5th CoNeScINTech
Conference on Business, Social Sciences and Technology

Volume 5 No 1 (2025)

Received : June 13th, 2025
Accepted : September 17th, 2025
Published : September 18th, 2025

Conference on Business, Social Sciences and Technology
https://journal.uib.ac.id/index.php/conescintech

Corporate Criminal Liabilty in Money Laundering Offenses from Online Gambling: A Case Study of PT AJP in the Digital Era

Eka Binaria Manullang[1], Nopita Sari Br Tarigan[2], Roshinta[3], Emiliya Febriyani[4]
emiliya@uib.ac.id
[1-4]Faculty of Law, Universitas Internasional Batam, Batam, Indonesia

Abstract

Digital transformation has significantly reshaped the landscape of economic crime, particularly in the context of money laundering offenses (TPPU) involving or facilitated by corporations. This study examines Indonesia's positive legal framework governing corporate criminal liability in cases of money laundering, with a specific focus on proceeds derived from online gambling activities. The analysis is grounded in a case study of PT AJP, a corporation designated as a suspect by the Indonesian National Police (Bareskrim Polri) for allegedly receiving and managing funds totalling IDR 40.56 billion originating from online gambling operations. These funds were subsequently utilized for the construction and operation of Hotel Aruss. The corporation's conduct is deemed to fulfil the elements stipulated in Articles 3, 4, and 5 of Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering, particularly regarding concealing, disguising, and utilizing criminal proceeds. This article also explores the application of the principles of strict liability and corporate criminal liability, under which a corporation may be held criminally liable irrespective of subjective fault, provided the act is committed by an authorized individual acting on behalf of the corporation. The findings highlight the urgent need for robust and adaptive legal enforcement in addressing technology-driven economic crimes and underscore the importance of regulatory reforms that can effectively respond to the increasingly sophisticated methods employed by corporate actors in the digital era.

Keywords:

Money Laundering Offense, Corporate Liability, Strict Liability

Introduction

The digital era has ushered in a profound transformation across virtually every sector of life, including criminal activity. One offense that has rapidly evolved alongside advances in information technology is money laundering, particularly when it originates from illicit online gambling. Online gambling not only poses moral and social challenges but also legal ones—especially when such activities are concealed through legally constituted entities (corporations). Corporate-perpetrated crimes are notoriously difficult to trace because they tend to be carried out systematically and in a structured manner, involving a range of supporting entities, from digital service providers to banking and investment institutions. The PT AJP case constitutes a pivotal starting point for understanding the complexity of corporate criminal responsibility in cases of money laundering sourced from online gambling. This case is a significant legal precedent in Indonesia because it demonstrates how a corporation can be employed as a vehicle to obscure funds obtained from illicit networked criminal activities in cyberspace (Gemilang, 2024: 8455-8471)

In the case that came to light in 2024, PT AJP is alleged to have acted as a principal facilitator in concealing the flow of funds derived from illegal online gambling conducted via various digital platforms. Although the company formally operated in the information technology services sector, law enforcement investigations revealed that it was utilized to obscure the origin of gambling-derived funds through money laundering mechanisms. In collaboration

with multiple parties, PT AJP managed a system comprised of networks of fake accounts, fictitious transactions, and complex financial transfer schemes designed to create the appearance that the funds originated from legitimate business activities. This phenomenon underscores that, in the digital era, corporations can not only serve as potential victims of cybercrime but also function as active perpetrators who misuse their legal persona to secure illicit profits.

The importance of examining corporate criminal liability in this case lies in the theoretical and practical challenges of recognizing a legal entity as a subject of criminal law. Classical criminal law originally recognized only the criminal responsibility of natural persons, since punishment was conceived as suffering that could not be imposed on non-human entities. However, with the rise of crimes committed through or by corporations, there emerged a legal need to acknowledge corporations as subjects of criminal offenses. In Indonesia, recognition of corporate criminal liability has begun to be accommodated in various sectoral laws and regulations, including Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering (UU TPPU). Nonetheless, enforcement of corporate criminal liability continues to face numerous obstacles, including issues related to burden of proof, organizational structure, and sentencing.

Within the context of the Money Laundering Law (Law No. 8 of 2010), a corporation may be held criminally liable if money laundering is carried out in the name of the corporation, for its benefit, or by utilizing the corporation's facilities. Article 7 of the Law explicitly states that when a predicate offence is committed by a corporate entity, criminal liability may be imposed on the corporation itself, its management, and/or any other individuals who issued orders or made decisions. Thus, corporate criminal liability extends beyond the legal entity itself and encompasses individuals within the organization who hold strategic decision-making authority.

In the case of PT AJP, investigations revealed that top management actively orchestrated money laundering schemes. This included manipulation of digital transaction data, concealing the identities of both remitters and recipients, and employing false identities to open bank accounts. These findings demonstrate the presence of mens reaa deliberate intent on the part of the corporation in executing the laundering operations (Iskandar, 2022: 51-59)

Despite this, in practice, proving the elements required for corporate criminal liability is not straightforward. One primary challenge is establishing the connection between individual conduct and the corporate entity. In many cases, corporations will attempt to evade liability by asserting that the misconduct was perpetrated by rogue actors acting outside official company policy. Consequently, it is essential to demonstrate that the individual's actions fell within their corporate authority and were carried out for the benefit of the corporation. In the PT AJP case, evidence presented by investigators revealed a consistent alignment between management directives and the operational activities of the money laundering. This consistency strengthens the prosecution's position in holding the corporation criminally responsible.

Furthermore, another significant challenge in establishing corporate criminal liability in cases of money laundering stemming from online gambling is the weakness of internal monitoring and compliance systems within corporations. Many companies merely implement compliance on an administrative level without genuinely integrating anti–money laundering principles. Moreover, corporations often exploit regulatory gaps and weaknesses in financial oversight, particularly in the use of financial technology (fintech), digital wallets, and online banking services, which remain vulnerable to misuse. For instance, PT AJP employed foreign-based servers and encryption systems to conceal transaction identities, complicating authorities' efforts to trace financial flows. This underscores that corporate criminal accountability in the digital context requires digital forensics and cooperation across borders and sectors.

Furthermore, another critical challenge in attributing criminal liability to corporations involved in money laundering derived from online gambling is the weakness of their internal monitoring and compliance systems. Many companies merely fulfill compliance obligations on paper, without genuinely internalizing anti money laundering principles. Additionally, corporations often exploit regulatory loopholes and deficiencies in financial oversight—particularly in fintech, digital wallets, and online banking services—which remain vulnerable to abuse. For example, PT AJP employed foreign based servers and encryption tools to conceal transaction identities, hindering authorities'

ability to trace the flow of illicit funds. This case underscores that in the digital context, corporate criminal accountability demands robust digital forensics and coordinated cooperation across jurisdictions and sectors. Furthermore, another critical challenge in attributing criminal liability to corporations involved in money laundering derived from online gambling is the weakness of their internal monitoring and compliance systems. Many companies merely fulfill compliance obligations on paper, without genuinely internalizing anti money laundering principles. Additionally, corporations often exploit regulatory loopholes and deficiencies in financial oversight particularly in fintech, digital wallets, and online banking services which remain vulnerable to abuse. For example, PT AJP employed foreign based servers and encryption tools to conceal transaction identities, hindering authorities' ability to trace the flow of illicit funds. This case underscores that in the digital context, corporate criminal accountability demands robust digital forensics and coordinated cooperation across jurisdictions and sectors (Saputra, 2021:124-135)

The case of PT AJP further highlights the critical need for synergy among law enforcement, financial institutions, and digital supervisory authorities to uncover corporate-based criminal schemes. Given the digital and decentralized nature of these modus operandi, traditional law enforcement approaches are no longer adequate. Therefore, bolstering Suspicious Transaction Reporting (STR) systems, enhancing investigators capabilities in digital forensics, and refining corporation-focused, risk-based regulatory frameworks are strategic steps toward preventing similar future cases. Academic and policy literature emphasizes that internal compliance weaknesses and regulatory gaps especially in fintech, digital wallets, and online banking facilitate abuse by criminal syndicates. Evidence also suggests that digital forensics is indispensable when predicate offenses are conducted online, yet investigators often face complications due to servers hosted abroad, rapidly changing bank account details, and fabricated credentials

This case study reinforces that corporate criminal liability in the digital age cannot be dissociated from advancing technologies, evolving regulations, and business ethics. Thus, the PT AJP case allows us to conclude that addressing corporate criminal liability in online gambling related money laundering requires a reformulated criminal law approach one that is not merely reactive, but also preventive and adaptive to digital developments. Enforcement must penetrate corporate power structures and dismantle legal façades that have traditionally shielded wrongdoing. The evolution of contemporary crime necessitates a legal system responsive to novel criminal methodologies without compromising justice and legal certainty.

Saputra, Pujiyono, and Purwoto (2021) highlight corporate criminal liability in money laundering cases specifically through their analysis of Decision No. 47/Pid.Sus TPK/2019/PN SMG. They assert that a corporation can qualify as a criminal subject if it fulfills the elements of fault, possesses capacity for responsibility, and lacks any legally recognized excuse for exoneration. Their study further emphasizes the need for more stringent regulations to enhance the effectiveness of enforcing corporate liability, given that corporations are often exploited as instruments of criminal activity. Meanwhile, Ginting, Chandra, and Mau (2022) examine the application of Supreme Court Regulation (Perma) No. 3 of 2016 in corporate money laundering cases. Using a normative juridical approach, they demonstrate the importance of a comprehensive understanding of legal norms and the preparedness of law enforcement agencies in handling the complexity of such cases. Their research highlights how judges and prosecutors can utilize existing legal frameworks to prosecute corporations both effectively and accountably (Yahya, 2020)

Research Methods

In this study, the author employs a normative juridical legal research method. The normative juridical legal research method is an approach used to analyze the law in terms of norms, principles, and written legal rules contained in legislation, as well as prevailing legal doctrine. This approach focuses on examining primary legal materials such as statutes, governmental regulations, and regional bylaws, alongside secondary sources including legal literature, journals, books, and other relevant legal documents. The objective of normative juridical research is to ascertain accurate interpretations of applicable legal provisions and to uncover the underlying legal principles

addressing specific legal issues. In other words, this study does not emphasize the collection of empirical field data but instead relies on a systematic analysis of legal sources to gain deep understanding of legal norms and their application.

In normative juridical research, the initial step involves identifying and gathering relevant legal materials relating to the issue under study. For instance, in research on corporate criminal liability in money laundering from online gambling, the researcher reviews statutes governing money laundering, corporate regulations, and judicial decisions that serve as legal precedents. Additionally, the literature review strengthens the theoretical foundation, incorporating doctrinal analysis and insights from legal scholars. This stage is vital to ensure that the legal examination has a robust basis and is directed toward resolving the specific problem at hand.

After collecting legal materials, the research proceeds with normative analysis systematically examining and interpreting the legal norms within the gathered documents. The purpose of this analysis is to identify applicable legal provisions, elucidate the intent and meaning behind legislative provisions, and assess the relevance of these norms to the problem under investigation. Researchers may apply a systematic approach to delineate relationships among different legal norms, as well as a hermeneutic approach to interpret legal texts in depth and contextually. Accurate interpretation is crucial in normative juridical methods, as it shapes the study's conclusions and informs any legal recommendations.

In addition, normative juridical research also considers unwritten legal norms and general legal principles such as the principles of legality, justice, and legal certainty. This aspect ensures that researchers do not confine themselves solely to positive legal texts but also consider the fundamental values underpinning the law. Consequently, this method provides a comprehensive perspective for understanding and evaluating law both normatively and philosophically. Normative juridical legal research is typically descriptive analytical, wherein the existing legal norms are examined and analyzed to offer clear insights and robust legal argumentation regarding the issues under investigation. In practice, this method is especially well suited for research aimed at developing theoretical legal studies, providing legal opinions, or evaluating legislation and judicial decisions. Because it does not rely on empirical field data, normative juridical research emphasizes the precision of legal interpretation and the ability to systematically analyze and synthesize various legal sources (Listawati, 2021).

Results and Discussion

1) Corporate Criminal Liability in ML from Online Gambling According to Law No. 8 of 2010 and the Elements of ML that are Fulfilled in the Case of PT AJP

Economic crime has undergone a major transformation in the digital era, where the modus operandi of criminals is increasingly sophisticated, structured, and utilizes loopholes in the financial system and information technology. One of the most complex forms of economic crime today is Money Laundering Crime (TPPU) committed by or through corporations. This phenomenon is becoming increasingly striking with the involvement of business entities in accommodating, managing and disguising the proceeds of crime, as happened in the case of PT AJP, a corporation named as a suspect in TPPU from online gambling proceeds by the Directorate of Special Economic Crimes of the Criminal Investigation Unit of the Criminal Investigation Unit of the National Police. In the context of positive law in Indonesia, the handling of corporations that commit ML has gained a firm legal footing, especially after the enactment of Law No. 8/2010 on the Prevention and Eradication of ML. Normatively, corporate criminal liability is regulated through several legal provisions scattered in various laws and regulations, both explicitly in the Anti-Money Laundering Law and principally in the Criminal Code (KUHP) and Supreme Court Regulation (Perma) Number 13 of 2016 concerning Procedures for Handling Criminal Cases by Corporations. In the Anti-Money Laundering Law, specifically Article 6 paragraph (1), it is stated that any person who conceals or disguises the origin of assets known or reasonably suspected of originating from a criminal offense may be subject to money laundering. In this case, what is meant by "person" in the explanation also includes legal entities or corporations. In line with that, Article 7 of the Anti-Money Laundering Law confirms that criminal liability can be imposed on corporations if

the crime is committed by persons acting for and on behalf of the corporation, either alone or jointly (Syakur, 2022: 101-112)

The PT AJP case is a clear example of how corporations are not only a passive means in the flow of illegal funds, but are actually an active instrument in disguising the proceeds of crime. During the period 2020 to 2022, PT AJP received funds from five escrow accounts for online gambling proceeds totaling IDR 40.56 billion, which were then diverted to build and operate Aruss Hotel in Semarang. The use of these funds was consciously intended to provide pseudo-legitimacy to the source of funds derived from gambling offenses. This is in line with the stages in money laundering, namely placement, layering and integration, where funds are inserted into the legal financial system, then rotated through several transactions, and finally "washed" to appear to come from legitimate activities. In this case, the construction and operation of the hotel is a form of integration, which shows the active involvement of the corporation in the ML process. In this context, Article 3 of the Anti-Money Laundering Law becomes very relevant, because it states that every person who places, transfers, spends, donates, entrusts, brings abroad, changes the form, exchanges with currency or securities, or other actions on assets that he knows or reasonably suspects are the proceeds of criminal acts with the aim of disguising the origin, can be subject to a maximum imprisonment of 20 years and a maximum fine of Rp 10 billion. As for corporations, according to Article 7 paragraph (2) of the Anti-Money Laundering Law, a maximum fine of IDR 100 billion can be imposed, as well as additional punishment in the form of revocation of business licenses, dissolution, or confiscation of assets (Saputri, 2021)

It is also important to examine Supreme Court Regulation No. 13/2016 as a technical guideline for law enforcers in determining corporations as perpetrators of criminal acts. This regulation stipulates that in order to convict a corporation, a minimum of two valid pieces of evidence are required to show that the criminal offense was committed for the benefit of the corporation and was committed by the management or a person who has the authority to act on behalf of the corporation. In the case of PT AJP, the involvement of an individual with the initials FH as a commissioner who is also directly involved in the management of funds is a strong basis for investigators to establish corporate criminal liability. This shows the directing mind and will of the corporate management which is a fundamental principle in the theory of corporate criminal liability. From a theoretical perspective, corporate criminal liability in the Indonesian legal system has shifted from a classical approach that only recognizes individual legal subjects to a modern approach that recognizes corporations as subjects of criminal law. This theory is known as the identification theory, which states that the actions and mistakes of high-ranking corporate officials who represent the will of the corporation can be identified as the actions of the corporation itself. Therefore, when FH as the commissioner of PT AJP is proven to channel gambling funds into the company's business activities, the fault is legally also attached to PT AJP as a legal entity.

In the digital era, forms of economic crime including ML from online gambling are increasingly difficult to trace because the perpetrators utilize the anonymity of electronic transactions and cross state legal jurisdictions. Therefore, law enforcement requires synergy between law enforcement officials, financial institutions, and supervisory authorities such as PPATK and OJK. PPATK stands for Financial Transaction Reports and Analysis Center, an independent institution in Indonesia whose main task is to prevent and eradicate money laundering (TPPU) and terrorism financing. This institution was established based on the provisions in Law No. 8/2010 on the Prevention and Eradication of Money Laundering Crimes, which is the legal basis for the implementation of its duties and functions. In the PT AJP case, PPATK's involvement was crucial in detecting suspicious transactions that indicated money laundering activities. The National Police in this case demonstrated a follow the money approach that succeeded in uncovering the flow of funds amounting to Rp 103.27 billion from 15 accounts allegedly related to online gambling. In policy terms, the PT AJP case reflects the government's commitment, especially under President Prabowo Subianto, to eradicate online gambling and ML as part of the development of a clean and equitable economy towards a Golden Indonesia 2045. The eradication of economic crimes is not only aimed at punishing the perpetrators, but also has strategic value to maintain the stability of the financial system, prevent the infiltration of illicit funds into the legal economy, and protect the public interest. In this context, confiscation of assets from the proceeds of crime is part of an unconventional approach in recovering state losses and breaking the cycle of

economic crime. With all its complexities, the PT AJP case provides important lessons for the development of economic criminal law in Indonesia. Strengthening the capacity of law enforcement officials, developing digital transaction tracking technology, and harmonizing banking and ML regulations are imperative so that the Indonesian legal system can adapt to the dynamics of crime in the digital era. In the future, further regulation of digital-based corporate crime is urgently needed, including the company's internal compliance mechanism and the legal responsibility of the management in the corporate financial supervision system (Ja'far, 2024: 8915-8930)

In the case of money laundering (TPPU) that ensnared PT AJP, there are a number of elements in Law Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes that are fulfilled, thus underlying the determination of the company as a corporate suspect. This law comprehensively regulates the act of disguising, hiding, and transferring the proceeds of criminal acts to make them appear legal. Based on Article 3, Article 4, and Article 5 of the Anti- Money Laundering Law, there are three main categories of actions that can be sanctioned, namely: disguise, hide, and use the proceeds of crime. These three elements are evident in PT AJP's modus operandi, where the proceeds of online gambling were diverted and utilized in property investment activities, namely the construction and management of Aruss Hotel in Semarang. This action not only disguises the origin of the funds but also integrates the proceeds of crime into the formal economic system, which is the main characteristic of the money laundering process. Article 3 of the Anti-Money Laundering Law states that every person who places, transfers, spends, donates, entrusts, brings abroad, changes the form, exchanges with currency, securities or other documents, or other actions on assets that he knows or reasonably suspects are the proceeds of a criminal offense, with the aim of hiding or disguising the origin of the assets, can be punished with a maximum imprisonment of 20 years and a maximum fine of Rp 10 billion. In the case of PT AJP, the company received a flow of funds amounting to IDR 40.56 billion from the deposit accounts of online gambling proceeds during the period 2020-2022. These funds were then used to finance hotel business projects, with the aim of making it appear as if they came from legitimate economic activities. These actions clearly fulfill the elements of "spending" and "changing the form" of funds originating from criminal acts, as well as disguising their origin. In this context, FH as a company commissioner has a policy-making capacity and is very likely to have awareness or at least should be suspected of knowing that the funds come from online gambling crimes (Azizah, 2023: 85-98)

Furthermore, Article 4 of the Anti-Money Laundering Law stipulates that every person who conceals or disguises the origin, source, location, allocation, transfer of rights, or actual ownership of assets that he knows or reasonably suspects are derived from criminal acts, is punishable by a maximum imprisonment of 20 years and a maximum fine of Rp 5 billion. The element of concealment and disguise in the PT AJP case can be traced from the financial strategy carried out to cover the traces of illegal funds. The layering and integration process in the money laundering scheme is clearly visible: illicit funds from online gambling are channeled to corporate entities, then used for legal business development, and finally the profits from the business are returned to the original owners through various channels. This mode shows a systematic attempt to disguise the origin of the funds and make them appear as proceeds from legal activities. In fact, further investigation found a direct link between the funds managed by PT AJP and online gambling platforms such as Dafabet, Agen138, and other gambling sites, which strengthens the proof of the element of origin of funds as the proceeds of crime. Article 5 of the Anti-Money Laundering Law regulates the act of using assets that are known or reasonably suspected to be the proceeds of a criminal offense. In this case, PT AJP as a corporate entity used funds originating from online gambling to build and manage Aruss Hotel. The project clearly uses unauthorized funds, which means that the element of "using the proceeds of a criminal offense" has been fulfilled. PT AJP is not only a passive channel, but also actively manages the funds in the context of real business activities, so that corporate criminal responsibility becomes relevant. FH as the commissioner of the company can also be held personally liable for his involvement in directing, approving, or at least knowing the use of the illegal funds.

Systematically, the money laundering process in the PT AJP case has gone through three main stages in the money laundering model: placement, layering, and integration. The placement stage is carried out by putting the gambling proceeds into the company's account. The layering stage occurs when the funds are used to finance the

construction of hotels, which is a legitimate real sector activity. Meanwhile, the integration stage can be seen from the profits obtained by the hotel being channeled back into the accounts of FH and PT AJP, so that the illicit funds appear to have turned into legal funds. This shows that the three stages of money laundering mentioned in the legal literature and in the explanation of the Anti-Money Laundering Law have been fulfilled. In addition to these material offense elements, this case also fulfills the requirements of corporate criminal liability as stipulated in Articles 6 to 10 of the Anti-Money Laundering Law. In this case, PT AJP as a corporation is considered capable of being criminally liable if the criminal offense is committed for the benefit of or on behalf of the corporation, and the act is committed by the management or parties who have the authority to act on behalf of the corporation. This is in line with the principle of strict liability in corporate criminal law, where what is held accountable is not the malicious intent of the corporation as a legal entity, but the acts or omissions of the management or parties acting on behalf of the corporation. In this case, FH as a commissioner has an important position in the managerial structure of PT AJP, so his actions and knowledge related to the flow of illicit funds can be accounted for as corporate misconduct.

It should be emphasized that the Anti-Money Laundering Law also allows criminalization of corporations in the form of fines as stipulated in Article 7. In the context of PT AJP, the National Police has seized assets worth more than Rp 103 billion from the accounts of related companies and individuals, as part of the process of proving and recovering the proceeds of crime. This reflects the implementation of the follow the money and asset recovery principles, which are the main strategies in combating ML. Thus, the successful confiscation of assets is not only a form of punishment, but also an effort to eliminate the economic incentives of the crime and restore potential state losses. It can be concluded that the elements of the crime of money laundering as formulated in Article 3, Article 4, and Article 5 of Law Number 8 Year 2010 are cumulatively fulfilled in the case of PT AJP. The flow of funds from illegal activities (online gambling) that are diverted and managed by corporations, then used to finance the legal business sector, shows all elements of the crime of money laundering ranging from actions, objects, perpetrators, to the intention to hide or disguise the origin of funds. Coupled with the active involvement of FH as a manager who has decision-making capacity in the corporation, the determination of suspect status against PT AJP has a strong legal basis. Therefore, this case is an important precedent in law enforcement against corporations involved in digital economic crimes and shows that law enforcement officials have an adequate juridical framework to ensnare perpetrators who utilize advances in information technology in committing money laundering (Rosyidah, 2021: 1245-1263)

2) Elements of Money Laundering Established in the PT AJP Case under Law No. 8 of 2010 on Money Laundering (UU TPPU)

In the case of money laundering (TPPU) involving PT AJP, several elements of Law No. 8/2010 on the Prevention and Eradication of Money Laundering (UU TPPU) were fulfilled, which provided the legal basis for naming the corporation as a corporate suspect. This law comprehensively regulates actions intended to disguise, conceal, or transfer the proceeds of criminal activity to make them appear legitimate. Under Articles 3, 4, and 5 of the UU TPPU, there are three principal categories of punishable conduct placement, concealment, and use of criminal proceeds. These three elements were manifestly present in PT AJP's modus operandi. Online gambling proceeds were diverted and used to finance property investment activities, specifically the construction and operation of the Hotel Aruss in Semarang.

This conduct not only obscured the origin of the funds but also integrated illicit proceeds into the formal economy characteristic of the money laundering process. According to Article 3 of the UU TPPU, anyone who places, transfers, spends, deposits, carries abroad, alters the form of, or exchanges assets known or reasonably suspected to be proceeds of crime, with the intent of hiding or disguising their origin, is subject to imprisonment for up to 20 years and a fine of up to Rp 10 billion. In PT AJP's case, the company received funds amounting to Rp 40.56 billion from several online gambling escrow accounts during 2020–2022, which were then used to finance the hotel project, to give the appearance that they derived from legitimate economic activity . These actions clearly satisfy the "spending" and "alteration of form" components, as well as the element of concealment of origin. Moreover, FH, as the company's commissioner, held decision-making authority and, at a minimum, is presumed to

have known or should reasonably have known that these funds were generated by online gambling crimes (Azizah,2023: 85-98)

Article 4 of the UU TPPU stipulates that anyone who conceals or disguises the origin, source, location, intended use, transfer of rights, or true ownership of assets that they know, or should reasonably suspect, are proceeds of crime, shall be subject to a maximum of 20 years' imprisonment and a fine of up to IDR 5 billion. The concealment and disguise elements in PT AJP's conduct are evident from the financial strategies designed to obscure the illicit money trail. The layering and integration stages in the money laundering scheme are clear: illicit online gambling funds were routed through a corporate entity, used to finance a legitimate property venture, and subsequently the business profits were channeled back to the original owner through various conduits. This modus operandi demonstrates a systematic effort to conceal the funds' criminal origin and present them as legitimate earnings. Further investigation uncovered direct links between funds managed by PT AJP and online gambling platforms such as Dafabet and Agen138, which reinforce the evidentiary basis for proving the criminal origin of the money (Mahardhika, 2023: 247-262)

Meanwhile, Article 5 of the UU TPPU criminalizes the use of assets that one knows, or should reasonably suspect, to be proceeds of crime. In this case, PT AJP, as a corporate entity, employed these illicit gambling proceeds to build and manage the Hotel Aruss. This constitutes a direct instance of using criminally derived assets, thereby satisfying the "use of criminal proceeds" element. PT AJP was not merely a passive conduit; the company actively managed these funds within the framework of a genuine business operation, thus validating the relevance of corporate criminal liability. Moreover, FH, as the company's commissioner, may be held personally accountable for having directed, approved, or at least known about the use of these illicit funds.

Systematically, the money laundering process in the PT AJP case follows the three primary stages recognized in legal and academic literature placement, layering, and integration. In the placement stage, illicit gambling proceeds were introduced into the financial system via corporate bank accounts. The layering stage occurred when these funds were used to finance the legal construction of a hotel an ostensibly lawful real sector activity. The integration phase became evident when the hotel's profits were redirected back into the accounts of FH and PT AJP, transforming the illicit capital into seemingly legitimate assets. Collectively, these stages precisely reflect the conceptual model of money laundering as defined in both legal doctrine and Law No. 8/2010 on the Prevention and Eradication of Money Laundering.

Beyond the material elements of the predicate offences, the case also satisfies the requirements for corporate criminal liability under Articles 6 to 10 of the UU TPPU. PT AJP as a corporation is liable if the crime is committed in its name or for its benefit and executed by its management or agents with delegated authority. This aligns with the strict liability principle in corporate criminal law, wherein the corporation's responsibility arises not from its abstract intent, but from the actions or omissions of its authorized representatives. In this instance, FH, as the company's commissioner, occupied a critical managerial position; accordingly, his knowledge of and involvement in the illicit fund flows directly implicates corporate fault. It should be emphasized that the UU TPPU (Law No. 8/2010) also permits the imposition of corporate fines under Article 7. In the PT AJP case, the Indonesian National Police (Polri) seized assets worth over IDR 103 billion from corporate and related individual bank accounts, as part of the evidentiary process and efforts to recover proceeds of crime. This operation reflects the implementation of the "follow the money" principle and asset recovery strategies core tactics in countering money laundering.

Thus, successful asset seizure not only constitutes punitive action but also serves to eliminate the economic incentives for crime and restore potential losses to the state. Consequently, the material elements of money laundering as outlined in Articles 3, 4, and 5 of UU No. 8/2010 are cumulatively fulfilled in the PT AJP case. The flow of illicit funds from online gambling, diverted and managed by the corporation to finance legitimate business operations, demonstrates all elements of money laundering from the criminal act itself to the object, actors, and the intent to conceal or disguise the origin of the funds. Further, with the active involvement of FH, who holds decision-making power within the corporation, the designation of PT AJP as a suspect rest on a solid legal foundation. As such, this case sets an important precedent in prosecuting corporations implicated in digital economic crimes and

demonstrates that law enforcement officers possess an adequate juridical framework to hold wrongdoers accountable, even when they exploit advancements in information technology for money laundering (Rosyidah, 2021: 1245-1263)

3) Challenges and Prospects of Law Enforcement Against Corporations in Digital-Based Money Laundering Cases in Indonesia, and the Implementation of Asset Seizure as a Strategy for State Financial Recovery

Law enforcement against money laundering (TPPU) committed by digital-based corporations in Indonesia faces various structural and technical challenges that require a more adaptive legal approach. Along with the advancement of information technology and the digital economy, the nature of crimes has also evolved to become more complex, transnational, and multi-actor. The case of PT AJP serves as concrete evidence that corporations are not merely civil law subjects but can also be held criminally liable. The modus operandi of disguising proceeds from online gambling through investment in the construction of Hotel Aruss represents a sophisticated and structured form of money laundering, involving layering and integration strategies to obscure the illicit origins of the funds. This highlights the urgency of strengthening corporate criminal law and utilizing asset recovery instruments as part of a comprehensive criminal justice system (Gemilang, 2024: 8455-8471)

In terms of challenges, the enforcement of law against corporations in TPPU cases faces obstacles particularly in proving corporate criminal liability. As stipulated in Articles 7 and 9 of Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering Crimes (TPPU Law), a corporation can be held criminally liable if it is proven that the crime was committed for the benefit of the corporation by its management, either directly or indirectly. However, in practice, establishing a causal link between the actions of individuals (in this case, FH as commissioner) and the corporation is often hindered by the lack of internal administrative evidence, document manipulation, and the complex, labyrinthine structure of corporate organizations.

In addition, significant technical challenges arise from the use of financial technology (fintech), digital payment systems, and bank accounts under nominee names, which complicate the tracing of fund flows. The existence of cross-border digital transactions, use of cryptocurrency, and tax avoidance through tax haven jurisdictions further hinder law enforcement in tracking financial trails. In the PT AJP case, it was found that IDR 40.56 billion derived from online gambling activities was diverted into the hospitality sector as part of a money laundering scheme. The laundering process involved channeling funds into the company's accounts and subsequently integrating them into legal business operations. This demonstrates that money laundering is not limited to asset storage but also involves transforming illicit assets into legitimate economic forms.

Future prospects for law enforcement require improvements in two key areas: first, enhancing the capacity of law enforcement institutions to understand digital crime modes; and second, reforming corporate criminal law frameworks to adapt to the patterns of global economic crime. Indonesia has taken positive steps by regulating corporate criminal liability in various sectoral laws, including the TPPU Law. However, to address digital corporations that lack physical form or operate transnationally, a more holistic and transnational legal reform is necessary—such as through the ratification of international conventions like the United Nations Convention against Transnational Organized Crime (UNTOC) and the strengthening of mutual legal assistance (MLA) cooperation with other countries.

The effectiveness of asset seizure as a strategy for recovering state finances in digital-based TPPU cases, as exemplified by the PT AJP case, has shown significant results. The seizure of IDR 103.27 billion from various accounts belonging to PT AJP and FH demonstrates that law enforcement is not only aimed at punishing perpetrators but also at returning the proceeds of crime to the state or victims. Pursuant to Article 38C of the TPPU Law, asset seizure may be conducted on any wealth suspected to originate from a criminal act, even prior to court proceedings (provisional seizure). This strategy is crucial as assets derived from digital crimes can be quickly transferred, concealed, or dissipated. Hence, early seizure and asset freezing are preventive measures to ensure that assets are not lost or exhausted by the perpetrators.

Nonetheless, the effectiveness of asset seizure does not solely depend on the technical capabilities of law enforcement but also on inter-agency collaboration and legal systems that support swift and accountable asset recovery. In this context, the roles of the Financial Transaction Reports and Analysis Center (PPATK), the Financial

Services Authority (OJK), and the Directorate General of Taxes are critical in detecting suspicious transactions and conducting financial analyses that serve as the basis for legal action. Such inter-agency collaboration creates an effective national financial intelligence system to support investigations and seizures.

The asset seizure in the PT AJP case also underscores the importance of the follow the money approach in economic crimes. This principle emphasizes that law enforcement must follow the flow of funds wherever they move, rather than solely focusing on the perpetrator. In this case, not only was FH as an individual subject to investigation, but PT AJP as a legal entity was also held accountable. This principle aligns with Article 77A of the revised Criminal Procedure Code (KUHAP), which broadens the scope for asset seizure and confiscation through non-conviction based forfeiture—namely, when the perpetrator cannot be found or has died, but the asset can be proven to originate from a crime.

From a prospective standpoint, Indonesia has considerable potential to develop an effective law enforcement system against digital-based corporate TPPU, provided that regulatory strengthening, advanced fund-tracing technologies, and international cooperation are implemented. One concrete prospect is the formation of a cross-agency task force focused on digital economic crimes and integrated with a real-time financial transaction monitoring system. Strengthening digital forensics and training officers to analyze blockchain, crypto-assets, and alternative financial systems are also imperative. Furthermore, revising the TPPU Law to accommodate the definition of digital assets as crime objects would be a significant future breakthrough.

As part of the national policy towards Indonesia Emas 2045, asset recovery through seizure in digital-based TPPU cases is a vital instrument to reinforce the integrity of the national economy. The efforts of the National Police in seizing PT AJP's assets reflect that this strategy is not only legally effective but also creates a deterrent effect and maintains public trust in the financial system. However, for this strategy to be sustainable, improvements in the management of seized assets, transparency in asset distribution, and re-utilization of assets for public interests such as education, healthcare, and economic development are necessary. The PT AJP case illustrates both the challenges and prospects of enforcing laws against corporate TPPU in the digital era. Asset seizure has proven to be an effective strategy in breaking the cycle of economic crime and restoring state losses. However, this effectiveness must be supported by a responsive legal system, advanced technologies, and solid inter-agency cooperation. Law enforcement should not only aim to impose punishment, but also to restore economic justice and build a clean and sustainable financial system (Iskandar, 2022: 51-59).

Conclusions

Based on the discussion regarding corporate criminal liability in money laundering offenses originating from online gambling activities, particularly in the case of PT AJP, it can be concluded that Indonesia's positive law provides a sufficiently robust legal framework to prosecute corporations as perpetrators of economic crimes. Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes explicitly allows for the imposition of criminal liability on legal entities, a provision further reinforced by Supreme Court Regulation Number 13 of 2016. In the PT AJP case, the criminal elements stipulated in Articles 3, 4, and 5 of the Money Laundering Law were proven to be fulfilled, including acts of disguising, concealing, and utilizing proceeds from online gambling crimes. The corporation's action of channeling IDR 40.56 billion to construct and operate a hotel demonstrates active involvement in the money laundering process, encompassing all stages of placement, layering, and integration. The designation of PT AJP as a suspect also reflects the application of the principles of strict liability and corporate criminal liability, which permit the imposition of sanctions even if the corporation, as a legal subject, does not possess intent in the same manner as natural persons. Liability can instead be established through the actions of corporate executives, such as FH in his role as commissioner.

References

Ahuja, D., Bhardwaj, P., & Madan, P. (2023). Money laundering: A bibliometric review of three decades from

1990 to 2021. *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy*, *110*, 55-72.

Azizah, H., Santoso, T., Husein, Y., Mulyadi, M., & Sofian, A. (2023). Follow Up Crime dalam Tindak Pidana Pencucian Uang di Indonesia dan Malaysia. *Halu Oleo Law Review*, *7*(1), 85-98.

Duncan, P., & Lord, N. (2022). Organized crime money laundering through online gambling businesses in Great Britain. In *The Private Sector and Organized Crime* (pp. 195-209). Routledge.

Gemilang, G., Ismaidar, I., & Zarzani, T. R. (2024). Pertanggungjawaban Pidana Korporasi dalam Tindak Pidana Pencucian Uang. *Innovative: Journal Of Social Science Research*, *4*(2), 8455-8471.

Ginting, B. B., Chandra, T. Y., & Mau, H. A. (2022). Pertanggungjawaban korporasi dalam tindak pidana pencucian uang. *SALAM: Jurnal Sosial dan Budaya Syar-i*, *9*(4), 1223-1234.

Gupta, A., Dwivedi, D. N., & Shah, J. (2023). Overview of money laundering. In *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance* (pp. 1-11). Singapore: Springer Nature Singapore.

Iskandar, M. A. (2022). Pertanggungjawaban Pidana Korporasi Sebagai Subjek Tindak Pidana Pencucian Uang. *PALAR (Pakuan Law review)*, *8*(4), 51-59.

Ismail, I., Fahamsyah, E., & Suarda, I. G. W. (2021). Kewajiban Notaris Mengenali Pengguna Jasa dalam Upaya Pencegahan Tindak Pidana Pencucian Uang oleh Korporasi. *Syntax Idea*, *3*(10), 2131-2147.

Ja'far, M. N. (2024). Perbandingan Pertanggungjawaban Pidana Korporasi Terhadap Tindak Pidana Pencucian Uang Dengan Predicate Crime Korupsi Di Indonesia Dan Malaysia. *Dinamika*, *30*(1), 8915-8930.

Jayaningprang, H. (2023). *Analisis Pertanggungjawaban Pidana Korporasi Terhadap Tindak Pidana Pencucian Uang Yang Berasal Dari Tindak Pidana Korupsi* (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).

Ketcheson, R. (2022). Online Gaming: A Good Bet for Money Laundering? An Analysis of Money Laundering in the Canadian Online Gaming Industry. *UNLV Gaming LJ*, *13*, 21.

Kurniawan, K. D., & Hapsari, D. R. I. (2022). Pertanggungjawaban pidana korporasi menurut vicarious liability theory. *Jurnal Hukum Ius Quia Iustum*, *29*(2), 324-346.

Lin, C. H., & Shih, C. H. (2024). A case study on the Online Gambling industry in Taiwan. *Procedia Computer Science*, *246*, 4552-4562.

Listawati, L. (2021). Pertanggungjawaban Pidana Korporasi Pada Perkara Tindak Pidana Pencucian Uang. *Justitia et Pax*, *37*(2).

Mahardhika, V. (2023). Tindak Pidana Pencucian Uang Klasifikasi Dan Bentuk Sanksi Pidana Bagi Korporasi. *HUKMY: Jurnal Hukum*, *3*(1), 247-262.

Nimma, S. (2022). Money laundering in the cyberworld: emerging trends. *Part 1 Indian J. Integrated Rsch. L.*, *2*, 1.

Page, B. (2024). Remote Gaming and Organized Crime: Applying the ICH Organizational Structure to the Gambling Industry to Combat Money Laundering and Match-Fixing. *Geo. Wash. Int'l L. Rev.*, *55*, 99.

Rosyidah, H., Ndharma, B. S., & Zulfa, N. A. (2021). Inkonsistensi Aturan Pertanggungjawaban Pidana Pencucian Uang Oleh Korporasi: Perlukah Reformulasi?. *Jurnal Hukum Lex Generalis*, *2*(12), 1245-1263.

Saputra, F. R., Pujiyono, P., & Purwoto, P. (2021). Pertanggungjawaban Korporasi Dalam Tindak Pidana Pencucian Uang (Studi Putusan No. 47/Pid. Sus-Tpk/2019/Pnsmg). *Diponegoro Law Journal*, *10*(1), 124-135.

Saputri, O. (2021). Pertanggungjawaban Pidana Partai Politik Dalam Tindak Pidana Pencucian Uang. *Lex Lata*.

Senjaya, M. (2022). Law enforcement of the crime of money laundering that comes from online gambling. *International Journal of Social Science*, *2*(3), 1641-1650.

Supriadi, D. A., & SH, M. (2021). *Kecelakaan Lalu Lintas dan Pertanggungjawaban Pidana Korporasi: dalam Perspektip Hukum Pidana Indonesia*. Penerbit Alumni.

Syakur, S. (2022). Pertanggungjawaban pidana oleh pemilik manfaat (beneficial owner) sebagai pelaku pencucian uang dan kejahatan lainnya dalam perseroan terbatas. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing Terrorism*, *1*(1), 101-112.

Tomic, S. (2022). Regulatory approach to anti-money laundering in online gambling in the UK. In *Financial Technology and the Law: Combating Financial Crime* (pp. 47-65). Cham: Springer International Publishing.

UANG, P. (2021). Pertanggungjawaban pidana korporasi.

Wronka, C. (2022). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*(2), 330-344.