NURANI:
JURNAL KAJIAN SYARI'AH DAN MASYARAKAT
VOLUME 25. NO. 1. JUNE 2025
website: http://jurnal.radenfatah.ac.id/index.php/Nurani Email: jurnalnurani@radenfatah.ac.id
E-ISSN: 2460-9102 P-ISSN: 1693-8437

Legal Challenges of Asset Misappropriation in the Digital Era

Emiliya Febriyani,[1] Tantimin[2]
Faculty of Law, Universitas Internasional Batam, Indonesia[1,2]
Email: emiliya@uib.ac.id

Keywords: *Asset misappropriation; Corporate governance; Criminal law; Digital era.*

DOI: https://doi.org/10.19109/nurani.v25i1.26821

Submitted: December 18, 2024

Accepted: April 15, 2025

Published: May 12, 2025

Pages: 141 - 156

Abstract: *The growing challenges of addressing asset misappropriation in Indonesia's digital era highlight the need for a thorough examination of the existing legal framework to assess its effectiveness and adaptability. This paper examines legal challenges of digital asset misappropriation in Indonesia. It explores the legal implications of asset misappropriation as a crime within the context of digital technology, analyzing current Indonesian legislation's adequacy in addressing these issues. Employing a normative legal research method and statutory approach, this research investigates relevant laws and regulations in Indonesia that can be used to criminalize asset misappropriation. In addition, this study employs a case approach by analyzing court decisions related to asset misappropriation, providing practical insights into how the legal framework is applied in real-world scenarios. Key findings suggest that while current Indonesian legislation addresses various aspects of asset misappropriation, it lacks specific provisions for the digital context. This gap necessitates a more holistic legal approach that integrates both traditional and digital environments, while also acknowledging the legal implications on digital aspects, namely data as the center of focus. Recognizing asset misappropriation as a distinct criminal offense can serve as a foundational step in criminalization efforts. This approach can then be integrated with existing legal provisions relevant to the digital environment, allowing perpetrators to be prosecuted under multiple dimensions of Indonesia's legal framework for more comprehensive enforcement.*

Introduction

Digital transformation has fundamentally reshaped perspectives on various aspects of life, including **asset management** and **corporate governance**, by introducing new technologies, risks, and regulatory challenges (Ahn, 2014). In the rapidly evolving landscape of digital technology, asset misappropriation has emerged as one of significant concern for businesses and many legal systems around the world (Mat Ridzuan et al., 2022). As a developing nation with a rapidly expanding digital economy (Margiansyah, 2020), Indonesia faces unique challenges in addressing asset misappropriation within its legal framework. This paper explores the legal challenges associated with asset misappropriation in the digital era from an Indonesian perspective, highlighting the complexities that emerge when traditional legal concepts intersect with modern technological advancements.

The theoretical foundations of asset misappropriation are deeply rooted in property law and criminal jurisprudence, reflecting the legal principles that govern ownership rights, fiduciary duties, and the criminalization of unlawful

asset transfers. However, the digital realm introduces novel considerations that challenge established legal principles. Along with the introduction of many forms of digital assets, traditional asset managements and records are increasingly integrated into many digital systems, to help many corporations in managing them. This does not always take the form of complex digital system like digital rights management (DRM) (Ding, 2023). Instead, asset managements in the digital context can take many simpler forms such as sensitive corporate data saved in cloud storage (Ofori-Duodu, 2019), local servers, or physical electronic storage device, and digital financial records managed using certain a third-party fintech system (Haberly et al., 2019). This paper will analyze how Indonesia's legal framework currently addresses these challenges and identify potential areas for reform to enhance the protection of digital assets and strengthen measures against asset misappropriation in the digital age.

The implications of this research go beyond legal theory, potentially influencing Indonesia's economy and the corporate finance landscape by shaping policies that enhance investment security, corporate governance, and digital asset protection. As the country strives to position itself as a hub for digital innovation and investment (Rachman et al., 2024), the robustness of its legal system in addressing asset misappropriation becomes a topic of heightened importance. A comprehensive understanding of the legal challenges in this domain can inform policy decisions, enhance investor confidence, and contribute to the overall stability and growth of Indonesia's digital economy. Moreover, it may provide insights into how corporate governance structures and financial practices need to evolve to mitigate the risks associated with digital asset misappropriation. A broader implication of this study is its potential to shed light on the interplay between technological advancement and corporate governance, particularly in the context of legal development. This relationship underscores the need for regulatory frameworks that adapt to the evolving digital landscape while ensuring effective corporate oversight and accountability.

Rather than focusing exclusively on digital assets, this paper adopts a broader perspective on the general concept of assets, encompassing both traditional and digital forms. It explores how these assets are managed within the digital space, utilizing relevant technologies and systems, while examining their legal implications. The main domain of law of this research is ultimately criminal law, but branches of analysis might overlap with other domains of laws, particularly those that are highly relevant in the digital age, such as data protection, fintech governance, and intellectual property law. Recognizing the connections between these areas is essential for building a foundational understanding of the complexities surrounding asset misappropriation, particularly in the contexts of corporate governance and criminal law.

Asset misappropriation has been recognized as a prominent type of fraud that has garnered significant global attention, as highlighted in various studies (Utami et al., 2021). The study also found that financial pressure, opportunity, and individual capability were found to have significant positive effects on the occurrence of asset misappropriation. However, the same study indicated that non-financial pressure and integrity did not demonstrate a

significant impact on asset misappropriation incidents. Another study supported some of these findings, using fraud hexagon theory to examine factors influencing employee asset misappropriation at an Indonesian hospital (Wahyulistyo & Cahyonowati, 2023), using data from 218 employees, it finds that financial pressure, opportunity, ability, ego, and collusion positively affect misappropriation tendencies, while job pressure and seniority attitude do not show significant impacts. The gap in these studies stems from their focus on different organizational contexts, with none specifically examining the legal challenges of asset misappropriation within the digital landscape.

In the context of corporate governance, research has shown that internal controls within corporations play a crucial role in preventing asset misappropriation (Ramadlan et al., 2020). The study examines fraud star components and organizational commitment's effects on asset misappropriation, with internal control as a moderator. Using data from 71 employees, it finds opportunity significantly influences asset misappropriation, while other factors show no significant impact. Internal control is helpful in moderating relationships between opportunity, ability, and asset misappropriation. From the purely digital context, a study found that digital technologies can be utilized to analyze to detect some of the practices of asset misappropriation (Nomorissa & Suryadithya, 2022). This study explores how Forensic Data Analytics (FDA) can be used to detect fraud by analyzing Big Data. It identifies three main types of fraud in companies: asset misappropriation, fraudulent statements, and corruption. The research suggests that specific Fraud Detection and Analysis (FDA) tools, such as database forensics, email analysis, and memory forensics, can be utilized to identify different types of fraud by filtering and analyzing relevant data from Big Data sources.

Despite ongoing developments in the literature on asset misappropriation, a significant gap remains in analyzing the legal framework that defines and addresses it as a crime, particularly within the digital context. Filling this research gap is crucial in understanding the interplay between asset misappropriation done using digital technologies, particularly within the Indonesian perspective. This research narrows its focus on filling this gap by analyzing the legal norms within the relevant legal frameworks, to understand the legal implications of asset misappropriation in the digital context, and how such act can be criminalized to ensure better corporate governance and ultimately promote better growth in the Indonesian economic system. This study's main objectives are exploring the legal implications of asset misappropriation in Indonesia and assess the relevant legal frameworks' adequacy in tackling asset misappropriation as a crime. Examining these aspects can provide valuable insights into the effectiveness of existing legal frameworks in addressing this financial crime. These insights can serve as a foundation for future legal reforms aimed at enhancing regulatory measures and enforcement strategies.

Method

This research employs the normative legal research method to identify and analyze legal norms within the existing positive laws, providing a structured understanding of how asset misappropriation is addressed within the legal framework (Disemadi, 2022). Typically, a normative analysis, at least in its pure form, involves the identification and comprehensive analysis of primary law sources as secondary data, to be used as the basis of understanding a particular legal problem (Tan, 2021). The focus on analyzing legal norms make this research method suitable for this research, as it can better equip the analysis of certain provisions that can be utilized to criminalize asset misappropriation. Secondary data employed by this research are Law No. 40 of 2007 on Limited Liability Companies, Law No. 8 of 2011 on Electronic Information and Transaction, Law No. 19 of 2016 on Amendment to Law No. 11/2008 on Electronic Information and Transactions, Law No. 1 of 2024 on Second Amendment to Law No. 11/2008 on Electronic Information and Transactions, and Law No. 27 of 2022 on Personal Data Protection. This study also incorporates primary sources, specifically an asset misappropriation case law in Indonesia, focusing on Tax Court Decision No. PUT-008299.19/2022/PP/M.XVIIA of 2023 as a key reference for legal analysis.

Results and Discussion

Criminal Dimensions of Asset Misappropriation

At its core, asset misappropriation refers to the unauthorized use or theft of an organization's assets for personal benefit (Melinda et al., 2022). Conceptually, it encompasses a rather wide range of activities, from the physical theft of inventory to the manipulation of financial records. Conceptually, asset misappropriation can be defined as an illegal use of assets by someone who is given the responsibility to manage or oversee the assets (Syahria, 2019). This definition provides the basic understanding of what asset misappropriation is by highlighting the nature of asset misappropriation, which revolves around unauthorized exploitation of company resources. However, the full legal nuance of this act might not have been properly covered, particularly the illicit and self-serving nature of it. The intent behind asset misappropriation can be understood through the Fraud Diamond Theory, which identifies four key elements: incentive, pressure, rationalization, and ability. These factors collectively influence an individual's likelihood of engaging in fraudulent activities (Çollaku et al., 2024).

From a legal perspective, asset misappropriation generally consists of three key elements: (1) unauthorized taking or use of an asset, (2) intent to deprive the rightful owner, and (3) conversion of the asset for personal benefit. These elements establish the basis for legal accountability in cases of misappropriation (Bakri et al., 2017). These elements form the basis for criminal prosecution in many jurisdictions, although the specific legal terminology and treatment may vary. These three aspects are essential as they crucially highlight the entirety of the legal nuance of asset misappropriation, while also projecting certain legal implications, such as financial loss and other possible damages to a company. These fundamental elements are crucial in

linking asset misappropriation to relevant legal frameworks, particularly criminal provisions. Establishing this connection ensures that companies whose assets have been misappropriated can seek legal remedies, while also enabling the prosecution and punishment of those responsible for the illicit act.

In a corporate setting, asset misappropriation is commonly seen as a type of occupational fraud. It can occur in different ways, such as skimming, where cash is stolen before being recorded in the accounting system, fraudulent disbursements, which include schemes like fake billing or payroll fraud, and the theft of non-cash assets, such as inventory or company property (Kassem, 2014). The severity of asset misappropriation can range from minor theft to large-scale embezzlement schemes that can significantly impact an organization's financial health. It's also important to highlight the distinction provided by the theoretical framework provided by the corporate context, which is damage to organization. Since asset misappropriation does not directly result in financial harm to the state, it is not governed by corruption laws (Kharisma, Putra, and Hidayah, 2021). These laws primarily focus on illicit schemes that financially damage the country by viewing illegal financial gains as misused taxpayer money, which should have been allocated for the benefit of the broader community (Yustia & Arifin, 2023).

The digital era has added new layers of complexity to the issue of asset misappropriation. As organizations adapt to digital transformation, corporate activities are becoming increasingly digitalized, leveraging various technological tools to manage assets, financial transactions, and operational processes. This shift presents both opportunities and challenges, particularly in safeguarding assets from fraudulent activities within a rapidly evolving digital landscape (Aldboush & Ferdous, 2023). While this can offer more productivity, it can also open the doors to possible asset misappropriation practices, as corporate personnel behind some of the key accounting or asset management activities can manipulate the data input or other aspects of corporate asset that are saved or managed within the digital environment. This also involves digital assets such as customer databases and intellectual properties (Lehavi, 2019). The integration of complex digital systems in corporate operations can obscure traditional audit trails, making it much more difficult for organizations and law enforcement to detect and verify instances of asset misappropriation. This technological shift introduces new challenges in tracking financial irregularities, as digital transactions often lack the transparency and traceability of traditional paper-based records.

In the digital context, asset misappropriation can take on various forms, often leveraging technology to obscure fraudulent activities. These may include unauthorized fund transfers, data manipulation, digital invoice fraud, or cyber-enabled embezzlement, all of which exploit digital systems to misappropriate assets without immediate detection. These may include unauthorized access to sensitive data, theft of proprietary information or trade secrets, manipulation of digital financial records, or misuse of computing resources. Due to the data-driven nature of digital technology, asset misappropriation within the digital context typically involves the effort to cover the digital tracks associated with the illicit act, primarily through various forms of data manipulation. These techniques include automated scripts to alter or delete logs, targeted log

manipulation to remove specific entries, and the use of rootkits or custom malware to conceal these actions.

The Criminal Law Code serves a vital role in establishing fundamental provisions for criminalizing acts considered harmful or disruptive to the peace and stability of Indonesian society. The rationale for utilizing the Criminal Law Code in the context of corporate governance and asset misappropriation comes from Article 155 of Law No. 40 of 2007 on Limited Liability Companies, which governs that, "The provisions regarding the liability of the Board of Directors and/or the Board of Commissioners for their errors and omissions stipulated in this Law shall not prejudice the provisions stipulated in the Law on Criminal Law." While the Criminal Code does not explicitly define "asset misappropriation," several articles can be interpreted to address different aspects of this offense, as outlined in Table 1 below:

Table 1. Relevant Provisions Within the Criminal Law Code

Legal Norms	Provisions	Relevancy
Theft [Article 362]	Any person who takes property belonging wholly or partially to another, with the intent to unlawfully appropriate it, shall be guilty of theft, and shall be punished by a maximum imprisonment of five years or a maximum fine of sixty rupiahs.	Can be applied to physical or digital asset theft
Embezzlement [Article 372)	Any person who deliberately and unlawfully appropriates property which belongs in whole or in part to another, but which is in his power other than by reason of crime, shall, being guilty of embezzlement, shall be subject to a maximum imprisonment of four years or a maximum fine of sixty rupiahs.	Relevant for misuse of entrusted assets
Fraud [Article 378]	Any person who with intent to unlawfully benefit himself or another, by assuming a false name or a false capacity, by deception or by a web of lies, induces someone to hand over any property or to contract a loan or to cancel an outstanding debt, shall, being guilty of fraud, be punished by a maximum imprisonment of four years.	Applicable in cases involving deception.

Destruction of property [Article 406]	Any person who unlawfully and deliberately destroys, damages, renders useless or mislays any property which wholly or partially belongs to another, shall be punished by a maximum imprisonment of two years and eight months or a maximum fine of three hundred rupiahs.	May also be applicable to **tampering with digital assets**.
Document forgery [Article 263]	Any person who makes a false document or falsifies a document which can give rise to a right, an engagement or a release from a debt, or which is intended to serve as evidence of a fact, with the intent to use or to cause others to use said document as if it were genuine and not falsified, shall, if such use can cause any loss, be punished by a maximum imprisonment of six years.	Could relate to falsifying digital records

Source: Primary Law (Criminal Law Code)

These provisions in the KUHP, as outlined in Table 1 above, serve as the legal basis for addressing cases of asset misappropriation and confiscation. Unfortunately, these provisions do not create a distinction on what asset misappropriation is, and covering only the aspects that make up an asset misappropriation, such as theft, embezzlement, fraud, destruction of property, and document forgery. Due to this problem, the application of these problems within the digital contexts may present challenges due to the unique nature of digital assets and the methods used to misappropriate them. From a criminal law perspective, this issue reveals a potential gap that must be thoroughly addressed to effectively combat asset misappropriation in the digital era.

A specific case law can offer valuable insights into the complexity of legal norms surrounding asset misappropriation, demonstrating how a single case can encompass multiple legal aspects of this offense. PUT-008299.19/2022/PP/M.XVIIA of 2023 addresses a case of asset misappropriation involving the theft of raw materials with import duty exemption facilities. This incident occurred due to a conspiracy between several company employees from the purchasing, warehouse, and production departments and an external fence who was a recognized partner for scrap disposal. The scheme involved the purchasing department recording inflated purchase data, the warehouse department acknowledging receipt of goods not fully received, and the production department inflating raw material usage while underreporting output. An internal audit uncovered these irregularities, revealing a discrepancy between purchased raw materials and production output. Following an appeal by the company, the Tax Court reduced a portion of the administrative sanctions initially imposed. This case underscores the

vulnerabilities in company operations that can be exploited for asset misappropriation, along with the legal consequences and the appeals process that may follow (Widjaja & Budiman, 2024).

Based on the description of the asset misappropriation case, the most relevant legal norms from Table 1 of this research paper include theft, along with other applicable provisions addressing fraud, embezzlement, and misuse of authority (Article 362), which directly addresses the core criminal act of unlawfully taking the company's raw materials for personal gain. Furthermore, the deceptive actions undertaken by the employees, such as manipulating records to conceal the theft, fall under the purview of Fraud (Article 378). Embezzlement (Article 372) is also applicable in this scenario, as the employees, who were entrusted with the company's assets as part of their roles, misappropriated those assets for their own benefit. Lastly, the likely falsification of purchase data, warehouse receipts, and production records to facilitate and cover up the misappropriation aligns with the legal norm of Document forgery (Article 263). This case law illustrates the complex nature of asset misappropriation. Despite its seemingly straightforward criminal dimension, it can involve multiple criminal aspects, potentially resulting in multiple charges under different legal provisions.

Electronic Transactions Laws

Indonesia has made efforts to integrate digital technology advancements into its legal framework by recognizing the role of electronic information and transactions in the evolving digital landscape. Law No. 8 of 2011 on Electronic Information and Transaction (EIT Law) became the first manifestation of this effort, marking Indonesia’s first comprehensive step into the dynamic and then unknown digital realm (Kharisma, 2022). The law provides some of the key provisions regarding the utilization of electronic systems, by providing legal certainties in key areas such as data, commercialization, documentation, and even conducts within the digital space. The enactment of this law marked Indonesia's commitment to adapting its legal system to address the challenges posed by digital transformation.

From a historical perspective, this commitment can be seen as somewhat delayed, especially considering that digital transformation began gaining attention in the 1980s, a time when only 1% of the world's technologically stored information was in digital format (Hilbert, 2020), is taken into account. Past 2010, digital transformation received an unprecedented level of momentum with technology like artificial intelligence (AI) receiving as much as $12.7 billion in 2015 to $67.9 billion in 2020 (Ing et al., 2022). This chronological indication shows that Indonesia, with the EIT Law, entered the race to adapt to digital transformation in a phase where it has become rather advanced with novel technology like machine learning getting considerable amount of boost financially in many research and development settings. This delay in legislative response reflects the challenges faced by many developing nations in adapting to the rapid pace of technological change (Shibambu, 2024). Therefore, it is reasonable to expect noticeable lags in the development of relevant legal frameworks in Indonesia, particularly in

the areas of corporate governance and, more specifically, asset misappropriation.

The delayed introduction of the EIT Law faced the challenging task of not only providing a framework for future digital developments but also retroactively addressing established practices and ensuring they align with evolving technological realities. EIT Law provides certain provisions that can be used to criminalize the act of asset misappropriation, as highlighted in the table 2 below:

Table 2. Relevant Provisions in the EIT Law

Legal Norms	Provisions	Application
Unauthorized access [Article 30 (1)]	Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems owned by other Persons in any manner whatsoever.	Could apply to accessing digital assets without permission
Alteration of electronic information [Article 32 (1)]	Any Person who knowingly and without authority or unlawfully in any manner whatsoever alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Documents owned by other Persons or owned by the public.	Pertinent to the alteration of digital financial records or other electronic assets.
Creation of false electronic information [Article 35]	Any Person who knowingly and without authority or unlawfully manipulates, creates, alters, deletes, destroys Electronic Information and/or Electronic Documents with the intent that such Electronic Information and/or Electronic Documents would seem as if they were authentic data.	Could apply to falsifying digital records related to assets
Causing damages to other people/entity through electronic systems [Article 36]	Any Person who knowingly and without authority or unlawfully commits the acts as intended by Article 27 through Article 34 that causes losses to other persons.	Broad provision that could cover various forms of digital asset misappropriation

Source: Primary Law (Law No. 11 of 2008)

Similar to the Criminal Law Code, the EIT Law lacks specific provisions that explicitly address asset misappropriation as a distinct criminal offense. Article 30 paragraph (1) could be applied to cases where digital assets are accessed without proper authorization as part of a misappropriation scheme, due to its primary focus on unauthorized access. Article 32 paragraph (1) is particularly relevant, as it covers a wide range of actions that could be involved in digital asset misappropriation, such as altering financial records or moving electronic documents without authorization. Article 35 addresses the creation of false electronic information, which could be crucial in prosecuting cases where digital assets are misrepresented or falsified. Lastly, Article 36 serves as a catch-all provision that could potentially cover various forms of asset misappropriation that result in financial losses. However, it's important to note that these provisions are not specifically tailored to asset misappropriation, which could lead to challenges in their application to complex cases involving sophisticated digital financial manipulations or misuse of intangible digital assets. The broad scope of these provisions, while allowing for flexibility, may also lead to challenges in interpretation when dealing with specific cases of corporate asset misappropriation in a digital setting.

Indonesia has also sought to integrate more of the changes brought about by digital transformation into the EIT legal framework, by introducing amendments with Law No. 19 of 2016 on Amendment to Law No. 11/2008 on Electronic Information and Transactions and Law No. 1 of 2024 on Second Amendment to Law No. 11/2008 on Electronic Information and Transactions. The revisions relevant to asset misappropriation are as per table 3 below:

Table 3. EIT Law Framework Developments in the Context of Asset Misappropriation

Revision	Changes Relevant to Asset Misappropriation
First Revision (Law No. 19 of 2016)	No significant changes directly addressing asset misappropriation
Second Revision (Law No. 1 of 2024)	Article 43(5)(l): Expanded investigative authority enables officials to temporarily suspend access to social media accounts, bank accounts, electronic funds, and digital assets.

Source: Primary law (Law No. 19 of 2016 and Law No. 1 of 2024)

Upon reviewing the two revisions presented in Table 3, it is evident that the amendments to the EIT Law have not significantly tackled the specific issue of asset misappropriation in the digital realm. The first revision in 2016 did not introduce any changes directly relevant to this area. The second revision in 2024, while expanding investigative powers that could potentially be applied in asset misappropriation cases, does not explicitly target this form of digital financial crime. The absence of specific provisions underscores an ongoing gap in the legal framework's capacity to address the evolving nature of asset misappropriation in the digital age. This suggests that further legal advancements may be required to effectively combat sophisticated financial crimes in Indonesia's rapidly digitalizing economy.

Data as the Key Component

As previously mentioned, Indonesia's delayed legal development in supporting the adoption of digital technologies may reflect challenges in integrating the changes brought about by digital transformation. This is especially true in the case of consolidating the rather technical aspects of digital technology like data protection and privacy, as the enforcement of possible legal norms regarding these are often face significant challenges (Qi et al., 2024). These two aspects are of utmost importance in the effort to regulate the utilization of digital technology, mainly because of the role that data plays in the current development trend of many digital technologies. The data-centric nature of this progression highlights the growing significance of data as a focal point for policymakers (Das 2024). This ensures that legal frameworks effectively regulate both the use and protection of data as a fundamental element, alongside safeguarding privacy (Bygrave, 2014).

The legal ramifications of data utilization are extensive and will continue to expand as digital technologies grow increasingly dependent on data. The legal implications of data are also followed by risks associated with its usage, particularly regarding data security. These two dimensions eventually set the stage for data governance, which focuses on two aspects: data protection and privacy. At a glance, it's quite easy to mistake one for the other, mainly because of the closely related and often intertwined aspects of both legal dimensions. However, both aspects have its own unique legal implications in the digital era, which require distinct provisions (Lynskey, 2023). Nevertheless, these two aspects are often regulated under one comprehensive legal framework. A key example of this is the General Data Protection Regulation (GDPR), which is widely regarded as the global benchmark for data protection and privacy (Mantelero, 2021).

The same applies to Indonesia, where, as previously mentioned, the legislative process toward establishing a comprehensive legal framework has been notably lengthy. EIT Law provided some of the basic provisions regarding data governance, but lacked specifics, particularly on the more technical side of it. Answering this problem, Indonesia brought some key provisions regarding this through Government Regulation No. 82 of 2012 on Implementation of Electronic Systems and Transactions, which was later incorporated into Minister of Communication and Information Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (Wahyulina et al., 2022). Indonesia's first comprehensive legal framework for data governance emerged later with Law No. 27 of 2022 on Personal Data Protection (PDP Law) (Admiral and Pauck 2023). This law consolidates all aspects covered by previous regulations while introducing several enhancements.

In the context of asset misappropriation, including traditional forms, data has always played a crucial role, though it is often overlooked in academic literature. Aspects such as purchase records and financial statements are data that often become the main object of asset misappropriation and other forms of fraud. Data governance in the digital context plays a much bigger role, as activities done using digital technologies are usually recorded by digital logs that can be accessed by certain users or in some operating system, system administrators. At first glance, the relationship between data governance,

privacy, and asset misappropriation may seem limited, as data governance is often associated with technical mechanisms for detecting and preventing different types of fraud.

However, any form of data manipulation carries serious legal implications, as it compromises not only the integrity of personal data but also the fundamental right to privacy. Asset misappropriation, to be more specific, causes an even wider set of legal implications. Data subjects already face risks from all kinds of data utilization, hence the creation of legal compliance for data security, integrity, and the protection against unlawful identification (Anyanwu et al., 2024). Asset misappropriation essentially multiplies these risks, as it renders the steps taken by a company as data processor to mitigate the risks through cybersecurity measures. In a sense, asset misappropriation can be viewed as a contributing factor to cybercrime, as it creates vulnerabilities that can be exploited (Trierweiler & Krumay, 2023).

Analyzing the Personal Data Protection (PDP) Law is crucial for understanding its role in preventing and addressing asset misappropriation in the digital age. By examining specific provisions, we can evaluate how the law safeguards personal data, which is often targeted in such crimes.

Table 4. Relevant Provisions in PDP Law

Article Number	Provision	Relevancy in Asset Misappropriation
Article 16(2)	The processing of personal data must ensure the security of data from unauthorized access, disclosure, alteration, misuse, destruction, or loss.	Relevant as it highlights the need to protect personal data from unauthorized actions which can be a form of asset misappropriation.
Article 32(1)	Controllers of personal data are required to provide data subjects with access to their personal data and processing logs, ensuring transparency and accountability in the handling of such information.	Ensures transparency and accountability, making it harder to hide asset misappropriation activities.
Article 34(1)	Controllers must assess the impact of personal data protection when processing data with high potential risk to data subjects.	Important for identifying vulnerabilities that could lead to asset misappropriation.
Article 36	Any violation of personal data processing that causes losses to other parties must be accountable.	Directly addresses the consequences of asset misappropriation and the accountability of the involved parties.

Source: Primary Law (Law No. 27 of 2022)

Table 4 above explains that the PDP Law provisions play both generalized and specific roles in preventing and addressing asset misappropriation. The generalized aspects include Articles 16(2) and 34(1), which outline broader protections related to data security and the rights of data subjects. Article 16(2) ensures the overall security of personal data by mandating protection from unauthorized access and misuse. This provision, although not directly incriminating, sets a broad standard for data security practices, thereby reducing the risk of asset misappropriation. Article 34(1) focuses on proactive risk management by requiring impact assessments for high-risk data processing, helping to identify and mitigate potential vulnerabilities that could be exploited for misappropriation. In contrast, Articles 32(1) and 36 contain more direct, criminally relevant provisions. Article 32(1) mandates transparency and accountability by requiring data controllers to provide data subjects with access to their personal data and processing logs. This provision aids in detecting and tracing unauthorized data manipulations, which are commonly involved in asset misappropriation cases. Article 36 explicitly addresses accountability, stating that any violation resulting in losses must be compensated, thus directly connecting data protection breaches to both legal and financial consequences.

Conclusion

The analysis of this research emphasizes the importance of understanding the interplay between asset misappropriation as a crime and its implications within the digital context. Data remain the key piece in this puzzle of legal challenge, as they are used in digital technologies to conduct key organizational activities. In particular, normative analyses of the relevant legal frameworks are found to have one similarity, which is the lack of recognition for asset misappropriation as distinct crime with its own unique set of legal implications. As the development of legal frameworks for electronic systems and data protection indicates a narrow focus on strictly digital issues, it'd be better for Indonesia to develop a generalized recognition of asset misappropriation as a crime, that can be used for both the traditional and digital context. This is especially relevant to provide a clearer distinction between this type of fraud with corruption, which normatively only applies when there's a damage to the country's finance. Provisions provided by EIT Law and PDP Law can then be used to ensnare perpetrators of asset misappropriation with multiple articles that can add more weight to the crime, while also protecting the integrity of Indonesia's digital environment. Further research could address a key limitation of this study, which is the lack of a comprehensive analysis on the severity of the crime. This can be done by focusing on financial losses and the extent of potential damages inflicted on data subjects.

References

Ahn, M. J. (2014). Enhancing Corporate Governance in High-Growth Entrepreneurial Firms. *International Journal of Innovation and Technology Management*, *11*(06), 1–16. https://doi.org/10.1142/S0219877014500382

Aldboush, H. H. H., & Ferdous, M. (2023). Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust. *International Journal of Financial Studies*, *11*(3), 1–18. https://doi.org/10.3390/ijfs11030090

Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., & Reis, O. (2024). Data Confidentiality and Integrity: A Review of Accounting and Cybersecurity Controls in Superannuation Organizations. *Computer Science & IT Research Journal*, *5*(1), 237–253. https://doi.org/10.51594/csitrj.v5i1.735

Bakri, H. H. M., Mohamed, N., & Said, J. (2017). Mitigating asset misappropriation through integrity and fraud risk elements: Evidence emerging economies. *Journal of Financial Crime*, *24*(2), 242–255. https://doi.org/10.1108/JFC-04-2016-0024

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199675555.001.0001

Çollaku, L., Ramushi, A. S., & Aliu, M. (2024). Fraud intention and the relationship with selfishness: the mediating role of moral justification in the accounting profession. *International Journal of Ethics and Systems*, *ahead-of-p*(ahead-of-print), 1–18. https://doi.org/10.1108/IJOES-10-2023-0220

Ding, S. (2023). Digital Rights Management. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), *Trends in Data Protection and Encryption Technologies* (pp. 163–169). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33386-6_28

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289–304. https://doi.org/10.37253/jjr.v24i2.7280

Haberly, D., MacDonald-Korth, D., Urban, M., & Wójcik, D. (2019). Asset Management as a Digital Platform Industry: A Global Financial Network Perspective. *Geoforum*, *106*, 167–181. https://doi.org/10.1016/j.geoforum.2019.08.009

Hilbert, M. (2020). Digital technology and social change: The digital transformation of society from a historical perspective. *Dialogues in Clinical Neuroscience*, *22*(2), 189–194. https://doi.org/10.31887/dcns.2020.22.2/mhilbert

Ing, L. Y., Grossman, G., & Christian, D. (2022). Digital Transformation: 'Development for All'? In *New Normal, New Technology, New Financing* (pp. 75–88). Economic Research Institute for ASEAN and East Asia (ERIA). https://doi.org/DOI:

Kassem, R. (2014). Detecting asset misappropriation: A framework for external auditors. *International Journal of Accounting, Auditing and*

Performance Evaluation, *10*(1), 1–42. https://doi.org/10.1504/IJAAPE.2014.059181

Kharisma, D. B. (2022). Kepatuhan Dan Kesadaran Hukum Kritis: Kajian Putusan Mahkamah Konstitusi Nomor 50/PUU-VI/2008. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *11*(1), 37–53. https://doi.org/10.33331/rechtsvinding.v11i1.832

Lehavi, A. (2019). *Intellectual Property, Data, and Digital Assets* (A. Lehavi (ed.)). Cambridge University Press. https://doi.org/10.1017/9781108595391

Lynskey, O. (2023). Complete and Effective Data Protection. *Current Legal Problems*, *76*(1), 297–344. https://doi.org/10.1093/clp/cuad009

Mantelero, A. (2021). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review*, *40*, 1–5. https://doi.org/https://doi.org/10.1016/j.clsr.2020.105500

Margiansyah, D. (2020). Revisiting Indonesia's Economic Diplomacy in the Age of Disruption: Towards Digital Economy and Innovation Diplomacy. *JAS (Journal of ASEAN Studies)*, *8*(1), 15–39. https://doi.org/10.21512/jas.v8i1.6433

Mat Ridzuan, N. I., Said, J., Razali, F. M., Abdul Manan, D. I., & Sulaiman, N. (2022). Examining the Role of Personality Traits, Digital Technology Skills and Competency on the Effectiveness of Fraud Risk Assessment among External Auditors. *Journal of Risk and Financial Management*, *15*(11), 1–14. https://doi.org/10.3390/jrfm15110536

Melinda, K., Susanti, A., Tarigan, J. K., Deliana, D., & Napitupulu, I. H. (2022). The Role Of Internal Audit In Fraud Prevention And Disclosure: Literature Review. *Kajian Akuntansi*, *23*(1), 50–66. https://doi.org/10.29313/ka.v23i1.9400

Nomorissa, T. A., & Suryadithya, C. (2022). Forensic Data Analytics dalam Mendeteksi Fraud. *Proceeding Accounting Skill Competition*, *1*(1), 161–180.

Ofori-Duodu, M. S. (2019). *Exploring Data Security Management Strategies for Preventing Data BreachesData Breaches*. Walden University.

Qi, M., Yao, X., Zhu, Q., & Jin, G. (2024). Network privacy protection and legal system in the digital era. *Science of Law Journal*, *3*(1), 127–132. https://doi.org/10.23977/law.2024.030120

Rachman, A., Jasmin, J., Ibadurrahman, I., & Utami, E. Y. (2024). The Relationship between Startup Incubator Development and Venture Capital Investment on Digital Economic Growth in Indonesia. *The Es Economics and Entrepreneurship*, *2*(03), 157–169. https://doi.org/10.58812/esee.v2i03.248

Ramadlan, F., Tarjo, & Yuliana, R. (2020). Analysis of Fraud Star and Organizational Commitment To Asset Misappropriation Detection With Internal Control System. *International Colloquium on Forensics Accounting and Governance (ICFAG)*, *1*(1), 189–201.

Shibambu, A. (2024). Transformation of digital government services in the public sector in South Africa. *Africa's Public Service Delivery and Performance Review*, *12*(1), 1–7. https://doi.org/10.4102/apsdpr.v12i1.753

Syahria, R. (2019). Detecting Financial Statement Fraud Using Fraud Diamond (A Study on Banking Companies Listed On the Indonesia Stock Exchange Period 2012-2016). *Asia Pacific Fraud Journal*, *4*(2), 183–190. https://doi.org/10.21532/apfjournal.v4i2.114

Tan, D. (2021). Metode Penelitian Hukum: Mengupas dan Mengulas Metodologi dalam Menyelenggarakan Penelitian Hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(5), 2463–2478.

Trierweiler, M. K., & Krumay, B. (2023). Managing Cybersecurity and Other Fraud Risks in Small and Medium Enterprises – A Framework to Build a Fraud Management Program in Times of Digitalization. *Wirtschaftsinformatik Proceedings 2023*, 1–19.

Utami, Y. L., Rakhmayani, A., Imtichana, D. O., & Hajar, N. (2021). Determinants of Asset Misappropriation by Employee from New Fraud Triangle Theory Perspective (Case Study on Holding Company in Central Java). *Business and Accounting Research (IJEBAR) Peer Reviewed-International Journal*, *5*(2), 2614–1280.

Wahyulina, D., Damayanti, E., Azizah, M. N., & Fatimah, W. N. (2022). Anotasi atas Regulasi Perlindungan Data Pribadi di Indonesia. *Jurnal Magister Hukum Perspektif*, *12*(2), 1–13. https://doi.org/10.37303/magister.v12i2.17

Wahyulistyo, F., & Cahyonowati, N.-. (2023). Determining Factors of Asset Misappropriation Tendency by Employees in Perspective of Fraud Hexagon Theory. *Jurnal Dinamika Akuntansi*, *15*(1), 52–67. https://doi.org/10.15294/jda.v15i1.42090

Widjaja, G., & Budiman, E. (2024). Konsekuensi Hukum atas Kehilangan Aset Perusahaan Berfasilitas Pembebasan Bea Masuk. *Netizen: Journal of Society and Business*, *1*(3), 156–170.

Yustia, D. A., & Arifin, F. (2023). Bureaucratic reform as an effort to prevent corruption in Indonesia. *Cogent Social Sciences*, *9*(1), 1–11. https://doi.org/10.1080/23311886.2023.2166196