HORIZON PUBLIC LEGAL STUDIES
Vol 2 Issue 1 Tahun 2025
Doi : https://doi.org/10.56087/k8sa7f51

Cyberlaundering sebagai Evolusi Pencucian Uang: Keterbatasan Konsep Pertanggungjawaban Pidana di Era Digital

Muhammad Imam Fakhri [1], Muhammad Kamal Hidjaz [2], Andi Istiqlal Assaad[3]

[1,2,3] Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Surel Koresponden: *imamfakhri13@gmail.com*

Abstrak: Penelitian ini bertujuan untuk menganalisis pengaturan hukum tindak pidana pencucian uang melalui teknologi digital (cyberlaundering) dalam sistem hukum Indonesia serta bentuk dan dasar pertanggungjawaban pidana terhadap pelakunya. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, kasus, dan komparatif. Bahan hukum yang digunakan meliputi bahan hukum primer, sekunder, dan tersier yang diperoleh melalui studi kepustakaan dan dokumentasi, kemudian dianalisis secara kualitatif untuk menafsirkan norma hukum terkait cyberlaundering. Hasil penelitian menunjukkan bahwa cyberlaundering belum diatur secara khusus dalam satu regulasi, namun dapat dijerat melalui ketentuan tindak pidana pencucian uang dan regulasi transaksi elektronik yang bersifat teknologi-netral. Peran Pusat Pelaporan dan Analisis Transaksi Keuangan penting dalam mendeteksi transaksi keuangan mencurigakan berbasis digital. Pertanggungjawaban pidana dapat dikenakan kepada individu maupun korporasi dengan dukungan alat bukti elektronik. Namun, masih terdapat kelemahan terkait klasifikasi aset digital, prosedur penyitaan aset virtual, serta pengaturan entitas teknologi seperti smart contract dan DAO sehingga diperlukan pembaruan hukum yang lebih adaptif terhadap perkembangan teknologi digital.

Kata Kunci: Pertanggungjawaban,Tindak Pidana,Pencucian Uang,Cyberlaundering.

Abstract: *This study aims to analyze the legal regulation of money laundering through digital technology (cyberlaundering) in the Indonesian legal system, as well as the forms and basis of criminal liability for perpetrators. This study uses a normative legal research method with a legislative, conceptual, case, and comparative approach. The legal materials used include primary, secondary, and tertiary legal materials obtained through literature and documentation studies, which are then analyzed qualitatively to interpret legal norms related to cyberlaundering. The results of the study show that cyberlaundering is not specifically regulated in any single regulation, but can be prosecuted under criminal provisions on money laundering and technology-neutral electronic transaction regulations. The Financial Transaction Reports and Analysis Center plays an important role in detecting suspicious digital-based financial transactions. Criminal liability can be imposed on individuals and corporations with the support of electronic evidence. However, there are still weaknesses related to the classification of digital assets, procedures for seizing virtual assets, and the regulation of technological entities such as smart contracts and DAOs, so legal reforms that are more adaptive to developments in digital technology are needed.*

Keywords: *Accountability, Criminal Offenses, Money Laundering, Cyberlaundering.*

A. INTRODUCTION

In the life of the nation and state, the Unitary State of the Republic of Indonesia (NKRI) is based on the 1945 Constitution of the Republic of Indonesia (UUD 1945) which guarantees the upholding of a state of law as stated in Article 1 paragraph (3) of the UUD 1945, which states that "The State of Indonesia is a state of law". The concept of a state of law demands the supremacy of law, equality before the law, and fair law enforcement, including in the fields of state economics and finance. The development of information and communication technology in the modern era has brought significant changes in various areas of human life, including economic, social, and financial systems.[1] The digitalization of the financial sector, marked by the emergence of electronic payment systems, cryptocurrencies, peer-to-peer lending services, and digital wallets (e-wallets), has made it easier for people to conduct cross-border transactions with high efficiency and low costs. While this progress has had a positive impact on economic progress, it has also created new threats in the form of increased risks of financial crime, particularly money laundering.[2]

From an Islamic legal perspective, the development of financial technology and the potential for crimes such as money laundering also have a strong relevance to Sharia principles. Islam, as a comprehensive value system, not only regulates aspects of worship but also regulates social life, including economic and financial activities. In this regard, the main principles upheld are justice (al-'adl), honesty (as-shidq), and the prohibition of all forms of illegitimate acquisition. The Quran expressly prohibits the practice of acquiring wealth through unlawful means, as stipulated in Surah Al-Baqarah, verse 188, which states that humans are prohibited from consuming the wealth of others through unlawful means and bringing cases to a judge for the purpose of illicit gain. This principle serves as the normative basis for all forms of financial crime, including money laundering, as it contradicts Islamic values because it aims to disguise the origins of assets obtained through unlawful acts. Furthermore, in Surah Al-Baqarah, Verse 29 of An-Nisa also emphasizes the prohibition for believers to consume one another's wealth unlawfully, except through consensual trade. This verse demonstrates that transparency and legitimacy in transactions are fundamental principles of Islamic economics. Therefore, money laundering practices that attempt to conceal the origin of wealth clearly contradict the principles of openness and honesty in transactions.[3]

Furthermore, a hadith narrated by the Prophet Muhammad (peace be upon him) states that "any flesh that grows from something unlawful is more deserving of Hell" (Narrated by Tirmidhi). This hadith provides a stern warning against all forms of illegitimate wealth acquisition, including proceeds of crime that are then "cleansed" through money laundering. This demonstrates that in Islam, not only the process of acquiring wealth is considered, but also its source and its lawfulness. Therefore, the development of modern financial technology must be balanced with the strengthening of moral and ethical values rooted in Islamic teachings. State regulations to prevent and eradicate money laundering are in line with sharia principles, which

emphasize the importance of safeguarding assets (hifz al-mal) as one of the primary objectives of Islamic law (maqasid al-syariah). Therefore, the integration of the positive legal system and Islamic values is crucial in creating a fair, transparent, and just financial system.[4]

One of the major challenges in enforcing modern economic law is the rise in money laundering, which not only harms state finances but also threatens the stability of the national financial system. In line with the mandate of Article 33 paragraph (4) of the 1945 Constitution, national economic development must be carried out based on the principles of economic democracy with fair efficiency, sustainability, environmental awareness, independence, and maintaining a balance between progress and national economic unity. The crime of money laundering clearly contradicts these principles because it creates economic distortions and obscures legitimate sources of wealth.[5] As a derivative of the 1945 Constitution, Indonesia enacted Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (UU TPPU), which replaced Law Number 15 of 2002 in conjunction with Law Number 25 of 2003. This law aims to provide a strong legal basis for the prevention, detection, and prosecution of money laundering practices, as well as strengthening the Financial Transaction Reports and Analysis Center (PPATK) as an independent institution in the supervision and analysis of suspicious financial transactions.[6] However, the rapid development of digital technology has created a new form of money laundering crime known as cyberlaundering. Cyberlaundering is the practice of money laundering using information technology, digital banking systems, cryptocurrencies, and difficult-to-trace cross-border electronic transactions. This phenomenon has created new challenges in terms of criminal liability, both for individuals, corporations, and parties indirectly involved in facilitating money laundering through digital systems.[7] In the context of Indonesian positive law, law enforcement against digital technology-based money laundering crimes still faces various obstacles, including limited legal instruments specifically for handling digital assets, difficulties in tracking virtual asset transactions, and differences in jurisdiction between countries. Although the Money Laundering Law generally regulates money laundering, it has not fully adapted to new, complex forms of digital crime.[8].

Against this backdrop, this research is crucial for comprehensively understanding the challenges and strategies for law enforcement against digital-based money laundering. This study not only highlights the normative aspects of criminal law but also considers the technological implications and dynamics of cybercrime, thereby providing appropriate recommendations for improving the effectiveness of money laundering prevention and prosecution in the digital era. Therefore, this research is expected to serve as a reference for developing legal policies and enhancing the capacity of law enforcement officials to address the complexities of modern financial crimes. Based on this description, this research then formulates the problems that it wants to answer, namely: (1) What are the legal regulations regarding the crime of money laundering using digital technology (cyberlaundering)?; and (2) What is the form of criminal responsibility for perpetrators of the crime of money laundering using digital technology?.

B. METHOD

This research is a normative legal research, namely research that regulates the responsibility of perpetrators of money laundering crimes using digital technology (cyberlaundering). The approaches used include a legislative approach by examining various laws and regulations that form the basis for regulating money laundering and digital crimes; a conceptual approach that examines basic concepts related to criminal responsibility, economic crimes, and cyberlaundering, with reference to criminal law theory, criminal responsibility theory, and digital economic crime theory; a case approach to analyze concrete cases or court decisions related to digital technology-based money laundering crimes (cyberlaundering), both at the national and international levels. For example: decisions related to money laundering through cryptocurrency, e-wallet, or other digital transactions; and Comparative Approach To compare the application of law in Indonesia with other countries in dealing with the phenomenon of cyberlaundering, in order to see the effectiveness and gaps in legal regulations in Indonesia. The legal materials used consist of primary legal materials in the form of laws and regulations that are binding, secondary legal materials in the form of books, scientific journals, research results, and opinions of relevant experts, as well as tertiary legal materials such as dictionaries and legal encyclopedias that support the understanding of terms and concepts. The collection of legal materials is carried out through literature studies by tracing various sources related to the issue of cyberlaundering.

C. DISCUSSION

1. Legal Regulations Concerning the Crime of Money Laundering Using Digital Technology (cyberlaundering)

Money laundering (TPPU) in Indonesia is comprehensively regulated in Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering. This law defines money laundering as any act that fulfills the elements of placing, transferring, spending, paying, donating, entrusting, transporting abroad, or other acts involving assets known or reasonably suspected to originate from criminal acts, with the aim of disguising or concealing the origin of said assets. This regulation serves as the primary legal basis for law enforcement against various money laundering methods, including those carried out through digital technology.[9] Advances in information technology have given rise to a new form of money laundering known as cyberlaundering. Cyberlaundering is money laundering that utilizes digital media such as internet banking, electronic money (e-money), cryptocurrency, and technology-based financial platforms (fintech). This method allows perpetrators to conduct cross-border transactions quickly, anonymously, and with difficulty being traced, posing new challenges for the legal system and law enforcement officials in detecting and proving these crimes.[10]

Normatively, cyberlaundering in Indonesia has not been explicitly regulated in a specific regulation. However, the provisions of Law No. 8 of 2010 can still be applied because the

formulation of the elements of the crime of money laundering is technology-neutral. This means that the media or means used, including digital technology, do not eliminate the illegal nature of the money laundering act as long as the elements of the crime are met. Therefore, cyberlaundering can be classified as part of conventional money laundering crimes with a technology-based modus operandi.[11] Regulations regarding cyber laundering are also closely related to Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 [12]. The ITE Law provides the legal basis for the validity of electronic transactions and electronic evidence, which are crucial in proving digital-based money laundering. Furthermore, digital banking and finance regulations issued by Bank Indonesia and the Financial Services Authority (OJK) play a role in preventing and detecting suspicious transactions that could potentially involve money laundering.[13]

Although cyberlaundering can be legally prosecuted under existing regulations, there are various challenges in its implementation, including the limited capabilities of law enforcement officials in digital technology, the anonymity of transactions, and the borderless nature of cybercrime. Therefore, strengthening regulations, increasing international cooperation, and developing the capacity of law enforcement officials are necessary to ensure that legal regulation of cyberlaundering is effective and responsive to technological developments.[14] The Financial Transaction Reports and Analysis Center (PPATK) plays a strategic role in preventing and eradicating money laundering, including those conducted through digital technology. PPATK is authorized to receive, analyze, and evaluate reports of suspicious financial transactions from digital financial service providers. In practice, monitoring electronic transactions has become increasingly important with the increasing use of fintech and crypto assets. The results of PPATK's analysis are then submitted to law enforcement officials as the basis for investigating and prosecuting money laundering crimes.[15] Proof is a crucial aspect in enforcing cyberlaundering laws. Under Indonesian law, electronic evidence has been recognized as valid evidence, as stipulated in the Electronic Information and Transactions (ITE) Law. This recognition strengthens law enforcement against digital-based money laundering crimes, given that most cyberlaundering activities are conducted through electronic systems. However, the use of electronic evidence must still meet the principles of authenticity, integrity, and reliability of electronic systems to be admissible in court.[16] Cyberlaundering is cross-border, so its legal regulation cannot rely solely on national law. Indonesia has ratified various conventions and established international cooperation to eradicate money laundering, including cooperation on the exchange of financial information and mutual legal assistance. This cooperation is crucial for tracking the flow of digital funds through other countries' jurisdictions and for addressing differences in legal systems in handling technology-based money laundering crimes.[17] Based on the above description, it can be concluded that legal regulations related to cyberlaundering in Indonesia are essentially available through various sectoral and complementary laws and

regulations. However, these regulations are still scattered and do not specifically address cyberlaundering as a crime with its own characteristics. Therefore, an update to criminal law policy is needed that is more adaptive to developments in digital technology so that money laundering legal regulations remain effective and provide legal certainty. [18]

The legal framework for cyberlaundering in Indonesia relies on the expanded interpretation of assets in Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU Law). Article 1, paragraphs 4 and 5 of the TPPU Law broadly define assets as movable or immovable, tangible or intangible, objects obtained either directly or indirectly.[19] This explanation allows for digital assets such as cryptocurrency or e-money to be categorized as objects of money laundering. However, because the TPPU Law was enacted before the widespread adoption of blockchain technology, the norm remains conventional and relies heavily on the involvement of Financial Services Providers (PJK) as reporting parties. To address this gap, Law No. 1 of 2024 (the Second Amendment to the ITE Law) provides a formal normative basis through Article 5, which stipulates that electronic information and documents constitute valid legal evidence. Thus, there is a normative integration between substantive law (the TPPU Law) and formal law (the ITE Law) in prosecuting money laundering crimes in cyberspace.[20]

A normative advantage of Indonesian regulations is the progressive adoption of the Know Your User Principles (PMPJ). Although the Money Laundering Law does not explicitly mention "virtual assets," implementing regulations such as PPATK Regulation No. 1 of 2021 have included virtual asset service providers as reporting parties.[21] This creates a legal safety net that requires digital platforms to report suspicious transactions. Furthermore, the extraterritorial principle in Article 2 of the ITE Law and Article 2 of the Money Laundering Law provides the legal framework's reach across national borders. This demonstrates that Indonesian law has anticipated the borderless nature of cyberlaundering, ensuring there is no legal vacuum regarding jurisdiction over crimes committed abroad but affecting domestically.[22]

Indonesia's legal regulations still face fundamental weaknesses regarding legal certainty in the classification of digital assets. On the one hand, the Money Laundering Law (AML) views digital assets as assets, but on the other hand, sectoral regulations (Bappebti) categorize them only as commodities, not as means of payment. This dualism of norms creates ambiguity in the confiscation and execution procedures stipulated in the Criminal Procedure Code (KUHAP). Normatively, the KUHAP does not yet regulate procedures for decentralized asset confiscation (without central authority), so existing confiscation norms are often incompatible with the technical characteristics of cyberlaundering.[19]

There is a legal gap in regulating criminal liability for smart contract technology or decentralized autonomous organizations (DAOs). Because Indonesian criminal law strictly upholds the nullum delictum principle and limits legal subjects to individuals and

corporations, it is legally difficult to prosecute money laundering conducted entirely through automated code protocols without a clear legal entity.[20]

2. Forms of Criminal Responsibility for Perpetrators of Money Laundering Crimes Using Digital Technology.

Criminal liability is a legal consequence imposed on a person who has been proven to have committed a crime by fulfilling the elements of a criminal act and an element of guilt. In the context of money laundering, criminal liability is imposed on anyone who intentionally places, transfers, diverts, spends, or conceals assets known or reasonably suspected to originate from a criminal act. This principle also applies to perpetrators who utilize digital technology as a means of carrying out money laundering.[23] In normative legal research, the element of fault (schuld) is the primary requirement for determining whether or not a perpetrator can be held criminally responsible. The element of fault in money laundering includes intent (dolus) or at least knowledge that the assets being managed originate from criminal activity. In cyberlaundering, this element of fault can be proven through digital transaction patterns, the use of fictitious accounts, and electronic footprints that indicate an intention to disguise the origin of the assets.[24] Perpetrators of money laundering using digital technology can be individuals who directly conduct electronic transactions to disguise the proceeds of crime. Under Law No. 8 of 2010, individual perpetrators can be held criminally liable as principal perpetrators, accomplices, or accomplices. The use of digital technology does not eliminate criminal liability as long as the elements of the money laundering crime and the elements of guilt can be legally proven.[25]

In addition to individual perpetrators, criminal liability for digital money laundering crimes can also be imposed on corporations. Law No. 8 of 2010 expressly recognizes corporations as subjects of criminal law. Corporate criminal liability can be applied if the money laundering crime is committed for the benefit of the corporation or on the orders of corporate management, including the use of the corporation's information technology systems and digital platforms.[26] Criminal liability for digital money launderers is realized through criminal sanctions, as stipulated in Law No. 8 of 2010, in the form of imprisonment and fines. Additionally, corporations can be subject to additional penalties such as asset confiscation, freezing of business activities, or revocation of business licenses. The imposition of these criminal sanctions aims to provide a deterrent effect and prevent the use of digital technology as a means of money laundering.[19]. In digital money laundering crimes, electronic evidence plays a crucial role in proving the perpetrator's criminal liability. The ITE Law recognizes electronic information and/or electronic documents as valid legal evidence. In normative research, this recognition of electronic evidence strengthens the basis for criminal liability, as digital transactions and electronic traces can be used to prove the elements of the act and the elements of the perpetrator's guilt.[27] Based on a normative analysis of existing laws and regulations, criminal liability for perpetrators of money laundering using digital technology is essentially legally sound. However, challenges remain in its implementation, particularly regarding proving fault and identifying perpetrators in

anonymous, cross-border digital transactions. Therefore, strengthening criminal law regulations and policies that are more adaptive to developments in digital technology is necessary.[14].

This normative legal research shows that the criminal liability of cyberlaunderers depends not only on the existence of legal norms, but also on the law's ability to keep up with technological developments. Therefore, the results of this research can be used as a basis for consideration in criminal law reform, particularly in formulating regulations that explicitly regulate criminal liability for digital technology-based money laundering crimes to provide legal certainty and justice.[28] The current criminal liability framework for cyberlaundering in Indonesia remains patchy, relying on the analogy of expanding elements in Law No. 8 of 2010 (the Money Laundering Law). Normatively, criminal liability in this phenomenon can be derived through the doctrine of mens rea (malicious intent) associated with the unlawful acquisition of digital assets. I believe that Articles 3, 4, and 5 of the Money Laundering Law have sufficient normative flexibility to encompass legal entities, both individuals and corporations, that conduct transactions through electronic systems.[29]

This is reinforced by Law No. 1 of 2024 (the Electronic Information and Transactions Law), which normatively positions digital evidence as a valid primary means of evidence. Therefore, when a perpetrator disguises the proceeds of their crime through a layering mechanism on a crypto exchange or e-wallet, criminal responsibility can still be placed on the culpability of the legal subject, despite the fact that the medium used is virtual. This legal enforcement is also normatively supported by Supreme Court Regulation No. 13 of 2016, which allows digital service providers to be held accountable if proven not to have implemented an adequate prevention system for suspicious transactions on their platforms.[22] The primary advantage of Indonesia's legal system lies in the highly aggressive "Follow the Money" nature of the Money Laundering Law. Normatively, criminal penalties no longer rely solely on thorough proof of the predicate crime, allowing law enforcement officials to independently pursue suspicious digital assets.[30]

Another advantage is the normative harmonization between the Money Laundering Law and the cyber legal regime in the Electronic Information and Transactions Law, which recognizes electronic signatures and digital footprints as concrete legal entities. The extraterritorial principle inherent in both laws, in my opinion, is also a crucial normative advantage; legally, Indonesia does not lose its sovereignty to pursue criminal responsibility even if the perpetrator commits cyberlaundering from outside its borders, as long as the digital infrastructure used or the resulting losses affect legal interests in Indonesia.[31] However, upon closer examination, a concerning legal vacuum exists regarding the definition and procedures for executing virtual assets. Normatively, our Criminal Procedure Code (KUHAP) remains behind, lacking a mechanism for confiscating decentralized assets, such as private keys or assets in smart contracts that lack a central administrator. This creates legal

uncertainty when investigators encounter the anonymous nature of blockchain technology.[32]

Furthermore, there is a normative dualism in the classification of digital assets; on the one hand, they are viewed as objects of money laundering (TPPU), but on the other, sectoral regulations only recognize them as traded commodities, not financial instruments. Another fundamental shortcoming is the lack of criminal liability for non-legal entities such as Decentralized Autonomous Organizations (DAOs). Within our criminal law framework, which adheres to the principle of lex stricta, it is difficult for law enforcement to hold accountable when money laundering is carried out entirely by automated code protocols without legally defined human directors or administrators.[33]

D. CONCLUSION

Based on the research and discussion, it can be concluded that the legal regulations regarding the crime of money laundering through digital technology (cyberlaundering) in Indonesia have been accommodated through Law No. 8 of 2010 and the ITE Law. However, the absence of lex specialis regulations results in legal uncertainty in law enforcement due to the anonymity and cross-border nature of digital transactions. This condition has implications for the ineffectiveness of norms in the aspect of supervision and legal limitations in the complex digital evidence process. Criminal liability for cyberlaundering is based on the fulfillment of the elements of acts and errors according to the Money Laundering Law, both for individuals and corporations, by utilizing electronic evidence that is valid according to the ITE Law. Although a normative legal basis is available, the anonymity of transactions and the cross-border nature create problems in qualifying the offense and limitations of proof in constructing the element of material intent of the perpetrator.

E. REFERENCE

[1] G. White, *Rinsed: From Cartels To Crypto How The Tech Industry Washes Money for The Worlds Deadliest Crooks*. Washington: Penguin Business, 2024.

[2] Yurizal, *Tindak Pidana Pencucian Uang di Indonesia*. Jakarta: Media Nusa Centre, 2017.

[3] Putri Kartika Nanda, "6.+349-355+UIN+Prinsip+Perdagangan+dalam+Islam+Menurut+Tafsir+Al-Quran+Analisis+Q.S.+Al-Baqarah+Ayat+275+dan+Q.S.+An-Nisa+ayat+29 (1)," *Sahmiyya*, vol. 3, no. 2, pp. 349–355, 2024.

[4] D. R. Yuliana *et al.*, "Peran Etika Moral dan Akhlak dalam Kultur Makan: Studi Mini Riset pada," *J. Ilm. Wahana Pendidikan, Juli*, vol. 2023, no. 13, pp. 161–177, 2023.

[5] B. P. Yuda, Y. Yoserwan, and R. Afrizal, "Analisis Yuridis Pertanggungjawaban Tindak Pidana Pencucian Uang Melalui Aset Kripto Di Indonesia," *Lareh Law Rev.*, vol. 1, no. 1, pp. 17–33, 2023, doi: 10.25077/llr.1.1.17-33.2023.

[6] E. Swasono, *Sistem Ekonomi Indonesia*. Jakarta: UI Press, 2016.

[7] P. U. N. O. Tahun and P. Uang, "No Title," vol. VII, no. 2, pp. 74–80, 2018.

[8] Lisnawati, *Hukum Money Laundering*. Setara Press, 2018.

[9] Y. Garnasih, *Tindak Pidana Pencucian Uang*. Jakarta: FH UI Press, 2016.

[10] I. M. P. Diantha, *Hukum Pidana Ekonomi*. Denpasar: Udayana University Press, 2018.

[11] A. Ali, *Hukum Pidana Khusus: Tindak Pidana Pencucian Uang*. Jakarta: Rajawali Pers, 2016.

[12] "UU No.19 tahun 2016," 2016.

[13] B. N. Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*. Jakarta: Kencana, 2018.

[14] R. Atmasasmita, *Globalisasi Kejahatan dan Penegakan Hukum*. Jakarta: Kencana, 2016.

[15] PPATK, *Tipologi Pencucian Uang Berbasis Teknologi Informasi*. Jakarta: Kencana, 2019.

[16] A. Syauket, *Pelaku Pasif Tindak Pidana Pencucian Uang*. Malang: Literasi Nusantara Abadi, 2023.

[17] D. Priyatno, *Tindak Pidana Pencucian Uang*. Jakarta: Prenada Media, 2023.

[18] SAPIDIN, "Kajian Hukum Tindak Pidana Pencucian Uang Dari Aspek Tindak Pidana Ekonomi Legal Review Of The Crime Of Money Laundering," vol. 21, no. 2, pp. 91–109, 2023.

[19] A. Amrullah, *Tindak Pidana Pencucian Uang dalam Perspektif Cybercrime.* Jakarta: RajaGrafindo Persada, 2016.

[20] I. Renzu, *Hukum Aset Kripto di Indonesia*. Jakarta: Salemba Humanika, 2020.

[21] D. E. Purwoleksono, *Hukum Pidana Khusus.* Surabaya: Airlangga Univesity Press, 2021.

[22] P. M. Marzuki, *Penelitian Hukum*, Revisi. Jakarta: Prenada Media, 2017.

[23] A. AZIS, "Kejahatan Pencucian Uang Sebagai Tindak Pidana Lanjutan Ditinjau Dari Undang Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang," vol. 1, no. 1, 2024.

[24] Simanjuntak, *hukum dan pembangunan*. Jawa Tengah: Eureka Media Aksara, 2022.

[25] A. Hamzah, *Hukum Pidana Indonesia*. Jakarta: Sinar Grafika, 2017.

[26] G. H. Silalahi and P. Jamba, "Pidana Berat Dikaji Dari Perspektif Hukum Positif Indonesia".

[27] S. Utami, "Tindak Pidana Pencucian Uang Terhadap Uang Virtual Money Laundering on Virtual Money," *Al-Adl J. Huk.*, vol. 13, no. 1, p. 1, 2021, doi: 10.31602/al-adl.v13i1.4224.

[28] T. Y. A. Maulia and R. I. Saptatiningsih, "Implementasi Undang-Undang No. 35 Tahun 2014 Tentang Perlindungan Anak," *J. Kewarganegaraan*, vol. 4, no. 1, pp. 10–16, 2020, doi: 10.31316/jk.v4i1.877.

[29] Y. Husein, *Bunga Rampai Anti Pencucian Uang*. Jakarta: Books Terrace and Library, 2007.

[30] Y. S. LAOWO, "Kajian Hukum Tindak Pidana Pencucian Uang," vol. 1, pp. 70–87, 2022.

[31] Pramono, "Tantangan Penegakan Hukum Terhadap Cyberlaundering Melalui Aset Kripto di Indonesia," *Huk. Dan Pembang.*, vol. 50, 2020.

[32] Santoso, "Analisis Yuridis Pertanggungjawaban Pidana dalam Transaksi Mata Uang Virtual," *Mimb. Huk.*, 2021.

[33] R. Amin, *Tindak Pidana Pencucian Uang*. Yogyakarta: Deepublish Digital, 2023.