Legitimasi: Jurnal Hukum Pidana dan Politik Hukum
P-ISSN 2088-8813 E-ISSN 2579-5104
Vol. 14, No. 2, July-December 2025
DOI: 10.22373/legitimasi.v14i2.32699

Legal Protection of Personal Data and Virtual Assets in the Metaverse: A Comparative Study of the United States, China, and South Korea

Muhammad Kandriana
Muhammadiyah University of Bima, Indonesia

Zuhrah
Muhammadiyah University of Bima, Indonesia

Iksan
Muhammadiyah University of Bima, Indonesia

Rahmad Maulana
University Of Belgrade, Serbia

Muhammad Yasir
University Ez-Zitouna, Tunisia
Muhammadkandriana1507@gmail.com

Abstract: The development of the metaverse as a new digital interaction space has given rise to increasingly complex legal challenges regarding the protection of personal data and virtual assets. This situation demonstrates the regulatory gap between countries in responding to the dynamics of the global digital economy. This study examines the comparison of regulations on personal data protection and virtual asset protection in the United States, China, and South Korea, and identifies lessons that can be applied to the Indonesian legal system. Utilizing a normative legal research method through a comparative approach, this study examines primary and secondary legal sources, including laws, national policies, and digital legal doctrines, in each country. The results show that the United States applies a liberal sectoral regulatory model, China adopts a centralistic model based on state control, while South Korea develops a hybrid model that balances innovation and legal protection. The comparative analysis reveals gaps in institutional aspects, regulatory integration, and legal recognition of activities and assets in the metaverse. The results of the study indicate that Indonesia should adopt an adaptive legal framework that comprehensively integrates personal data and virtual asset protection as a guiding principle for ius constituendum in establishing a safe, equitable, and globally competitive metaverse governance.

Keywords: Legal Protection, Virtual Assets, Metaverse, United States, China, South Korea

Submitted: November 8, 2025 Accepted: December 17, 2025 Published: December 19, 2025

Abstrak: *Perkembangan metaverse sebagai ruang interaksi digital baru memunculkan tantangan hukum terhadap perlindungan data pribadi dan aset virtual yang semakin kompleks. Kondisi ini memperlihatkan adanya kesenjangan regulatif antarnegara dalam merespons dinamika ekonomi digital global. Penelitian ini merumuskan masalah tentang bagaimana perbandingan regulasi perlindungan data pribadi dan perlindungan aset virtual di Amerika Serikat, China, dan Korea Selatan, serta apa pelajaran yang dapat diterapkan bagi sistem hukum Indonesia. Dengan menggunakan metode penelitian hukum normatif melalui pendekatan komparatif, penelitian ini menganalisis sumber hukum primer dan sekunder yang meliputi undang-undang, kebijakan nasional, serta doktrin hukum digital di masing-masing negara. Hasil penelitian menunjukkan bahwa Amerika Serikat menerapkan model regulasi sektoral yang bersifat liberal, China mengadopsi model sentralistik berbasis kontrol negara, sedangkan Korea Selatan mengembangkan model hibrida yang menyeimbangkan inovasi dan perlindungan hukum. Analisis perbandingan mengungkapkan adanya kesenjangan pada aspek kelembagaan, integrasi regulasi, dan pengakuan hukum terhadap aktivitas serta aset dalam metaverse. Hasil penelitian menunjukkan Indonesia perlu mengadopsi kerangka hukum adaptif yang mengintegrasikan perlindungan data pribadi dan aset virtual secara komprehensif sebagai arah ius constituendum dalam membangun tata kelola metaverse yang aman, berkeadilan, dan berdaya saing global.*

Keywords*: Perlindungan Hukum, Data Pribadi, Aset Virtual, Metaverse, Amerika Serikat, Cina, Korea Selatan*

A. Introduction

The development of *the metaverse* as a virtual space for social and economic interaction has given rise to new legal challenges, particularly regarding the protection of personal data and ensuring legal certainty over virtual assets transacted and traded within this environment.[1] The use of artificial Intelligence in law enforcement in Indonesia presents significant opportunities to enhance efficiency, strengthen transparency, and improve accuracy at various stages of the legal process.[2] This article examines how countries with different regulatory models, the United States, China, and South Korea, regulate the protection of personal data and virtual assets in the *metaverse context*, as well as their comparative implications for the direction of lawmaking (*Ius Constituendum*) in Indonesia.[3]

The importance of this study stems from two things: first, *the metaverse* accumulates much richer and more sensitive personal data than traditional *online interactions*, thus demanding an adaptive data protection framework; second, virtual

[1]V Xynogalas, "Metaverse: Searching for Compliance with the General Data Protection Regulation," *International Data Privacy Law* , 2024; Philipp Hacker, "Sustainable AI Regulation," *Common Market Law Review* 61, no. 2 (2024).

[2]Ifan Arsyad and Jamal Wiwoho, "Legal Framework For Protecting Banking Transactions In The Metaverse Against Deepfake Technology," *Journal of Law and Sustainable Development* 12, no. 2 (2024).

[3]Meera Abdulla Alshamsi and Attila Sipos, "The Legal Implications Of The Aviation Industry's Entrance To The Metaverse," *Access to Justice in Eastern Europe* 7, no. 1 (2024).

assets (*e.g., NFTs, tokens*, *items) Games* have transformed into real economic objects, creating a need for legal certainty regarding ownership, transactions, and consumer protection.[4] In modern electronic transaction practices, fulfilling the elements of a 'certain object' and a 'lawful cause' often presents a real obstacle.[5] Indonesia is shifting its focus from moral regulation to victim protection by expanding its complaint mechanism, allowing victims to participate more actively in the legal process. Current regulatory[6] landscapes vary: the US tends to be fragmented, with a sectoral approach and multi-agency involvement; China implements a robust PIPL framework and state control; and South Korea recently harmonized user protection through the Virtual Asset User Protection Act*. Act*.[7] *The asynchrony* of these models reveals regulatory gaps relevant to discuss in order to formulate recommendations for Indonesia, a country that implemented the Personal Data Protection Law in 2022 but still faces *implementation challenges* in the *metaverse realm*.[8]

This study uses a normative legal research method with a comparative approach. The analysis was conducted on primary legal sources (statutes, regulations, and authority decisions) and secondary sources (academic articles and policy reports) from each jurisdiction. Then, a regulatory typology and *regulatory* gap *analysis were constructed* to provide recommendations *for legal matters.* Adaptive [9]*constituendum. This method allows for the identification of policy patterns, supervisory institutions, and protection instruments that are most relevant to the Indonesian legal context.*

B. Comparison of Personal Data Protection Regulations

In the United States, personal data protection regulations are sectoral and market-based, resulting in a lack of a comprehensive federal law; instead, a collection of sectoral regulations govern specific aspects, such as health or finance. This situation creates regulatory fragmentation and a lack of certainty about user rights. [10]In contrast, in China, through Personal *Information Protection (PIPR), the Personal Information Protection Law* (PIPL), which came into effect on November 1, 2021, implements a

[4]Matías Mascitti, "The Metaverse Impact on the Politics Means," *Computer Law and Security Review* 55 (2024); Lokke Moerel, "Metaverse and Data Protection," in *Research Handbook on the Metaverse and Law*, 2024.

[5]Kateryna Nekit, "Social Media Account as an Object of Virtual Property," *Masaryk University Journal of Law and Technology* 14, no. 2 (2020).

[6]Muhamamd Kandriana et al., "The Expansion of the Concept of Complaint-Based Offenses in Indonesia's New Criminal Code (Law No. 1 of 2023): A Normative Study on the Effectiveness of Victim Protection," *Widya Pranata Hukum: Journal of Legal Studies and Research* 7, no. 1 (2025): 216–35.

[7]Korea Legislation Research Institute and Korean Law Translation Center, "Act on the Protection of Virtual Asset Users (English Text)" (nd), https://elaw.klri.re.kr.

[8]Republic of Indonesia, "Law Number 27 of 2022 concerning Protection of Personal Data" (2022).

[9]Bogdan Derevyanko et al., "On Pros and Cons of Legitimizing Cryptocurrency (Case Study of Ukraine)," *Social and Legal Studios* 6, no. 3 (2023); S Lim, "A Global Comparative Analysis of Data Protection Laws," *IET Research* , 2025, https://ietresearch.onlinelibrary.wiley.com.

[10]Rowin Jansen and Pieter Wolters, "The Access of US Intelligence Agencies, Transfers of Personal Data and the Trans-Atlantic Data Privacy Framework," *European Data Protection Law Review* 10, no. 4 (2024).

state-centric control model for personal data, including restrictions on cross-border data flows and centralized oversight. [11]In South Korea, the regulation is hybrid: through the Personal *Information Protection Law* (PIPL)*, as the PIPL is implemented. The Protection of Personal Information Act (PIPA) and the independent watchdog, the Personal Information Protection Commission (PIPC), are* attempting to balance the protection of individual rights with digital innovation and state regulation.[12] Meanwhile, in Indonesia, with the enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), basic regulations have been established, but actual implementation, the authority of independent institutions, and adaptation to new digital spaces such as *the metaverse* remain limited. This indicates that Indonesia is currently in a transitional phase from normative regulation to mature operational regulation.

C. In Virtual Asset Regulation

In the regulation of virtual assets, the United States demonstrates a fairly open but fragmented approach: regulation is distributed among agencies such as *the Securities and Exchange Commission* (*SEC*) and *the Commodity Futures Trading Commission* (*CFTC*), which has created uncertainty in classifying tokens as *securities* or commodities and created barriers for market participants.[13] In contrast, China has implemented a broad ban on *crypto transactions* and encouraged the development of state-controlled digital assets, reflecting a highly centralized regulatory strategy aimed at financial stability and controlling capital flows. [14]In South Korea, the enactment of *the Act on the Protection of Virtual Assets,* the 2023 Virtual Assets [15]*Act* (*VAUPA) introduced a legal definition for "virtual assets," user protection, and regulation of virtual asset services, demonstrating a more mature and protective regulatory paradigm for consumers.* Meanwhile, in Indonesia, although virtual assets are regulated as commodities by the Commodity Futures Trading Regulatory Agency (*Bappebti*), there is no adequate specific regulation for virtual assets in the *metaverse context*, so there are still significant gaps in legal certainty, user protection, and adaptation to the dynamics of the global digital economy.

---

[11]I Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)," *Smart Cities* 5, no. 3 (2022): 57, https://www.mdpi.com/2624-6511/5/3/57.

[12]Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020); Ninne Zahara Silviani et al., "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea," *Jurnal Hukum Dan Peradilan* 12, no. 3 (2023).

[13]Seung Jae Jeon, Myung Seok Go, and Ju Hyun Namgung, "Use of Personal Information for Artificial Intelligence Learning Data under the Personal Information Protection Act: The Case of Lee-Luda, an Artificial-Intelligence Chatbot in South Korea," *Asia Pacific Law Review* 31, no. 1 (2023).

[14]Zhicheng He, "When Data Protection Norms Meet Digital Health Technology: China's Regulatory Approaches to Health Data Protection," *Computer Law and Security Review* 47 (2022).

[15]T van der Linden and T Shirazi, "Markets in Crypto-Assets Regulation: Does It Provide Legal Certainty and Increase Adoption of Crypto-Assets?," *Financial Innovation* 9 (2023): 22.

D. Critical Comparison of Findings with Global Studies in the US, China, and South Korea

The findings of this study confirm that the three countries, the United States, China, and South Korea, have developed different approaches to protecting personal data and virtual assets in *the metaverse*, and these differences are rooted in their respective digital governance models (*market-driven, state-centric*, and *rights-oriented*). Placing these findings within the context of the current literature demonstrates that this study not only describes regulations but also explains how these policy configurations influence the design, architecture, and risks of the metaverse as a new socio-economic interaction space.[16]

A number of recent studies have emphasized that the main issue *with the metaverse* is not just the technical aspects, but the accumulation of high-resolution data (biometrics, behavior, and context) that has the potential to give rise to a form of "*surveillance. and"* new *capitalism. Through a systematic literature review, the review* shows that the dominant risks are persistent tracking, cross-platform data aggregation, and weak unified security standards in *immersive environments*. This research's findings complement those of previous studies by demonstrating how legal configurations in the US, China, and South Korea concretely limit or open up space for such data collection practices, providing a comparative legal dimension not yet explored in technical studies.[17]

Highlighting the absence of clear global standards regarding data protection and security in *the metaverse*, particularly in terms of identity *authentication* and *identity theft prevention. Rather* than -stopping at mapping technical risks, this research shows that differences in legal regimes across three jurisdictions result in asymmetric levels of protection for digital identity and user behavior data, which have direct implications for policy design for developing countries like Indonesia.[18]

1. Differences with *interoperability* and governance studies

Interoperability study. *The metaverse* demonstrates that cross-platform and cross-jurisdictional issues are increasingly crucial as data and virtual assets move between different ecosystems. These studies emphasize the need for technical and institutional *interoperability frameworks*, but generally do not detail how differing national regulations shape legal constraints on the movement of data and virtual assets. This research fills that gap by constructing a comparative map showing, for example, that the market-based sectoral approach in the United States contrasts

[16]Chang Zhang and Lexuan Wang, "Virtual Worlds, Real Politics: A Cross-national Comparative Study of Metaverse Policy Approaches," *Politics and Governance* 13 (2025).

[17]Nur Adlin Hanisah Shahul Ikram, "Data Breaches Exit Strategy: A Comparative Analysis of Data Privacy Laws," *Malaysian Journal of Syariah and Law* 12, no. 1 (2024).

[18]Sungjin Lim and Junhyoung Oh, "Navigating Privacy: A Global Comparative Analysis of Data Protection Laws," *IET Information Security* 2025, no. 1 (2025): 5536763.

sharply with China's cyber sovereignty approach and South Korea's user-oriented digital rights model, resulting in an unequal configuration of legal *interoperability.*[19]

"*A Tale 'The Two Metaverses " describes how the United States-China digital rivalry has shaped two competing metaverse models, particularly in terms of technological standards and macro-governance frameworks*. This study continues this discourse by adding South Korea as a "*middle power*" that develops a *metaverse strategy* based on public-private collaboration and digital rights protection, and sharpens the analysis on two specific issues that have not been widely discussed: personal data protection and virtual asset regulation in the *metaverse context*.[20]

2. Confirmation and expansion of findings in China

Several studies have confirmed that China's *metaverse* and digital economy policies are based on a *state-centric approach* that prioritizes state control, data sovereignty, and domestic technology industrialization. This research aligns with these findings but expands on them by demonstrating how the philosophy of *cyber -sovereignty* influences not only the regulatory architecture of personal data (e.g., through data localization rules and platform oversight), but also the economic structure of virtual assets through the prohibition of *crypto trading* and restrictions on *blockchain-based assets* in public *metaverses*. Thus, this research demonstrates that in China, *metaverse design* tends to be *closed. An ecosystem* that legally combines control over data flows and the design of virtual asset business models, a dimension that has not been discussed comparatively in the literature, focusing solely on industrial policy.[21]

Furthermore, a study of *metaverse policies* in China and South Korea reveals efforts by both countries to consolidate national strategies that encompass cybersecurity standards, infrastructure, and data governance. This research adds a layer of legal analysis by examining how more concrete normative instruments (personal data laws, virtual asset guidelines, and financial supervisory frameworks) in each country translate into *governance practices. metaverse*, especially regarding platform accountability for data breaches and misuse of virtual assets.[22]

3. Confirmation and enrichment of findings related to South Korea

Literature on South Korea's digital strategy depicts the country as a pioneer in integrating *metaverses* into its economic and public service agendas, including through

[19]Chuan Chen et al., "Privacy Computing Meets Metaverse: Necessity, Taxonomy and Challenges," *Ad Hoc Networks* 158 (2024): 103457.

[20]Kim Normann Andersen, Jungwoo Lee, and Soonhee Kim, "MetaVerse+ in South Korea and Denmark: Snapshots from Two Leading Digital Nations," in *Proceedings of the 25th Annual International Conference on Digital Government Research*, 2024, 827–31.

[21]Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity* 8, no. 1 (2022).

[22]Denindah Olivia, "Legal Aspects of Artificial Intelligence on Automated Decision-Making in Indonesia: Lessons from the European Union, the United States, and China," *Lentera Hukum* 7, no. 3 (2020).

state investment and the formation of a national *metaverse alliance*. This research confirms South Korea's position as a pioneer, while also underscoring the stringent regulations on personal data protection through PIPA and initiatives such as the Korea Digital Bill of Rights. Rights directs the national *metaverse model* towards a *user-centric* and *safe -by-design approach*, which places data rights and digital asset security as key pillars.[23]

On the virtual asset side, various digital regulatory reports indicate that South Korea is moving toward a comprehensive framework for *crypto* and digital assets, including plans to regulate *stablecoins* and report cross-border transactions to prevent money laundering and protect investors. This research's findings directly link these policy directions to the design of the *metaverse ecosystem*, asserting that the stability and legal protection of virtual assets are prerequisites for user trust and the economic viability *of the metaverse*, a relationship that has not been explored in detail in existing macro policy studies.[24]

4. The United States and The Market Approach to Data and Virtual Assets

Comparative research on global data protection laws reveals that the United States employs a sectoral and market-based approach, characterized by a combination of federal and state regulations, in contrast to omnibus models such as the GDPR or PIPA. In the context of *the metaverse*, several legal and policy studies have highlighted that the absence of a single federal framework leaves room for large technology companies to design privacy and data management policies that rely heavily on private contracts and *self-regulation*. This study's findings fill this gap by demonstrating how such approaches impact the level of personal data protection in *the metaverse*, for example, in terms of data processing transparency, cross-service data integration, and users' bargaining power over platforms.[25]

In terms of virtual assets, a recent report on digital asset regulation confirms that the United States is moving through a combination of securities and commodities law enforcement, *anti-money* laundering guidance, and phased regulation of *stablecoins* and virtual asset service providers. This research leverages these findings to demonstrate that, unlike China's blanket ban and South Korea's cautious approach, the United States' model is relatively open to virtual asset innovation in the metaverse, but this openness results in uncertainty over legal categories and a division of regulatory authority, potentially posing risks to cross-border users.[26]

5. Affirmation of Comparative Contributions and Implications for Indonesia

[23]Lim and Oh, "Navigating Privacy: A Global Comparative Analysis of Data Protection Laws."

[24]Statistics and the Rise of Digital Asset Regulations, "Update on Digital Asset Regulations and Rules Around the World 2024," nd, https://www.scb10x.com/en/blog/digital-asset-regulations-2024.

[25]Giulio Santoni, "Personal Data as a Market Commodity: Legal Irritants from China'experience," *European Journal of Privacy Law and Technologies* 2023, no. 1 (2023).

[26]Yang Feng, "The Future of China's Personal Data Protection Law: Challenges and Prospects," *Asia Pacific Law Review* 27, no. 1 (2019).

Several recent studies have conducted a general mapping of legal challenges in *the metaverse, but they typically stop at the global or regional level without constructing an in-depth cross-country comparison matrix that simultaneously protects personal data and virtual assets. This research contributes by constructing a sharper comparison of three key jurisdictions, the United States, China, and South Korea, and directly linking these to policy design implications for the formation of digital criminal law and metaverse* governance in Indonesia.[27]

Specifically, these findings provide a framework for policymakers in Indonesia to select or combine elements from each model: strong protection of data rights and virtual assets like South Korea, vigilance against *systemic risk* and data sovereignty like China, and a digital economy innovation space like the United States. Thus, the critical analysis and comparison with previous research not only strengthen the academic foundation of this article but also provide concrete normative contributions to enhancing the legal basis for personal data protection and regulating virtual assets in *the metaverse*.[28]

E. Research Contributions and Their Impact on the Development of Indonesian Criminal Law

This research contributes to the development of criminal law by explaining how the design of personal data protection and virtual asset regulations in *the metaverse* in the US, China, and South Korea shapes the scope of criminalization, enforcement, and criminal liability, and how these lessons can be used as a reference for reforming Indonesian criminal law.[29]

1. Framework for contributions to criminal law

This research first -provides a theoretical contribution by formulating a direct link between personal data protection regimes, virtual asset regulations, and the formation of new criminal offenses in the *metaverse ecosystem*. Recent studies on data and *metaverse regulation* indicate that data and digital asset protection cannot be separated from the design of cybercrime, as crimes such as *identity theft, fraud, and theft are becoming increasingly prevalent. Theft*, *unlawful* data *processing*, and manipulation of *crypto assets /virtual items* occur in the same space and often overlap. By mapping three regulatory models (*market-driven in the US, state-centric in China, and rights-oriented* in South Korea), this study shows how each legal configuration

[27]Muhammad Tukur et al., "The Metaverse Digital Environments: A Scoping Review of the Challenges, Privacy and Security Issues," *Frontiers in Big Data* 6 (2023): 1301812.

[28]Denny Suwondo, "The Legal Protection of Personal Data in the Perspective of Human Rights," *Law Development Journal* 5, no. 4 (2024).

[29]Lim and Oh, "Navigating Privacy: A Global Comparative Analysis of Data Protection Laws."

results in a different spectrum of criminalization and criminal liability for individual perpetrators, platform corporations, and virtual asset service providers.[30]

At the conceptual level, this research also enriches the discourse on the expansion of objective and subjective elements of crime in digital spaces. Recent literature emphasizes that crime in *the metaverse* involves new forms of "presence " and interaction, such as avatars*. harm*, *deep behavioral tracking*, and *high-frequency assets. Transactions* challenge traditional methods of assessing unlawful acts, losses, and mens rea. By linking the regulatory patterns of three countries with examples of criminalization (e.g., virtual asset *fraud*, data *breaches* with *immersive impacts*, or misuse of access authorization in *the metaverse*), this research offers a foundation for formulating new parameters *of mens rea* and *culpability* in the context of virtual assets and identities.[31]

2. The Impact of the Differences in the US, China, and South Korean Models

In the United States, a sectoral approach to data protection and enforcement-based regulation of digital assets has led to a focus in criminal law on fraud, identity theft, and financial crimes involving *crypto assets* and *tokens*. Several studies have shown that this framework creates a fragmented enforcement landscape, with different agencies (e.g., securities authorities, commodities authorities, and federal law enforcement) addressing violations largely through the concepts of fraud, breach of trust, and digital money laundering. This research confirms that in the *metaverse context*, such a model tends to prioritize protecting market integrity and investors, while protecting personal data and user rights is largely underpinned by private contracts and platform policies, thus opening up asymmetric criminalization risks between perpetrators of major financial crimes and individuals who violate privacy.[32]

In contrast, China, through its data sovereignty policy and broad ban on *crypto trading*, has constructed a criminal law model oriented toward national security and financial system stability. Digital policy studies show that violations of personal data regulations and unauthorized virtual asset activity are strongly constructed as threats to social order and national security, thus expanding the scope for the use of criminal instruments to control data flows and virtual asset experimentation in *the metaverse*. The study adds that this model leads to a more centralized and repressive form of criminalization, where control over the architecture of *metaverse platforms* and virtual assets becomes part of the state's macro-criminal policy, something that is relevant to consider but also critical of when adopted by other countries.[33]

---

[30]Ruoyu Zhao et al., "Metaverse: Security and Privacy Concerns," *Journal of Metaverse*, 2023. Zefeng Chen et al., "Metaverse Security and Privacy: An Overview," in *2022 IEEE International Conference on Big Data (Big Data)* (IEEE, 2022), 2950–59.

[31]H Laiz-Ibanez, "The Metaverse: Privacy and Information Security Risks," *ScienceDirect*, 2025.

[32]Elnur Karimov, "Meta-Morphosis of Copyright and User-Generated Content: Can East Asia's Emerging Policies Navigate through the Metaverse?," *Asian Journal of Law and Society*, 2024.

[33]Morgana Mo Zhou et al., "Understanding Chinese Internet Users' Perceptions of, and Online Platforms' Compliance with, the Personal Information Protection Law (PIPL)," *Proceedings of the ACM*

South Korea occupies an intermediate position, with a combination of strict data regulations and a virtual asset regime that is evolving toward user protection and market stability. The literature shows that PIPA treats violations of data controller obligations (including digital platforms) as serious offenses that can result in administrative and criminal sanctions, while virtual asset regulation and the comprehensive digital asset framework plan aim to prevent market manipulation, *insider trading, and fraud. trading*, and misuse of virtual assets. This research shows that this hybrid model provides a clearer basis for criminalizing *metaverse* platforms and service providers when they negligently or intentionally allow virtual asset fraud, massive data breaches, or security failures that result in user losses.[34]

3. Normative implications for Indonesian criminal law

For Indonesia, the differences in the three countries' models provide a roadmap for strengthening criminal law related to *the metaverse* and virtual assets. First, this study highlights that the current Indonesian legal framework lacks specific offenses related to virtual assets and crimes in *the metaverse*. Therefore, issues such as virtual asset theft, -*NFT-based* fraud, or economic manipulation in virtual spaces are potentially only covered in limited ways through general provisions on fraud, illegal access, or electronic system violations. A comparative study *of the metaverse's Data policy and law suggests that countries seeking to protect their citizens in immersive spaces need to formalize the categories of "virtual assets " and "virtual property* " in positive law, including regulating ownership status, protection, and criminal offenses against them. Thus, this research contributes to providing an empirical basis for formulating *ius constituendum* in the form of a new offense: the misuse of virtual assets, virtual *property fraud*, and *metaverse-based identity crime*.[35]

Second, this research emphasizes the importance of designing digital criminal law enforcement institutions capable of addressing cross-border crimes and across regulatory regimes. South Korea's experience with its increasingly integrated data protection and virtual asset regulatory authorities demonstrates the benefits of having an institution with a clear mandate for digital crime and user protection. For Indonesia, this could translate into the idea of establishing a dedicated digital crime unit, or "Digital Crime Unit," with coordinating authority over personal data protection, virtual assets, and metaverse crimes, while ensuring accountability and judicial oversight to prevent a shift toward excessive state control, as seen in some Chinese practices.[36]

---

on Human-Computer Interaction 8, no. CSCW1 (2024); Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)."

[34]Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime*, 2021.

[35]Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies," *Computer Law and Security Review* 34, no. 1 (2018).

[36]Liang Yang et al., "Interoperability of the Metaverse: A Digital Ecosystem Perspective Review," *IEEE Engineering Management Review* , 2025.

Third, this study highlights the intrinsic cross-border nature of *metaverse crime*, making harmonization of criminal norms and international cooperation mechanisms essential. A comparative study of *metaverse strategies* and digital asset regulation shows that different jurisdictions -develop their own standards regarding the legality of virtual assets, KYC/AML obligations, and definitions of sensitive data, creating a gray area when perpetrators, victims, and servers are located in different countries. This study contributes by demonstrating how the asymmetry of the US–China–South Korea approach can serve as a normative rationale for Indonesia to actively promote extradition treaties, *mutual* legal *assistance*, and the adoption of international *soft -law standards related to metaverses* and virtual assets, so that criminal law enforcement does not stop at national jurisdictional boundaries.[37]

Finally, this study provides practical contributions to Indonesian policymakers by presenting a selection of models that can be selectively adapted. Elements oriented toward protecting users' data rights and virtual assets from South Korea's experience, caution -against *systemic risk* and data sovereignty from China, and support for innovation and digital economic development from the United States can be integrated into the design of national criminal law, provided they are calibrated with the principles of the rule of law, human rights, and Indonesia's economic needs. Thus, this study not only fills the gap in the literature on comparative criminal law in the *metaverse realm* but also offers a conceptual framework and concrete normative recommendations for strengthening Indonesian criminal law in the era of *the metaverse* and digital economy.[38]

Table 1. The Relationship Between Regulatory Models and Their Implications for Indonesian Criminal Law

Aspect	**United States of America**	**China**	**South Korea**	**Implications for Indonesia**
Personal data regulation model	Sectoral and market-based approach; relies heavily on sectoral regulations and platform private policies.	State approach centric with a strong emphasis on data sovereignty and state control over data flows.	Comprehensive and stringent regulations (e.g., PIPA) with a focus on data subject rights and strong obligations for data controllers.	There is a need to encourage a more integrated and clear model by strengthening the rights of data subjects as well as clarifying the criminal obligations of data controllers/processors.

[37]Viktoras Justickis, "Balancing Personal Data Protection with Other Human Rights and Public Interest: Between Theory and Practice," *Baltic Journal of Law and Politics* 13, no. 1 (2020).

[38]Svitlana Khadzhiradieva et al., "Personal Data Protection: Between Human Rights Protection and National Security," *Social and Legal Studios* 7, no. 3 (2024).

Virtual asset regulation	Relatively open; emphasis on commodity securities fraud, AML/CFT, and investor protection through various authorities.	crypto assets and strict oversight of virtual assets; a focus on national security and system stability.	model -with a strengthened virtual asset framework and a comprehensive regulatory plan (e.g., VAUPA, digital asset framework).	There is a need for a clear legal definition of "virtual assets" and "virtual property ", including their ownership status and criminal protection.
The main focus of criminal policy	Fraud, identity theft, and financial crimes related to digital assets and data.	Security of social control and stability of the financial system; criminal space is used to control data and virtual assets.	User protection, market stability, and platform accountability; a combination of administrative and criminal sanctions.	It can combine strong user protection and system stability while maintaining the innovation space of the digital economy.
Law enforcement patterns	Fragmented , involving multiple authorities (securities, commodities, general law enforcement); relies heavily on litigation and ex-law enforcement post .	Centralized under state control; use of criminal instruments to secure control over data and technology.	More coordinated, with dedicated data protection authorities and increasingly strengthened virtual asset oversight.	It can be a reference for the formation of a special digital crime unit/authority (Digital Crime Unit) with a cross-sectoral mandate, but remains accountable.
Typical types of metaverse-related offenses	Virtual asset fraud, identity theft, and data security breaches that harm investors and users.	Violations of data and virtual asset rules associated with threats to national security or public order.	User data protection violations, virtual asset manipulation, and platform negligence that result in losses.	Becoming the basis for formulating a new crime: virtual assets misuse, virtual property fraud, and metaverse-based identity crime in national criminal law.
Relevance for Indonesian criminal law reform	Demonstrates the importance of investor protection and the integrity of virtual asset markets in the metaverse .	Reminds of the risks of overuse of criminal law for technology and data control.	Provides concrete examples of the integration of data protection, virtual asset regulation, and user-centric focus in criminal policy design.	Offering a model map that can be combined: a combination of rights protection, -sy stemic prudence, and innovation support for the Indonesian

	metaverse ecosystem.

F. Regulatory Gap Analysis

Table 2. Regulatory Gap

Aspect	Conditions in Indonesia	Main Gap	Evidence/Regulation Examples per Country
Institutional	Regulations are still spread between the Ministry of Communication and Information , Bappebti , and OJK without a single authority.	The absence of an independent agency that integrates data protection and virtual assets.	US: FTC & SEC act sectorally; China: Cyberspace Administration of China (CAC) single control center; South Korea: independent PIPC under the President.
Legal Terminology & Definitions	The PDP Law and the Futures Trading Law have not yet defined "virtual assets" and " metaverse ".	Legal uncertainty over the status of digital assets, NFTs, and virtual identities.	US: SEC defines "digital asset securities " on a limited basis; China: definition of digital assets under the PBOC; South Korea: VAUPA 2023 provides the first legal definition for virtual assets.
Cross-Border Data & Assets	interoperability standards or data export mechanisms between countries.	Risk of data leaks and jurisdictional conflicts between authorities.	AS: Cloud The 2018 Act regulates cross-border data requests; China: PIPL Article 38 requires security assessments before data transfers abroad; South Korea: PIPA Article 29 supports data exports with equivalent security requirements.
Regulatory Integration	The PDP Law and virtual asset regulations operate separately; coordination is not yet synchronized.	Oversight gaps exist when metaverse activities involve data, assets, and digital identities together.	US: SEC–CFTC interactions remain overlapping; China: CAC and MIIT integration is relatively effective; South Korea: VAUPA is integrated with PIPA.
Metaverse Governance	There are no national governance guidelines regarding metaverse platforms and user rights.	There is no legal basis for platform liability and digital dispute resolution.	US: Meta Platforms under FTC scrutiny for privacy violations; China: VR platforms subject to PIPL & Cybersecurity Law; South Korea: drafting *Metaverse Basic Law* (Bill 2024).

G. Gap Description & Implications

A comparative analysis reveals five key gaps: (1) the absence of a single, independent authority hinders regulatory coordination and enforcement against data and virtual asset breaches, making it difficult for victims of breaches to obtain effective remedies; (2) the absence of legal terminology and definitions for "virtual assets" and " metaverse " means courts and regulators face difficulties in establishing the legal status of digital transactions and ownership; (3) the absence of a trusted data transfer mechanism across data and assets opens up opportunities for vulnerable data flows

and jurisdictional conflicts, reducing the protection of citizens' privacy; (4) the integration of the separation of the PDP Law and virtual asset regulations creates a loophole where metaverse activities can operate in legal loopholes; and (5) the metaverse Without a clear governance framework, platform responsibilities, consumer protection, and dispute resolution mechanisms in virtual spaces remain unclear, leading to the risk of digital rights violations (privacy, digital property, access) and potential user exploitation.[39] Real-world legal impacts include the potential for large-scale data leaks without effective sanctions, ambiguity over NFT/ asset ownership when the platform shuts down, and limited legal recourse for metaverse users in cross-jurisdictional conflicts.[40]

H. Relevance for Indonesia

Comparisons with the United States, China, and South Korea show that Indonesia is in a regulatory transition phase, where a legal foundation has been established through Law Number 27 of 2022 concerning Personal Data Protection, but it has not yet been accompanied by adequate institutional design and digital governance to address the increasingly complex [41]metaverse ecosystem. Going forward, the direction of the ius Indonesia's constituency should focus on three main issues. First, policy integration between the PDP Law and virtual asset regulations to synchronize cross-domain oversight of data, identity, and digital assets.[42] Second, establishing an independent data protection authority, similar to the Personal Information Protection Act. Protection Commission in South Korea, to ensure accountability and transparency in digital law enforcement. Third, the development of a national metaverse governance framework (Metaverse Governance Framework), which is aligned with the ASEAN Digital Framework Agreement (2025), enabling Indonesia to play an active role in harmonizing regional regulations. If this institutional and integration gap is not immediately closed, the risks to citizens' digital rights, such as data leaks, unprotected ownership of virtual assets, and exploitation of the digital economy by foreign platforms, will increase. Therefore, efforts to develop laws that are

[39]M Goldberg, "Metaverse Governance: An Empirical Analysis of Voting within Virtual Worlds," *Journal of Business Research* 160 (2023): 113–29.

[40]L Yang et al., "Recommendations for Metaverse Governance Based on Technical Standards," *Humanities and Social Sciences Communications*,2023, https://www.nature.com/articles/s41599-023-01750-7.

[41]Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfillment," *Hasanuddin Law Review* 10, no. 1 (2024).

[42]Rohan Grover, Kyooeun Jang, and Li wen Su, "Beyond Digital Protectionism? Comparing Personal Data Regulation Frameworks in China, India, and South Korea," in *Research Conference on Communication Information and Internet Policy*, 2022; Dmytro Prokopovych-Tkachenko et al., "Legal Framework For Cybersecurity In The Context Of The Metaverse Formation," *Metaverse Science, Society and Law* 1, no. 1 (2025).

futuristic and adaptable to technological innovation are part of the vision of Indonesian *ius constituendum* in the digital era.[43]

I. Conclusion

Based on a comparative analysis of the United States, China, and South Korea, it can be concluded that regulations on the protection of personal data and virtual assets in the metaverse context in Indonesia are still at an early, normative stage and have not yet been institutionally integrated. The United States excels in market flexibility and innovation, but is weak in cross-sectoral legal certainty; China is strong in state control and data sovereignty, while South Korea demonstrates a balance between protection policies and digital freedoms through its independent Personal Information Protection Agency. Protection Commission (PIPC). This comparison confirms the urgent need for Indonesia to establish an independent data protection authority, clarify the legal definition of virtual assets, and develop a national metaverse governance framework to close regulatory gaps and ensure the protection of citizens' digital rights in the era of social and economic virtualization.

As a direction of *ius Constituendum*, this study recommends three things: (1) strengthening the integration between the Personal Data Protection Law and digital asset regulations through cross-ministerial policies; (2) establishing an independent, adaptive, and accountable data and virtual asset protection agency; and (3) developing a Metaverse Governance National framework in line with the ASEAN Digital Economy Framework Agreement (2025) to guarantee Indonesia's digital sovereignty on the global stage.

The author expresses his appreciation to the academics and legal practitioners who have extensively researched the issues of data protection and cross-border virtual asset regulation, particularly the journal's editorial team and colleagues who provided input during this writing process. Further research is expected to deepen the aspects of law enforcement and cross-jurisdictional regulatory interoperability, so that the concept of *ius* Indonesia's *constituendum* is not only normative, but also capable of responding to the challenges of an increasingly autonomous and decentralized digital world.

Bibliography

Alshamsi, Meera Abdulla, and Attila Sipos. "The Legal Implications Of The Aviation Industry's Entrance To The Metaverse." *Access to Justice in Eastern Europe* 7, no. 1 (2024).

Andersen, Kim Normann, Jungwoo Lee, and Soonhee Kim. "MetaVerse+ in South Korea and Denmark: Snapshots from Two Leading Digital Nations." In *Proceedings of*

[43]Fitriani and D. Rafitrandi, "Preparing for ASEAN Digital Economy Framework Agreement (DEFA)," *Journal of Competition Law and Economics* 16, no. 3 (2023); ASEAN Secretariat, *ASEAN Digital Economy Framework Agreement (DEF): Policy Overview* (ASEAN, 2023).

the 25th Annual International Conference on Digital Government Research, 827–31, 2024.

Arsyad, Ifan, and Jamal Wiwoho. "Legal Framework For Protecting Banking Transactions In The Metaverse Against Deepfake Technology." *Journal of Law and Sustainable Development* 12, no. 2 (2024).

Calzada, I. "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)." *Smart Cities* 5, no. 3 (2022): 57.

Chen, Chuan, Yuecheng Li, Zhenpeng Wu, Chengyuan Mai, Youming Liu, Yanming Hu, Jiawen Kang, and Zibin Zheng. "Privacy Computing Meets Metaverse: Necessity, Taxonomy and Challenges." *Ad Hoc Networks* 158 (2024): 103457.

Chen, Zefeng, Jiayang Wu, Wensheng Gan, and Zhenlian Qi. "Metaverse Security and Privacy: An Overview." In *2022 IEEE International Conference on Big Data (Big Data)*, 2950–59. IEEE, 2022.

Creemers, Rogier. "China's Emerging Data Protection Framework." *Journal of Cybersecurity* 8, no. 1 (2022).

Derevyanko, Bogdan, Nadiia Ivanchenko, Oleksandr Podskrebko, Alina Prylutska, and Olha Turkot. "On Pros and Cons of Legitimizing Cryptocurrency (Case Study of Ukraine)." *Social and Legal Studios* 6, no. 3 (2023).

Feng, Yang. "The Future of China's Personal Data Protection Law: Challenges and Prospects." *Asia Pacific Law Review* 27, no. 1 (2019).

Fitriani, and D. Rafitrandi. "Preparing for ASEAN Digital Economy Framework Agreement (DEFA)." *Journal of Competition Law and Economics* 16, no. 3 (2023).

Goldberg, M. "Metaverse Governance: An Empirical Analysis of Voting within Virtual Worlds." *Journal of Business Research* 160 (2023): 113–29.

Grover, Rohan, Kyooeun Jang, and Li wen Su. "Beyond Digital Protectionism? Comparing Personal Data Regulation Frameworks in China, India, and South Korea." In *Research Conference on Communication Information and Internet Policy*, 2022.

Hacker, Philipp. "Sustainable AI Regulation." *Common Market Law Review* 61, no. 2 (2024).

He, Zhicheng. "When Data Protection Norms Meet Digital Health Technology: China's Regulatory Approaches to Health Data Protection." *Computer Law and Security Review* 47 (2022).

Indonesia, Republik. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (2022).

Institute, Korea Legislation Research, and Korean Law Translation Center. Act on the Protection of Virtual Asset Users (English Text) (n.d.).

Jansen, Rowin, and Pieter Wolters. "The Access of US Intelligence Agencies, Transfers of Personal Data and the Trans-Atlantic Data Privacy Framework." *European Data Protection Law Review* 10, no. 4 (2024).

Jeon, Seung Jae, Myung Seok Go, and Ju Hyun Namgung. "Use of Personal Information

for Artificial Intelligence Learning Data under the Personal Information Protection Act: The Case of Lee-Luda, an Artificial-Intelligence Chatbot in South Korea." *Asia Pacific Law Review* 31, no. 1 (2023).

Justickis, Viktoras. "Balancing Personal Data Protection with Other Human Rights and Public Interest: Between Theory and Practice." *Baltic Journal of Law and Politics* 13, no. 1 (2020).

Kandriana, Muhamamd, Muhammad Rifaid, Muhammad Wildan, Faculty Of Law, Kota Bima, Faculty Of Law, Kota Bima, et al. "The Expansion of the Concept of Complaint- Based Offenses in Indonesia's New Criminal Code (Law No. 1 of 2023): A Normative Study on the Effectiveness of Victim Protection." *Widya Pranata Hukum: Jurnal Kajian Dan Penelitian Hukum* 7, no. 1 (2025): 216–35.

Karimov, Elnur. "Meta-Morphosis of Copyright and User-Generated Content: Can East Asia's Emerging Policies Navigate through the Metaverse?" *Asian Journal of Law and Society*, 2024.

Khadzhiradieva, Svitlana, Tatiana Bezverkhniuk, Oleksandr Nazarenko, Serhii Bazyka, and Tetiana Dotsenko. "Personal Data Protection: Between Human Rights Protection and National Security." *Social and Legal Studios* 7, no. 3 (2024).

Laiz-Ibanez, H. "The Metaverse: Privacy and Information Security Risks." *ScienceDirect*, 2025.

Lim, S. "A Global Comparative Analysis of Data Protection Laws." *IET Research*, 2025.

Lim, Sungjin, and Junhyoung Oh. "Navigating Privacy: A Global Comparative Analysis of Data Protection Laws." *IET Information Security* 2025, no. 1 (2025): 5536763.

Linden, T van der, and T Shirazi. "Markets in Crypto-Assets Regulation: Does It Provide Legal Certainty and Increase Adoption of Crypto-Assets?" *Financial Innovation* 9 (2023): 22.

Mascitti, Matías. "The Metaverse Impact on the Politics Means." *Computer Law and Security Review* 55 (2024).

Moerel, Lokke. "Metaverse and Data Protection." In *Research Handbook on the Metaverse and Law*, 2024.

Nekit, Kateryna. "Social Media Account as an Object of Virtual Property." *Masaryk University Journal of Law and Technology* 14, no. 2 (2020).

Olivia, Denindah. "Legal Aspects of Artificial Intelligence on Automated Decision-Making in Indonesia: Lessons from the European Union, the United States, and China." *Lentera Hukum* 7, no. 3 (2020).

Prokopovych-Tkachenko, Dmytro, Volodymyr Sarychev, Vitaliy Derkach, Yevheniy Rudenko, and Volodymyr Matzko. "Legal Framework For Cybersecurity In The Context Of The Metaverse Formation." *Metaverse Science, Society and Law* 1, no. 1 (2025).

Regulations, Statistics and the Rise of Digital Asset. "Update on Digital Asset Regulations and Rules Around the World 2024," n.d.

Santoni, Giulio. "Personal Data as a Market Commodity: Legal Irritants from China'experience." *European Journal of Privacy Law and Technologies* 2023, no.

1 (2023).

Secretariat, ASEAN. *ASEAN Digital Economy Framework Agreement (DEF): Policy Overview*. ASEAN, 2023.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020).

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (2024).

Shahul Ikram, Nur Adlin Hanisah. "Data Breaches Exit Strategy: A Comparative Analysis Of Data Privacy Laws." *Malaysian Journal of Syariah and Law* 12, no. 1 (2024).

Silviani, Ninne Zahara, Rina Shahriyani Shahrullah, Vanessa Riarta Atmaja, and Park Ji Hyun. "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea." *Jurnal Hukum Dan Peradilan* 12, no. 3 (2023).

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime*, 2021.

Suwondo, Denny. "The Legal Protection of Personal Data in the Perspective of Human Rights." *Law Development Journal* 5, no. 4 (2024).

Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula. "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies." *Computer Law and Security Review* 34, no. 1 (2018).

Tukur, Muhammad, Jens Schneider, Mowafa Househ, Ahmed Haruna Dokoro, Usman Idris Ismail, Muhammad Dawaki, and Marco Agus. "The Metaverse Digital Environments: A Scoping Review of the Challenges, Privacy and Security Issues." *Frontiers in Big Data* 6 (2023): 1301812.

Xynogalas, V. "Metaverse: Searching for Compliance with the General Data Protection Regulation." *International Data Privacy Law*, 2024.

Yang, L, and et al. "Recommendations for Metaverse Governance Based on Technical Standards." *Humanities and Social Sciences Communications*, 2023.

Yang, Liang, Shi-Ting Ni, Yuyang Wang, Ao Yu, Jyh-An Lee, and Pan Hui. "Interoperability of the Metaverse: A Digital Ecosystem Perspective Review." *IEEE Engineering Management Review*, 2025.

Zhang, Chang, and Lexuan Wang. "Virtual Worlds, Real Politics: A Cross-national Comparative Study of Metaverse Policy Approaches." *Politics and Governance* 13 (2025).

Zhao, Ruoyu, Yushu Zhang, Youwen Zhu, Rushi Lan, and Zhongyun Hua. "Metaverse: Security and Privacy Concerns." *Journal of Metaverse*, 2023.

Zhou, Morgana Mo, Zhiyan Qu, Jinhan Wan, Bo Wen, Yaxing Yao, and Zhicong Lu. "Understanding Chinese Internet Users' Perceptions of, and Online Platforms' Compliance with, the Personal Information Protection Law (PIPL)." *Proceedings*

of the ACM on Human-Computer Interaction 8, no. CSCW1 (2024).