of wealth (P.P., 2019). The TPPU Law adheres to a unique maximum sentence system. The threat of imprisonment for perpetrators of active money laundering crimes is 20 years and a fine of Rp. 5 Billion to Rp. 10 billion.

Furthermore, the politics of criminal law also includes the application stage or the implementation/operational stage of criminal law by law enforcers, both the Police, the Prosecutor's Office and the Courts. The current regulations have yet to be able to cover money laundering crimes committed through cyber media. The TPPU Law and ITE Law only cover conventional money laundering crimes and regulate unlawful financial transactions through cyber media.

The Money Laundering Law is a legal instrument issued to accommodate the multi-dimensional and varied modes of money laundering. The TPPU Law perfects the criminalization of money laundering crimes, including regulation of criminal and administrative sanctions, application of the principle of recognizing service users, expansion of reporting parties, predicate crime investigators are given the authority to investigate money laundering in their respective sectors, rearrange the criminal procedure law money laundering and arrange for the confiscation of assets obtained from criminal acts.

Furthermore, the ITE Law does not contain any provisions regarding cyber-based crimes in the modus operandi of money laundering. The ITE Law only regulates the abuse of cyberspace, which harms consumers in electronic transactions. Furthermore, in the National Criminal Code as ius constituendum, the crime of money laundering has been regulated in Chapter XXXV regarding specific crimes, precisely in Article 607 and Article 608. The National Criminal Code changes several provisions in the TPPU Law, including the provisions of Article 2 paragraph (1), Articles 3 to 5 of the TPPU Law are repealed and declared no longer valid.

Setting the criminal act of laundering in the National Criminal Code, on the one hand, is a historic decision since Indonesia's attempts to replace the colonial Criminal Code. However, on the other hand, the regulation of money laundering crimes in the National Criminal Code creates problems, among other things, causing multiple interpretations of investigators in money laundering crimes because the National Criminal Code does not determine which investigators are authorized in money laundering cases.

So far, the authority to investigate special crimes is regulated in the lex specialis law in the respective agency sector. This raises the question of whether special criminal investigators have the authority to investigate crimes regulated in the National Criminal Code, a lex generalis. The National Criminal Code has not yet determined in detail the authority to investigate money laundering cases, whereas, for other crimes, such as corruption and narcotics, the

investigative authority has been regulated. The National Criminal Code, which was promulgated on 2 January 2023 (digital era) and came into effect three years from the date of promulgation, should contain new provisions that accommodate the development of money laundering in the digital era instead of adapting provisions in the ML Law which are lex specialis rules.

The politics of criminal law in dealing with money laundering through cyber media at the level of execution are also faced with several challenges, including in confiscating assets. Various laws and regulations regulate the confiscation of assets in Indonesia (Lukito, 2020). Generally, asset confiscation can only be carried out when the perpetrator of the crime has been found guilty based on an inkracht court decision. Indeed, based on Article 67 paragraph (2) of the TPPU Law, it is possible to confiscate assets without being prosecuted or without waiting for a court decision (Non-Conviction Based Asset Forfeiture) (Priyatno, 2018).

This mechanism positions the resulting assets or means of committing a crime as legal subjects or parties, with the assets suspected of being the proceeds of crime or the means of crime being the respondent, and the state represented by money laundering crime investigators as the applicants/prosecutors. The investigator may petition the district court to decide whether the assets are state assets or should be restored to individuals who are entitled to them if the suspected criminal is not apprehended within 30 (thirty) days.

Even though it is possible to confiscate assets without punishment, this mechanism can only be carried out in certain cases, namely if, within 30 (thirty) days, the perpetrators of the crime are not found, and no person/third party submits an objection within 20 (twenty) days from the date of suspension of the transaction. Therefore, in general, the assets of the perpetrators of money laundering are executed or confiscated after an inkracht court decision. Such an asset confiscation mechanism will certainly become a stumbling block at the level of execution of the assets of the perpetrators of cyber laundering crimes. This is because cyber laundering actors' assets will be easily transferred through online transactions before the court decides the case. In addition, the assets of cyber laundering actors are also stored across national borders, so a mechanism for confiscating assets and progressive international cooperation is needed to ensure that these assets are not transferred or transferred. The process of money laundering can be categorized into three stages, namely:

a) Placement stage: the process of transferring proceeds from a crime into the financial system or attempts to do so. Demand deposits include things like checks, bank draughts, certificates of deposit, and other items.
b) Layering stage: attempts to effectively move assets obtained through illicit activity that were deposited with a financial service provider (particularly a bank) to another financial service provider.
c) Integration stage: attempts to transform assets obtained via illicit activity that have made it into the financial system through placement or transfer into halal assets (clean money) in order to engage in legitimate business or to fund criminal activity. (Hadi, 2003).

The return of assets resulting from criminal acts that were carried out by perpetrators abroad can be carried out by referring to the provisions of the United Nations Convention Against Corruption (KAK), which consist of 4 (four) stages, including tracking assets, preventing the transfer of assets, confiscating and transferring assets to the victim country where the assets were illegally acquired (Yanuar, 2007). One of the highlights in the formation of KAK is the effort to return assets directly or indirectly purchased/obtained illegally. Often these assets are so large that their return requires a procedure that takes work.

Based on the above review, the politics of criminal law in dealing with cyber laundering in Indonesia is still partial. The crime of cyber laundering has not been specifically regulated but only accommodated using the National Criminal Code as a lex generalis, the AML Law as a lex specialis and supplemented by the ITE Law. The National Criminal Code only adapts the provisions of the Money Laundering Law, which are intended for conventional money laundering and has not been able to reach perpetrators of money laundering crimes who use cyberspace as a medium for money laundering. Likewise, the ITE Law only unlawfully regulates cyberspace use but has not explicitly regulated cyber laundering.

2. The Urgency of Updating Regulations for Combating Money Laundering Crimes in the Digital Age

Various daily activities have been facilitated by the presence of digitalization, including money launderers, who are known as cyber laundering (Putri Fajariah Sabda, 2023). In the digital era, the laundering mode has developed using various digital media such as e-commerce, digital currency, online games, crowdfunding, etc. The crime of cyber laundering through e-commerce is carried out using legal payment methods like a member of ISIS in the United States who allegedly earned money from a crime through selling computers on eBay and using Paypal as a transaction medium. Then the crime of cyber laundering using digital currency is also more complex because the privacy of the perpetrators is more secure, so the obscuration of the origin of money is difficult to detect.

Online games also have the potential to be used as a new mode of cyber laundering, like the actions of a Sony Online Entertainment user who transferred money from an account in the United States to Russia through an online game (Muchamad Kibar Kaloka, 2018). Furthermore, cyber laundering is also possible through crowdfunding, which allows perpetrators to create fictitious campaigns and donate money from criminal acts to these fictitious campaigns. Thus, the bank will record the money as legal because it comes from crowdfunding.

Although the objectives of conventional money laundering and cyber laundering tend to be the same, namely disguising the proceeds of crime, there are several specific differences between conventional money laundering and cyber laundering, including:

a) In conventional money laundering, transactions are carried out with cash. In cyber laundering, social engineering carries out transactions through digital banks.
b) The crime of cyber laundering is motivated by falsifying identity to open credit cards, online deposits and loans.
c) In conventional money laundering crimes, perpetrators invest in high-value and movable commodities such as diamonds and gold, unlike the case with cyber laundering crimes that use anonymous online payment services, gift cards, prepaid cards and prepaid credit cards.
d) In conventional money laundering crimes, perpetrators secretly buy and sell assets such as land, buildings and other assets. In cyber laundering crimes, perpetrators tend to conduct online transactions such as buying and selling cryptocurrency.

Based on the description above, technology has opened up opportunities to facilitate cyber laundering. However, the TPPU Law was a regulation that existed before cyber laundering developed massively. So that when money laundering through cyber media becomes real in society, the TPPU Law has many weaknesses to compensate for new modes that were not previously regulated. Likewise, with the ITE Law, it has not yet reached cyber crimes related to illegal/unlawful financial transactions. As with the ASABRI corruption and money laundering case, the mode used was in the form of purchasing several bitcoins from PT Indodax Nasional Indonesia from money resulting from corruption at PT ASABRI (placement) and buying bitcoin transactions using a nominee (other person's name) to create a bitcoin account/token (layering).

Cyber laundering is money laundering in the digital era that has yet to be regulated specifically and comprehensively, even though the ITE Law has accommodated several aspects of cyber-based offenses. However, technical matters regarding cyber laundering countermeasures have yet to be regulated in these existing regulations. Therefore, it is urgent to update regulations on dealing with cyber laundering crimes that can accommodate the complexity of the problem. Furthermore, cyber laundering is multi-dimensional. In addition to money laundering, the perpetrator simultaneously commits cyber crimes or crimes using computer networks. Conventional money laundering and cyber laundering crimes have different characteristics, especially in terms of processes or procedures. In conventional money laundering crimes, disguised money is easily traced and visible. For example, it is transferred in the form of goods. Unlike cyber laundering crimes, the disguised origin of the proceeds of crime is not easily seen because it is transferred in digital form, making it difficult to track it.

As with conventional money laundering, cyber laundering is carried out through the placement, layering and integration stages. However, in cyber laundering, intermediary computer networks carry out the three stages. Thus, preventing cyber laundering crimes requires the readiness of law enforcement in terms of expertise in the fields of computers, finance and law. Unfortunately, the current regulations do not explicitly regulate the authority of agencies in the

anti-money laundering regime, both the authority of predicate crime investigators to carry out cyber laundering investigations and the authority of PPATK to conduct investigations of cyber laundering.

The crime of cyber laundering is a transnational crime that crosses territorial boundaries (Kresnawati, 2020). Therefore, cooperation between countries is needed to create regulations that can prevent cyber laundering crimes. These regulations are prepared with international standards that can encourage various countries to jointly tackle cyber laundering from the investigation process to court hearings. A global money-laundering eradication regime has been developed through the Financial Action Task Force on Money Laundering (FATF). However, the FATF still needs to improve regarding the gap between state losses due to money laundering and the costs incurred in enforcing the law. Regulations in the FATF also raise issues related to state sovereignty; in this case, a country that has not ratified the FATF is forced to implement it. This contradicts the principle of sovereign equality and non-intervention in international law. Deviation from the extra-territorial principle is necessary to eradicate cyber laundering, a cross-border crime, effectively.

Based on the above review, to optimize the prevention of cyber laundering crime, it is necessary to update regulations that are accommodative and implementable in the future. The regulation reform is expected to be a solution to overcoming the problem of overcoming cyber laundering crimes, especially in Indonesia. It is also hoped that the renewal of this regulation will strengthen PPATK's authority as the Indonesian Financial Intelligence Unit (FIU) in conducting investigations into cyber laundering crimes. The granting of investigative authority to PPATK will also reduce the burden on the police and prosecutors, which are also general criminal investigators.

CONCLUSIONS AND RECOMMENDATIONS

Based on the discussion above, it is concluded that the politics of criminal law in dealing with cyber-based money laundering or cyber laundering at the normative level is still partial and has not been specifically regulated. Currently, the crime of cyber laundering is only accommodated by several separate legal regimes, including the TPPU Law and the ITE Law as lex specialis and the National Criminal Code as lex generalis. The TPPU Law has not focused on conventional money laundering and has not regulated in detail regarding cyber laundering. The ITE Law does not contain any provisions regarding cyber-based crimes in the modus operandi of money laundering. Next, the National Criminal Code only adapts the provisions of the TPPU Law, which are intended for conventional money laundering and have not been able to reach the perpetrators of cyber laundering crimes.

Second, countermeasures against money laundering in the digital era, such as cyber laundering, are still regulated by conventional regulations. The TPPU Law was a regulation that existed before cyber-laundering crimes developed massively. Likewise, with the ITE Law, it has not yet reached cyber crimes related to illegal/unlawful financial transactions. Therefore, it is urgent to update regulations on dealing with cyber laundering crimes that can

accommodate the complexity of the problem. Therefore, it is necessary to reform regulations that are accommodative and implementable for cyber laundering crimes in the future.

FURTHER STUDY

The anti-cyber laundering regime in Indonesia needs to strengthen international cooperation, build a cutting-edge digital identification system, improve technology in every agency involved in money laundering, and hire qualified experts in the future. These are just a few of the things it needs to do. Additionally, while still allowing for the existence of two distinct legal systems the ML Law as a lex specialis and the ITE Law as a complement special restrictions specific to cyber laundering were developed.

REFERENCES

Aditya, N. R. (2021). *Tersangka Kasus Asabri Cuci Uang Lewat Bitcoin, PPATK: Modus Baru TPPU*. Nasional.Kompas.Com. https://nasional.kompas.com/read/2021/04/22/10341781/tersangka-kasus-asabri-cuci-uang-lewat-bitcoin-ppatk-modus-baru-tppu?page=all

Alda Satrya, B. N. dan S. (2022). Tindak Pidana Pencucian Uang Terhadap Perjudian Online. *Al-Manhaj: JurnalHukum Dan PranataSosial Islam*, *4*(2), 287–296. https://doi.org/https://doi.org/10.37680/almanhaj.v4i2.1863

Amrani, H. (2015). *Hukum Pidana Pencucian Uang: Perkmebangan Rezim Anti Pencucian Uang dan Implikasinya terhadap Prinsi Dasar Kedaulatan Negara, Yurisdiksi Pidana, dan Penegakan Hukum*. UII Press.

Artha, K. A. A. dan I. G. (2019). Pertanggungjawaban Pidana Pelaku Tindak Pidana Pencucian Uang Melalui Transaksi Game Online. *Kertha Wicara*, *8*(2).

Atmasasmita, R. (2016). Analisis Hukum Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. *PADJAJARAN Jurnal Ilmu Hukum*, *3*(1), 1–23. https://doi.org/https://doi.org/10.22304/pjih.v3n1.a1

Bumeter, B. (2001). *Cyberlaundering: Low Tech Meets High Tech*. Www.Softduit.Com.

Bunga, D. (2019). Politik Hukum Pidana Terhadap Penanggulangan Cybercrime. *Jurnal Legislasi Indonesia*, *16*(1), 1–15.

Filipkowski, W. (2008). Cyber Laundering: An Analysis of Typology and Tecniques. *International Journal of Criminal Justice Sciences*, *3*(1), 15–27.

Garnasih, Y. (2015). *Penegakan Hukum Anti Pencucian Uang dan Permasalahannya di Indonesia*. Rajawali Pers.

Hadi, S. (2003). Analisis Penegakan Hukum Korupsi sebagai Predicate Crime dalam Tindak Pidana Pencucian Uang. *Jurnal Praevia*, *7*(2), 210.

Harahap, H. H. (2020). Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang. *Amaliah: Jurnal Pengabdian Kepada Masyarakat*, *4*(2), 186–190. https://doi.org/https://doi.org/10.32696/ajpkm.v4i2.551

Indiraphasa, N. S. (2021). *Kenali Risiko Pencucian Uang di Balik Transaksi E-Commerce*. Www.Nu.or.Id. https://www.nu.or.id/nasional/kenali-risiko-pencucian-uang-di-balik-transaksi-e-commerce-pXcuN

Irina, C. (2018). Cryptocurrencies Legal Regulation. *BRICS Law Journal*, *5*(2), 128–153. https://doi.org/https://doi.org/10.21684/2412-2343-2018-5-2-128-153

Iskandar, Y. (2022). *Peran Bank Menghadapi Ancaman Baru dalam Kejahatan Pencucian*

Uang. Www.Hukumonline.Com. https://www.hukumonline.com/berita/a/peran-bank-menghadapi-ancaman-baru-dalam-kejahatan-pencucian-uang-lt638557e274cdc?page=2

Kresnawati, A. R. dan M. A. (2020). Hubungan Amerika Serikat dan Meksiko Menghadapi Money Laundering Tahun 2008-2012. *Global and Policy Journal of International Relations*, *10*(1), 1–18.

Leslie, D. A. (2010). *Anti-Cyberlaundering Regulation And Control*. Faculty of Law University of the Western Cape.

Lukito, A. S. (2020). Revealing The Unexplained Wealth In Indonesian Corporation: A Revolutionary Pattern In Non-Conviction-Based Asset Forfeiture. *Journal of Financial Crime*, *27*(1), 29–42. https://doi.org/https://doi.org/10.1108/JFC-11-2018-0116

Merdeka. (2022). *Data PPATK: Pencucian Uang Hasil Judi Online Capai Rp81 Triliun*. Www.Merdeka.Com. https://www.merdeka.com/uang/data-ppatk-pencucian-uang-hasil-judi-online-capai-rp81-triliun.html

Muchamad Kibar Kaloka, I. R. P. dan S. P. (2018). Cyber Laundering melalui Online Games: Potensi Ancaman Keamanan Ekonomi. *Journal of International Relations*, *1*(1), 31–40. https://doi.org/https://doi.org/10.14710/jirud.v1i1.19127

Nuryanto, A. D. (2019). Problem Penyidikan Tindak Pidana Pencucian Uang Yang Berasal Dari Predicate Crime Perbankan. *Bestuur*, *7*(1), 54–65. https://doi.org/https://doi.org/10.20961/bestuur.v7i1.43437

P.P., A. R. (2019). Analisis Ekonomi terhadap Hukum Tindak Pidana Pencucian Uang. *Lex Renaissance*, *4*(2), 303–316. https://doi.org/https://doi.org/10.20885/JLR.vol4.iss2.art6

Priyatno, D. (2018). Non Conviction Based (NCB) Asset Forfeiture for Recovering the Corruption Proceedings in Indonesia. *J. Advanced Res. L. & Econ*, *9*(31), 219–233.

Putri Fajariah Sabda, N. dan M. I. H. (2023). Implementasi Digitalisasi sebagai Upaya Meningkatkan Jumlah Nasabah Asuransi Syariah: Studi Kasus Kantor Prudential Syariah Cabang Binjai. *JIKEM: Jurnal Ilmu Komputer, Ekonomi Dan Manajemen*, *3*(1), 1311–1346.

Reuter, M. L. dan P. (2006). *Money Laundering*. The University of Chicago.

Sari, H. Y. dan F. P. (2022). Telaah Pembuktian Terbalik Tindak Pidana Pencucian Uang Dalam Proses Peradilan. *Jurnal Hukum Dan Bisnis (Selisik)*, *8*(2), 98–109. https://doi.org/https://doi.org/10.35814/selisik.v8i2.4492

Sidik, S. (2021). *Pandemi Covid-19 Tingkatkan Risiko Pencucian Uang*. Cnbcindonesia.Com. https://www.cnbcindonesia.com/tech/20210919184646-37-277461/pandemi-covid-19-tingkatkan-risiko-pencucian-uang

Sudarti, S. L. dan E. (2021). Pembuktian Terbalik pada Tindak Pidana Pencucian Uang. *Refleksi Hukum*, *5*(2), 199–218. https://doi.org/https://doi.org/10.24246/jrh.2021.v5.i2.p199-218

Sutedi, A. (2008). *Tindak Pidana Pencucian Uang*. Citra Aditya Bakti.

Yanuar, P. M. (2007). *Pengembalian Aset Hasil Korupsi berdasarkan Konvensi PBB Anti Korupsi 2003 dalam Sistem Hukum Indonesia*. Alumni.