Vifada Assumption Journal of Law, E-ISSN 2987-1263

The Urgency of Reformulating Criminal Offences on the Misuse of Personal Data in Indonesia's Crypto Asset Ecosystem

Dian Eka Kusuma Wardani [(1*)] *Amir* [(2)] *Muh. Iqbal* [(3)]

[(1,2,3)] *Faculty of Law, Universitas Sawerigading Makassar, Indonesia*

Received: 2025, 02, 21 **Accepted:** 2025, 10, 29
Available online: 2025, 11, 30

*Corresponding author.
E-mail addresses: dianunsa@gmail.com, amir013@gmail.com, iqbalmuh@gmail.com

KEYWORDS

Keywords:
Personal Data Protection; Crypto Assets; Criminal Law.

Conflict of Interest Statement:
The author(s) declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

ABSTRACT

Purpose: This study examines the urgency of reformulating criminal offences for the misuse of personal data within Indonesia's crypto-asset ecosystem, based on the hypothesis that current offence design is not commensurate with the level of risk and complexity of crypto data-processing practices.

Research Design and Methodology: Using a normative legal method with a doctrinal design, this research is supported by conceptual, comparative, and analytical approaches to national legislation, data-protection and crypto-asset regimes in several countries, and relevant scholarly literature and institutional reports.

Findings and Discussion: The study finds that although the Personal Data Protection Law, the Electronic Information and Transactions Law, and sectoral crypto-asset regulations provide a basis for criminalisation, existing offence constructions remain general, fragmented, and insufficiently responsive to the technological and institutional characteristics of the crypto ecosystem.

Implications: The study proposes a sector-specific model of criminalisation that clearly articulates the protected legal interests, liable subjects, prohibited conducts, and standards of corporate criminal liability, and offers a conceptual foundation for legislative reform while inviting further mixed normative-empirical research on its operationalisation.

Introduction

The development of the digital economy and the information technology revolution have transformed personal data into a "strategic asset" with high economic value that is at the same time highly vulnerable to misuse. Within this landscape, the crypto-asset ecosystem introduces a new configuration of legal relationships between platform providers, users, and the state, as all investment, storage, and value-exchange activities rely on digital infrastructure that massively absorbs and processes personal data. The misuse of personal data in this context is no longer merely a matter of business ethics, but has shifted into a potential criminal offence that threatens citizens' constitutional rights to privacy and security.

In the context of national law, Law Number 27 of 2022 on Personal Data Protection (the PDP Law) explicitly positions the protection of personal data as part of human rights, while at the same time criminalising the acts of unlawfully obtaining, disclosing, and using personal data belonging to another, subject to significant penalties of imprisonment and fines.[1] On the other hand, the Electronic Information and Transactions Law (ITE Law) and its amendments provide a basis for criminal sanctions against illegal access, manipulation, and diversion of electronic information, including personal data

[1] Muhammad Khaeruddin Hamsin, Abdul Halim, and Rizaldy Anggriawan, "Addressing Cybercrime in the Sharia Digital Wallet Industry: A Legal Perspective in the Indonesian Context," ed. D. Mutiarin et al., *E3S Web of Conferences* 440 (November 1, 2023): 04016, https://doi.org/10.1051/e3sconf/202344004016.

stored or processed through electronic systems. Thus, normatively, Indonesia has recognised that the misuse of personal data constitutes a criminal offence, although the construction of its constitutive elements remains general and has not yet specifically targeted the crypto-asset context.

The crypto-asset ecosystem adds a further layer of complexity because it combines the decentralised characteristics of blockchain with centralised mechanisms at exchanges (centralised exchanges) that conduct know-your-customer (KYC) and customer due diligence (CDD) processes. On the one hand, blockchain technology enables the use of pseudonymisation and cryptography that should, in principle, enhance data protection; on the other hand, platform operators store vast repositories of users' identity data (ID cards, passports, addresses, phone numbers, transaction records), which become prime targets for cyberattacks and data breaches. Studies on the pseudonymisation of personal data of crypto-asset users underscore that such data, even when pseudonymised, can still potentially be re-identified and therefore requires a robust protective framework within the Indonesian legal system.[2]

Indonesia's regulatory framework on crypto-assets has evolved from a futures commodity regime under the Commodity Futures Trading Regulatory Agency (Bappebti) to a digital financial asset regime under the Financial Services Authority (OJK). Minister of Trade regulations and Bappebti rules govern crypto-assets as commodities that may be traded on the physical market, whereas OJK Regulation Number 27 of 2024 on the Organisation of Digital Financial Asset Trading (including crypto-assets) restructures regulatory authority, reporting obligations, and governance standards for digital financial asset business actors. However, these regulations still place greater emphasis on financial system stability and general investor protection, rather than specifically formulating criminal offences for the misuse of personal data by business actors or third parties within the crypto ecosystem.

At the international level, the European Union has long developed the General Data Protection Regulation (GDPR), which sets high standards on consent, transparency, accountability, and very severe administrative sanctions for violations of personal data protection, including where data processing is carried out in the context of financial services and crypto-assets. This policy is reinforced by the Markets in Crypto-Assets Regulation (MiCA), which standardises crypto market rules in the European Union, with an emphasis on transparency, investor protection, and a risk-based supervisory framework for crypto-asset service providers. Japan has taken a similar path through the Act on the Protection of Personal Information (APPI), which is strictly applied to digital system operators, including crypto-asset providers, and requires robust data governance as well as accountability for every form of personal data processing.

A number of recent studies, both in Indonesia and abroad, demonstrate growing attention to the intersection between crypto-assets, personal data protection, and criminal law. Research on personal data protection and criminal sanctions under the PDP Law highlights that the criminal sanctions regime in Indonesia still faces implementation challenges, including clarifying the types of conduct that are to be classified as data-related offences and the appropriate model of corporate liability.[3] On the other hand, studies on the risks and potential misuse of crypto-assets as instruments of crime, particularly money laundering, show that the anonymity, speed, and cross-border nature of crypto-assets create a shadow space that is difficult for traditional law enforcement mechanisms to reach.[4] However, few studies specifically dissect the construction of criminal offences for the misuse of personal data within the crypto ecosystem, whether from the perspective of the formulation of offence elements, the subjects of law, or the relationship between data protection regulation and digital financial sector regulation.

Academic debate has also emerged regarding the status of personal data as an object of protection under criminal law. Some studies criticise the limitations of provisions in the classical Criminal Code, such as Article 362 on theft, when confronted with immaterial digital objects like personal data, and question how the elements of "unlawfulness" and "taking a thing, wholly or partly belonging to

[2] I K. O. Mayuna, R. Dewantara, and P. A. Ruslijanto, "Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia," *Journal of Digital Technologies and Law* 3, no. 2 (July 6, 2025): 275–303, https://doi.org/10.21202/jdtl.2025.12.

[3] Kukuh Dwi Kurniawan et al., "Criminal Sanctions and Personal Data Protection in Indonesia," *Lex Publica* 11, no. 2 (December 3, 2024): 221–47, https://doi.org/10.58829/lp.11.2.2024.255.

[4] Muh Afdal Yanuar, "Risiko Dan Posibilitas Penyalahgunaan Aset Kripto Dalam Kejahatan Pencucian Uang: Risks and Possibilities of Misuse of Crypto Assets in Money Laundering Crimes," *Majalah Hukum Nasional* 52, no. 2 (2022): 169–88.

another" should be understood in the context of digital data theft.[5] In the realm of legal theory, this issue is linked to the Rechtsgutstheorie (the theory of legally protected interests), the human rights theory of privacy, systems theory of law, and risk-based regulation approaches, which are increasingly dominant in the regulation of crypto-assets in Europe.[6] Taken together, this body of discourse demonstrates the need for a reconstruction of criminal offences that no longer rests on a paradigm of tangible objects, but instead focuses on protecting the legal interest in personal data as a manifestation of the right to privacy and individual autonomy.

At the empirical level, the phenomenon of personal data misuse within the crypto-asset ecosystem in Indonesia and globally shows a worrying trend. The surge in the number of retail crypto investors in Indonesia, accompanied by the proliferation of crypto-asset trading platforms, has turned KYC databases into one of the most valuable yet most vulnerable assets. Studies on consumer protection and crypto-asset risks in Indonesia, including those examining hacking practices targeting domestic crypto exchanges and local token rug-pull cases, affirm that user losses are not limited to the disappearance of crypto-assets, but also include the potential leakage of personal data that may subsequently be exploited for other crimes.[7] Patterns of cyberattacks against crypto platforms tend to target both financial infrastructure and data infrastructure.

More broadly, international reports on security incidents at both centralised and decentralised crypto exchanges indicate that the leakage of users' personal data has become one of the main impacts of such attacks. Empirical studies on incidents at centralised exchanges (CEX) and decentralised exchanges (DEX) reveal that security breaches not only cause financial losses, but also expose sensitive data such as email addresses, phone numbers, and official identities, which are then exploited for identity theft and subsequent attacks.[8]Cases such as fraudulent schemes that exploit illegal access to customer data at major global exchanges and data leaks involving users of bankrupt crypto-exchange subsidiaries illustrate how personal data has become a criminal commodity traded on the digital black market.[9]

In Indonesia, although media coverage more frequently highlights the loss of crypto-assets, fraudulent schemes exploiting personal data such as phishing that mimics official exchange notifications, account takeovers via SIM swapping, and identity fraud based on leaked KYC data are being reported with increasing frequency.[10] This phenomenon shows that offences involving the misuse of personal data in the crypto ecosystem do not always stand alone, but often intersect with other offences such as fraud, money laundering, and banking crimes. Legal studies on personal data protection in Indonesia emphasise that the trade in personal data, including that related to the financial sector, has evolved into a distinct illegal market, with criminal penalties that are severe in nominal terms yet have not fully created a deterrent effect due to weak law enforcement and the difficulty of proving data flows.

In the international context, offences involving the misuse of personal data related to crypto-assets frequently take the form of fraudulent schemes that exploit the legitimacy of major exchange brands to obtain users' seed phrases or credentials, subsequently draining the victims' crypto-assets and laundering the proceeds of crime through gambling platforms and swapping services.[11] In addition,

---

[5] Camiliya Fakhriyah Garnita and Kuswandi Kuswandi, "Analisis Kriminologi Dalam Tindak Pidana Pencurian Data Pribadi Di Era Digital," *Indonesian Journal of Law and Justice* 3, no. 2 (December 28, 2025): 11, https://doi.org/10.47134/ijlj.v3i2.5288.

[6] Gunawan A. Tauda, Andy Omara, and Gioia Arnone, "Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union," *BESTUUR* 11, no. 1 (August) (April 12, 2023): 1, https://doi.org/10.20961/bestuur.v11i1.67125.

[7] Dominic Imanuel Vidianto et al., "Legal Protection for Consumers Who Lose Assets on Crypto Exchange Platforms in Indonesia: A Case Study of Hacking and Rug Pull," *Justice Voice* 4, no. 2 (December 31, 2025): 83–93, https://doi.org/10.37893/jv.v4i2.1204.

[8] Akinlemi Olushola and S. P. Meenakshi, "Cybersecurity Crimes in Cryptocurrency Exchanges (2009–2024) and Emerging Quantum Threats: The Largest Unified Dataset of CEX and DEX Incidents," *Frontiers in Blockchain* 8 (November 27, 2025), https://doi.org/10.3389/fbloc.2025.1713637.

[9] Adik Nur Luthiya, Benny Irawan, and Rena Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi," *Jurnal Hukum Pidana Dan Kriminologi* 2, no. 2 (September 22, 2021): 14–29, https://doi.org/10.51370/jhpk.v2i2.43.

[10] Gunsu Nurmansyah, Rudi Natamiharja, and Ikhsan Setiawan, "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach," *Pancasila and Law Review* 6, no. 1 (August 25, 2025): 15–44, https://doi.org/10.25041/plr.v6i1.4138.

[11] Irina Astrakhantseva, Roman Astrakhantsev, and Alexey Los, "Cryptocurrency Fraud Schemes Analysis," ed. A.D. Nazarov, *SHS Web of Conferences* 106 (May 18, 2021): 02001, https://doi.org/10.1051/shsconf/202110602001.

the exposure of GDPR violation cases involving data-driven technology companies, as well as efforts by several European jurisdictions to test the possibility of corporate criminal liability and liability of corporate managers for serious personal data breaches, indicate a global trend toward more assertive criminalisation of large-scale data misuse.[12] The crypto ecosystem, with its cross-border and pseudo-anonymous characteristics, has become fertile ground for new modi operandi that challenge the traditional jurisdictional boundaries of criminal law.

From the perspective of Indonesian criminal law, these conditions give rise to a number of conceptual and normative issues. First, there is still debate on how to qualify acts involving the misuse of crypto-asset users' personal data: whether they fall solely under the specific offences in the PDP Law, or may also be construed as forms of theft, fraud, or illegal access under the ITE Law, and to what extent the principle of *lex specialis derogat legi generali* operates when several provisions potentially overlap. Second, the boundaries of corporate criminal liability for crypto-exchange operators that negligently fail to protect users' personal data, as compared to the liability of individual perpetrators of cyber intrusions or employees who abuse their access authority, remain unclear.

A normative gap is also apparent when the generally applicable, technology-neutral framework for personal data protection is juxtaposed with sectoral crypto-asset regulations that focus on financial system stability and investor protection. MiCA and the broader digital finance framework in the European Union have begun to integrate these approaches by positioning data governance and system security obligations as an integral part of investor protection and the stability of crypto markets.[13] Indonesia does not yet have a comprehensive framework that explicitly formulates offences for the misuse of personal data by crypto-asset service providers, including standards of due diligence, obligations to report data-breach incidents, and the qualification of acts giving rise to criminal liability. This creates a wide scope for interpretation and potentially generates legal uncertainty for both law enforcement authorities and business actors.

In addition, there is a conceptual tension between core principles of personal data protection—such as data minimisation, purpose limitation, and the right to be forgotten—and the immutable, distributed nature of blockchain technology. The literature on data protection in blockchain systems underscores the importance of technical design measures such as pseudonymisation and off-chain storage; however, from a criminal law perspective, questions remain as to the point at which a failure to design a "privacy by design" system may be regarded as criminal negligence, and when data processing that exceeds its original purpose can be qualified as misuse of personal data.[14] These challenges become even more complex when violations are committed by entities operating across jurisdictions, thereby giving rise to difficulties in clearly determining the *locus* and *tempus delicti*.

Based on the foregoing discussion, it is evident that there is a gap between the empirical developments in the misuse of personal data within the crypto-asset ecosystem and the current normative design of criminal offences. Existing studies generally continue to focus on personal data protection in a broad sense or on the use of crypto-assets as instruments for traditional offences such as money laundering, while specific offence constructions concerning the misuse of crypto-asset users' personal data have not been extensively developed, particularly from the perspective of Indonesian criminal law, which adheres to the civil law tradition.[15] This gap creates a lack of synchronisation between the practical needs of law enforcement and the conceptual and normative tools currently available to legislators and law enforcement authorities.

Therefore, this study is directed at addressing several key questions: how the characteristics of offences involving the misuse of personal data within the crypto-asset ecosystem are to be understood under the current Indonesian positive law; to what extent the regulatory frameworks of other jurisdictions, such as the European Union and Japan, provide models for dealing with similar offences that may serve as comparative references; and how the ideal formulation of criminal offences for the

[12] Glenn Wijaya, "Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum," *Law Review* 19, no. 3 (August 12, 2020): 326, https://doi.org/10.19166/lr.v19i3.2510.
[13] Hasret Ozan Sevim, "European Union's Approach to Crypto-Assets and Distributed Ledger Technologies," *Studia Sieci Uniwersytetów Pogranicza* 6 (2022): 139–47, https://doi.org/10.15290/sup.2022.06.10.
[14] Mayuna, Dewantara, and Ruslijanto, "Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia."
[15] Yanuar, "Risiko Dan Posibilitas Penyalahgunaan Aset Kripto Dalam Kejahatan Pencucian Uang: Risks and Possibilities of Misuse of Crypto Assets in Money Laundering Crimes."

misuse of personal data in Indonesia's crypto-asset ecosystem should be designed so as to align with the principles of human rights protection, legal certainty, and effective law enforcement in a cross-border digital space. By articulating these questions, the study seeks to fill the gap between empirical developments and a still-fragmented theoretical construction.

More specifically, this study aims to develop a comprehensive normative construct regarding the urgency of reformulating criminal offences concerning the misuse of personal data within Indonesia's crypto-asset ecosystem, through an analysis of national positive law, comparisons with foreign legal systems, and an examination of relevant legal theories. The novelty of this research lies in its specific focus on the intersection between personal data protection, crypto-assets, and criminal law, with an orientation toward offence reformulation that not only adds new statutory provisions but also restructures the paradigm of protecting the legal interest in personal data as a human right amid digital transformation. Accordingly, this study is expected to make a conceptual contribution to the development of criminal law scholarship and, at the same time, provide an academic foundation for legislative reform in the fields of personal data protection and crypto-asset regulation in Indonesia.

Literature Review

Personal Data Protection and Criminal Offences in Indonesian Positive Law

Personal data protection in Indonesia generally stems from the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) as a major milestone in recognising the right to personal data as part of human rights and a legal interest worthy of criminal law protection. The PDP Law regulates principles, categories of personal data, data subjects' rights, the obligations of data controllers and processors, as well as administrative and criminal sanctions for acts such as unlawfully obtaining, disclosing, and using personal data. Several normative analyses emphasise that the PDP Law was designed to address the previously fragmented regulatory framework (the Government Regulation on Electronic Systems and Transactions and Ministerial Regulations of the Ministry of Communications and Informatics), which was regarded as weak in terms of business actors' compliance and insufficient in providing a deterrent effect against serious violations.[16] In this context, the misuse of personal data is no longer treated merely as a civil or administrative matter, but has been explicitly constructed as a criminal offence.

Indonesian data and criminal law scholars note that the enactment of the PDP Law opens up opportunities to strengthen privacy protection, but at the same time raises implementation challenges. Syailendra, Yuniarti, and other authors, for example, point out that although the institutional framework and data subjects' rights have been accommodated, concerns remain regarding the effectiveness of enforcement, particularly in proving the element of unlawfulness and in allocating the burden of responsibility between data controllers and data processors.[17] Kurniawan et al. specifically analyse the criminal sanctions under the PDP Law and conclude that, normatively, Indonesia has adopted a pattern similar to that of other jurisdictions (a combination of administrative and criminal sanctions). However, the application of criminal sanctions still requires clearer stipulation regarding which actors may be held liable, whether individuals or corporations, as well as the causal relationship in cases of data breaches.[18]

From a statutory perspective, Indonesian literature situates offences involving the misuse of personal data at the intersection of the PDP Law, the Electronic Information and Transactions Law (ITE Law) and its amendments, and the provisions of the classical Criminal Code. The ITE Law criminalises illegal access, interception, manipulation, and diversion of electronic information, which may encompass personal data, whereas the Criminal Code still contains concepts of "property" and "theft" that were developed in the context of tangible objects, thereby giving rise to debate when

[16] Valentina Ancillia Simbolon and Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (December 30, 2022): 178, https://doi.org/10.31314/pjia.11.2.178-190.2022.
[17] Moody Rizqy Syailendra, "Personal Data Protection Law in Indonesia: Challenges And Opportunities," *Indonesia Law Review* 14, no. 2 (August 31, 2024), https://doi.org/10.15742/ilrev.v14n2.4.
[18] Kurniawan et al., "Criminal Sanctions and Personal Data Protection in Indonesia."

applied to digital objects.[19] On the other hand, sectoral regulations in the field of crypto-assets from the futures commodity regime under Bappebti to their reclassification as digital financial assets under the Financial Services Authority (OJK) through OJK Regulation 27/2024 have primarily focused on market stability, investor protection, and platform governance, rather than on formulating specific criminal offences for the misuse of personal data by crypto-asset service providers.

Overall, the national literature shows that, normatively, Indonesia already has a basis for criminalising the misuse of personal data through the PDP Law and the ITE Law, but there is still no offence construction explicitly directed at the crypto-asset ecosystem. This gap is evident in the lack of integration between data protection norms and digital financial sector regulations within a single specific offence framework, while market practice demonstrates an increasing volume of KYC data processing and heightened risks of data breaches on crypto platforms.[20] It can thus be affirmed that there is a need to reformulate criminal offences that do not merely rely on general norms, but specifically target modes of personal data misuse within the crypto-asset ecosystem, including a clear delineation of the subjects of law, forms of culpability, and corporate standards of due diligence.

International Regulation and Comparative Law on the Misuse of Personal Data in the Crypto-Asset Ecosystem

At the international level, the literature shows that personal data protection has evolved through a combination of data protection regimes and criminal law instruments. In the European Union, the General Data Protection Regulation (GDPR) sets high standards regarding legal bases for processing, data subject rights, controller obligations, and data breach notification duties, accompanied by very severe administrative sanctions and the possibility of civil and criminal liability under the national laws of Member States.[21]

In the United Kingdom, the UK GDPR and the Data Protection Act 2018 explicitly criminalise certain data-related acts, such as the re-identification of de-identified data without the controller's consent and the processing of data in connection with criminal offences, thereby affirming the penal dimension of personal data protection.[22] Japan, through the Act on the Protection of Personal Information (APPI), has adopted a similar approach, imposing stringent obligations on business operators and providing for substantial fines as well as imprisonment for individuals and corporations that misuse or leak personal data.[23]

Comparative literature shows that these three regimes (the GDPR, the UK GDPR/Data Protection Act 2018, and the APPI) all shift the paradigm of data protection from being merely a private right towards a public interest that deserves protection through criminal law. Simbolon, Kurniawan, and several other scholars position Indonesia's PDP Law within the same spectrum as the GDPR and APPI, but emphasise that those jurisdictions have been quicker to develop enforcement mechanisms, including criminal sanctions that explicitly attach to corporations and their management.[24] In Europe, recent discourse has also evolved around the standard of damage that can be compensated under Article 82 of the GDPR, illustrating that personal data breaches are understood not merely as administrative violations, but as events that may give rise to civil harm and even trigger a criminal law response.[25]

In the specific context of crypto-assets, the European Union has introduced the Markets in Crypto-Assets Regulation (MiCA) as a comprehensive framework that standardises the rules on the issuance,

[19] Aliman, "Criminal Law Implications of Personal Data Misuse in the Digital Age ," *International Journal of Health, Economics, and Social Sciences (IJHESS)* 7, no. 2 SE-Articles (April 30, 2025): 986–991, https://doi.org/10.56338/ijhess.v7i2.8300.
[20] Kurniawan et al., "Criminal Sanctions and Personal Data Protection in Indonesia."
[21] Chris Norval et al., "Data Protection and Tech Startups: The Need for Attention, Support, and Scrutiny," *Policy & Internet* 13, no. 2 (June 7, 2021): 278–99, https://doi.org/10.1002/poi3.255.
[22] Uu Nurul Huda, Dian Rachmat Gumelar, and Alwi Al Hadad, "Fortifying Democracy: Deploying Electoral Justice for Robust Personal Data Protection in the Indonesian Election," *Khazanah Hukum* 6, no. 1 (March 1, 2024): 24–33, https://doi.org/10.15575/kh.v6i1.30734.
[23] Dewi Sulistianingsih et al., "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)," *Masalah-Masalah Hukum* 52, no. 1 (March 31, 2023): 97–106, https://doi.org/10.14710/mmh.52.1.2023.97-106.
[24] Simbolon and Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation."
[25] Jonas Knetsch, "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases," *Journal of European Tort Law* 13, no. 2 (August 4, 2022): 132–53, https://doi.org/10.1515/jetl-2022-0008.

trading, and provision of crypto-asset services, with the primary aims of safeguarding market integrity, financial stability, and investor protection.[26] Although MiCA does not function as a data protection regulation, it is designed to operate alongside the GDPR: crypto-asset service providers (CASPs) are required to comply with standards of transparency, risk disclosure, governance, and cybersecurity which, in practice, demand data governance aligned with GDPR principles. In Japan, the application of the APPI to digital platform operators, including crypto-asset service providers, reflects a similar pattern: serious violations involving unlawful data processing and transfers may result in criminal sanctions for business operators and their management, in addition to administrative penalties and civil liability.[27]

The literature also highlights a number of contemporary cases and debates that underscore a trend toward the criminalisation of data misuse in the digital and financial ecosystem. In Europe, for example, the imposition of GDPR fines on technology companies and initiatives to test criminal liability for massive data breaches including cases involving the processing of biometric data serve as important references for how data violations are framed as serious crimes rather than merely administrative infractions. Within the crypto ecosystem, the increasingly stringent supervision of CASPs by ESMA, including criticism of misleading marketing practices concerning regulatory status under MiCA, reflects regulators' concern that exploiting regulatory gaps can expose investors' data and assets to high levels of risk.

From this comparative review, it can be concluded that the global trend is moving toward strengthening the synergy between personal data protection regimes and sectoral regulation of crypto-assets, through a firm combination of administrative and criminal sanctions against data misuse. Regimes such as the GDPR, the Data Protection Act 2018, the APPI, and MiCA demonstrate that the protection of personal data within the crypto ecosystem cannot be separated from clearly formulated criminal offences, robust supervisory mechanisms, and stringent data-governance standards for platform operators. From this perspective, Indonesia's position, as reflected in the PDP Law and the regulation of digital financial assets, remains at an early stage of integration: the normative foundation for data protection has been established, but it has not yet been followed by specific offence formulations that explicitly govern the misuse of personal data in the crypto-asset ecosystem. This gap, both theoretically and practically, reinforces the urgency of the criminal-law offence reformulation that forms the focus of this article.

Research Design and Methodology

The research method employed in this article is normative legal research with a doctrinal study design, relying on an analysis of statutes, legal doctrines, and judicial decisions relevant to the issue of reformulating offences concerning the misuse of personal data within Indonesia's crypto-asset ecosystem. The approaches used include: a conceptual approach to trace and rearticulate key concepts such as personal data, legally protected interests (*rechtsgut*), offences involving data misuse, and the characteristics of the crypto-asset ecosystem; a comparative approach to examine and compare the regulatory frameworks and practices of several jurisdictions, such as the European Union and Japan, with the position of Indonesian law; and an analytical approach to test the coherence, gaps, and disharmony of norms in the PDP Law, the ITE Law, crypto-asset regulations, and relevant principles of criminal law in light of the research background and problem delimitation that have been established.

The research materials consist of primary legal materials (national and international legislation related to personal data protection and crypto-assets), secondary legal materials (literature, journal articles, expert opinions, and reports issued by credible institutions), and tertiary legal materials (legal dictionaries, encyclopaedias, and indexes). Data collection is carried out through library research and searches of legal and scientific databases, using an instrument in the form of a legal-issue

[26] Vladlena Benson et al., "Harmonising Cryptocurrency Regulation in Europe: Opportunities for Preventing Illicit Transactions," *European Journal of Law and Economics* 57, no. 1–2 (April 4, 2024): 37–61, https://doi.org/10.1007/s10657-024-09797-w.
[27] Dian Purwaningrum Soemitro, Muhammad Arvin Wicaksono, and Nur Aini Putri, "Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore," *SIGn Jurnal Hukum* 5, no. 1 (July 31, 2023): 155–67, https://doi.org/10.37276/sjh.v5i1.272.

identification guideline to select and classify legal materials in accordance with the research questions. The data collected comprise norms, concepts, and legal arguments, which are then analysed qualitatively through the stages of inventory, systematisation, interpretation, and legal argumentation, arranged in a sequential and logical manner to answer the research questions, assess the extent to which the existing offence design aligns with the practical needs of law enforcement, and formulate a model for the reformulation of criminal offences concerning the misuse of personal data within Indonesia's crypto-asset ecosystem.

Findings and Discussion

Normative Construction and Gaps in Criminal Offences Concerning the Misuse of Personal Data in Indonesia's Crypto-Asset Ecosystem

Findings

The offence of misusing personal data within the crypto-asset ecosystem has characteristics that differ from data misuse in conventional digital services. In the crypto ecosystem, users' personal data include not only basic identity information such as name, address, and identification number, but also financial data and risk profiles collected through know-your-customer (KYC) processes, on-chain and off-chain transaction data, and various other digital markers that allow the tracking of investment behaviour. The literature on the pseudonymisation of personal data of crypto-asset users emphasises that even when user identities are pseudonymised at the blockchain level, such data can still be correlated with real-world identities when combined with KYC data held by exchanges. Consequently, data misuse in this context can give rise to layered harms: loss of privacy, identity abuse, and further financial exploitation.[28]

From the perspective of national regulation, an examination of Law Number 27 of 2022 on Personal Data Protection indicates that Indonesian positive law has, in fact, criminalised acts of unlawfully obtaining, collecting, disclosing, and using personal data belonging to another, with the threat of substantial imprisonment and fines. The provisions of the PDP Law position personal data as an object of legal protection and recognise data subjects' rights to claim compensation for unlawful data processing, accompanied by obligations imposed on data controllers and processors to implement principles such as purpose limitation, data minimisation, and secure processing.[29] However, these criminal provisions are designed to be technology-neutral and do not explicitly refer to the crypto-asset context, so the offence construction remains general in nature and must be reinterpreted when applied to modes of data misuse at crypto exchanges and digital wallet providers.

The relationship between personal data protection and the crypto-asset ecosystem in Indonesian law has become increasingly complex following the transfer of regulatory and supervisory authority over crypto-assets from Bappebti to the Financial Services Authority (OJK). Through OJK Regulation 27/2024 on the Organisation of Digital Financial Asset Trading, which is further reinforced by OJK Regulation 23/2025, OJK has established an institutional and governance framework for digital financial asset trading providers (including crypto-assets), imposing licensing requirements, periodic and incidental reporting obligations, as well as direct and indirect supervisory mechanisms by OJK.[30] Within this framework, providers are required to maintain market integrity, prevent abnormal transactions, and report suspicious financial transactions; however, the protection of users' personal data is largely relegated to general compliance with the PDP Law and the anti-money laundering regime, without any specific offence formulation that directly links failures in data protection to clearly defined criminal sanctions in the crypto-asset sector.

The comparative analysis with international regimes shows that several jurisdictions have already established a closer linkage between data protection regulation and crypto-asset regulation. In the

[28] Mayuna, Dewantara, and Ruslijanto, "Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia."
[29] Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (September 28, 2021): 177, https://doi.org/10.25072/jwy.v5i2.460.
[30] Maria Arbina and M Ilham F Putuhena, "Tata Kelola Pembentukan Regulasi Terkait Perdagangan Mata Uang Kripto (Cryptocurrency) Sebagai Aset Kripto (Crypto Asset)," *Mahadi: Indonesia Journal of Law* 1, no. 1 (February 10, 2022): 33–57, https://doi.org/10.32734/mah.v1i1.8314.

European Union, the GDPR sets out in detail the legal bases for processing personal data, data subject rights, controller obligations, and severe sanctions for violations, while MiCA establishes a comprehensive framework for the issuance and trading of crypto-assets, including obligations of transparency, risk disclosure, governance, and the safeguarding of users' assets by crypto-asset service providers (CASPs).[31] The analysis of the relationship between the GDPR and MiCA shows that, in practice, CASPs are required to implement stringent data protection standards because they process various types of personal data (identity data, contact data, authentication data, transaction data). As a result, serious breaches of data protection obligations may trigger administrative sanctions, civil claims, and even criminal liability under the national laws of Member States.[32]

Empirically, the risk landscape in Indonesia shows that the vulnerability of crypto-assets to misuse, including data misuse, is recognised in a number of studies and policy reports, even though publications on concrete cases of personal data misuse at domestic crypto exchanges remain relatively limited and tend not to be disclosed transparently. The Indonesian Corruption Watch report on the risks of using crypto-assets for criminal activities, for example, emphasises that the anonymous, cross-border, and rapid nature of crypto transactions creates gaps for new criminal schemes that are difficult for law enforcement authorities to monitor.[33] On the other hand, studies on digital assets and personal data protection in Indonesia underline that the collection and processing of personal data in digital services, including digital finance, take place on a massive scale, while data governance and the enforcement of sanctions for violations remain far from optimal.[34] This situation enables the misuse of crypto-asset users' personal data through leaks of KYC databases, the sale of data to third parties, or excessive profiling practices that do not necessarily result in criminal enforcement.

Viewed on a global scale, empirical data on personal data breaches and misuse at crypto exchanges provide a concrete picture of the types of crimes that also threaten users in Indonesia. Several reports have revealed major incidents at leading crypto exchanges, such as a security breach that led to the leakage of data from nearly 70,000 Coinbase customers in an extortion scheme, in which users' names, addresses, phone numbers, and identity documents were illegally accessed and used as objects of threats to publish them.[35] Conversely, lists of the ten largest hacks against centralised exchanges show that cyberattacks on crypto exchanges often not only drain crypto-assets, but also open up the possibility of access to systems and databases that store users' sensitive information.[36] Although these incidents have occurred outside Indonesia's jurisdiction, the attack patterns and modes of personal data exploitation that have emerged strongly indicate that similar threats may be posed to domestic crypto-asset providers if data security governance is not strengthened and is not supported by an adequate construction of criminal offences.

Based on this normative and empirical mapping, it may be concluded that there is no absolute legal vacuum in Indonesia regarding the misuse of personal data in the crypto-asset ecosystem, since the PDP Law and the ITE Law provide a general basis for criminalising the unlawful acquisition and use of personal data[37], meanwhile, OJK Regulation 27/2024 in conjunction with OJK Regulation 23/2025 regulates governance and reporting obligations for digital financial asset trading providers. However, there remains a significant normative gap: **First**, the absence of a specific offence that explicitly links failures in data protection by crypto-exchange operators to corporate criminal liability and the liability of their management; **Second**, the lack of clear obligations to report data-breach incidents to the

[31] Jean-Baptiste Poulle et al., "Markets in Crypto-Assets (MiCA) Regulation," in *EU Banking and Financial Regulation* (Edward Elgar Publishing, 2024), 662–69, https://doi.org/10.4337/9781035301959.00100.
[32] Els De Busser, "EU-US Digital Data Exchange to Combat Financial Crime: Fast Is the New Slow," *German Law Journal* 19, no. 5 (October 6, 2018): 1251–67, https://doi.org/10.1017/S2071832200023026.
[33] Okta Ariani and Aji Lukman Ibrahim, "Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia," *JURNAL USM LAW REVIEW* 7, no. 1 (December 31, 2023): 30–44, https://doi.org/10.26623/julr.v7i1.8027.
[34] Admiral Admiral and Mega Ardina Pauck, "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services," *Lex Scientia Law Review* 7, no. 2 (November 30, 2023): 995–1048, https://doi.org/10.15294/lesrev.v7i2.77881.
[35] S. V. Muradyan, "Digital Assets: Legal Regulation and Estimation of Risks," *Journal of Digital Technologies and Law* 1, no. 1 (March 15, 2023): 123–51, https://doi.org/10.21202/jdtl.2023.5.
[36] Chris Gilbert and Mercy Gilbert, "Patterns and Vulnerabilities of Cryptocurrency-Related Cybercrimes," *SSRN Electronic Journal*, 2025, https://doi.org/10.2139/ssrn.5196069.
[37] Muhammad Gustryan and Zainal Arifin Hoesein, "Peran Undang-Undang ITE Dan Undang-Undang Perlindungan Data Pribadi Dalam Perlindungan Data Dan Privasi Di Era Ekonomi Digital," *Jurnal Minfo Polgan* 14, no. 2 (December 26, 2025): 3333–43, https://doi.org/10.33395/jmp.v14i2.15746.

authorities and to data subjects within the crypto ecosystem as part of victim-protection mechanisms; and **Third**, the unclear boundaries for applying the *lex specialis* principle among the PDP Law, the ITE Law, and sectoral regulations on crypto-assets. This gap creates a wide room for interpretive discretion on the part of law enforcement and potentially generates legal uncertainty for both business actors and users.

To reinterpret and restructure this normative construct, the study employs several analytical tools drawn from legal theory. At the level of grand theory, human rights theory positions the right to privacy and the protection of personal data as fundamental rights that must be guaranteed by the state, so that the personal data of crypto-asset users are understood as a *rechtsgut* that ought to be an object of protection under criminal law.[38] At the level of middle-range theory, Friedman's legal system theory can be used to unpack how structure (institutions such as the Financial Services Authority, the Ministry of Communication and Informatics, and law enforcement agencies), substance (the PDP Law, the ITE Law, OJK Regulation 27/2024 in conjunction with OJK Regulation 23/2025), and legal culture (business compliance practices and public awareness) interact in responding to the misuse of personal data in the digital sphere. At the level of applied theory, criminal policy theory and risk-based regulation help explain why high-risk sectors such as crypto-assets require specifically formulated offences and stricter standards of due diligence, as reflected in the integration between the GDPR and MiCA in the European Union. By combining these theoretical frameworks, the normative construction and the gaps in offences concerning the misuse of personal data in Indonesia's crypto-asset ecosystem can be analysed more sharply as a basis for designing a reformulated offence model that is more responsive to technological developments and to the need to protect data subjects' rights.

Discussion

This sub-discussion on the normative construction and gaps in offences concerning the misuse of personal data within Indonesia's crypto-asset ecosystem departs from the finding that the current structure of positive law still rests on general norms of data protection and cybercrime, without a specific offence design explicitly tailored to the unique characteristics of crypto-assets. The analysis of the PDP Law, the ITE Law, and sectoral regulations on crypto-assets shows that the existing offence elements are, in principle, capable of encompassing acts of unlawfully obtaining, disclosing, or using personal data, yet they have not fully internalised the technological and economic context of crypto activities, which are heavily characterised by KYC practices, digital wallet management, and cross-border transactions. This lack of synchronisation explains why, normatively, there is no absolute legal vacuum, but functionally a grey area emerges when law enforcement authorities are confronted with modes of data misuse in the crypto ecosystem involving multiple actors and jurisdictions.

When viewed from the basic concept of *rechtsgut*, the personal data of crypto-asset users ought to be positioned as an independent legal interest, and not merely as a derivative of proprietary interests, electronic system security, or public order. The PDP Law explicitly affirms the right to personal data protection as part of human rights, yet its offence formulations remain general in nature and do not anticipate the configuration of legal relations formed around crypto platforms, in which identity data, financial data, and transactional behaviour data are processed in an integrated manner. The gap between the theoretical recognition of personal data as an object of legal protection and the absence of specific offences in the crypto sector raises the question of why the harm suffered by victims of data misuse at crypto exchanges often fails to elicit a proportionate criminal law response and is instead more frequently framed as a business risk or a civil matter between users and service providers.

From the perspective of legal system theory, the findings indicate that the substantive law governing data protection and crypto-assets is not yet fully supported by a coherent legal structure and legal culture. Structurally, authority over these issues is dispersed among the Financial Services Authority (OJK), the Ministry of Communication and Informatics, the Financial Transaction Reports and Analysis Center (PPATK), and law enforcement agencies, each with different and sometimes overlapping mandates. This fragmentation of mandates renders the pathway for handling cases of

[38] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (March 25, 2021): 38, https://doi.org/10.47268/sasi.v27i1.394.

personal data misuse in the crypto ecosystem unclear, particularly when the unlawful conduct simultaneously engages aspects of data protection, anti-money laundering, and consumer protection. At the level of legal culture, the low transparency in disclosing data-breach incidents by service providers and the limited willingness of users to pursue legal remedies further weaken the actualisation of existing criminal norms, so that in practice the available offences become "cold" and rarely invoked.

The comparative discussion with other jurisdictions shows that, in the European Union, for example, the relationship between the GDPR and MiCA is constructed in such a way that serious violations of data protection in the crypto sector are not merely treated as administrative matters, but can serve as an entry point for imposing criminal liability on corporations and their managers. This illustrates why Indonesia, having adopted a broadly similar data protection model through the PDP Law and at the same time transferred crypto-asset supervision to the Financial Services Authority (OJK), needs to consider a much closer integration between these two regimes. Otherwise, a persistent gap will remain between public expectations regarding data protection in crypto activities and the capacity of the legal system to respond with criminal sanctions when violations with far-reaching impacts occur.

At the level of legislative technique, the analysis shows that the relationship between the PDP Law, the ITE Law, and the Criminal Code has the potential to generate conflicts in applying the principle of *lex specialis derogat legi generali* when an act of personal data misuse also contains elements of fraud, theft, or illegal access to electronic systems. In the crypto-asset context, where most interactions take place digitally and involve complex electronic systems, perpetrators frequently combine several modi operandi at once: from hacking databases and phishing for credentials to social engineering. In the absence of clear regulations delineating the scope and priority of each applicable norm, law enforcement authorities may hesitate in determining the appropriate provisions to apply, or may even opt for non-criminal avenues perceived as simpler. This situation deepens the gap between the potential for criminalisation under the written law and the realities of law enforcement practice.

The empirical data gathered indicate that vulnerabilities in KYC processes and user databases at domestic crypto exchanges are not merely hypothetical, but have a concrete basis in the form of uneven security practices and the absence of robust obligations to disclose data-breach incidents to the public. Although not always documented openly, case patterns in the international digital finance and crypto-asset sectors illustrate that once data are breached, they enter a criminal ecosystem that is extremely difficult to disrupt, as they may be traded on the dark market, used for identity theft, or exploited in subsequent fraud schemes. In this context, the absence of a specific offence that clearly criminalises the "misuse of crypto-asset users' personal data" as an autonomous act for example, by service providers that transfer or exploit data beyond KYC purposes makes it difficult for victims to demand criminal accountability and tends to shift the problem into purely contractual or administrative regimes.

The construction of corporate criminal liability constitutes another crucial point that remains insufficiently resolved. Crypto-exchange operators and digital wallet providers in practice occupy the position of data controllers while simultaneously holding technical authority over the infrastructure that stores and processes users' personal data. However, the offence formulations in the PDP Law remain relatively general when addressing the liability of legal entities, whereas sectoral regulations on crypto-assets place greater emphasis on administrative sanctions such as licence revocation or fines. When data breaches or systemic data misuse occur for example, due to system designs that disregard the *privacy by design* principle or business practices that aggressively monetise user data—there is no clear certainty as to whether corporations may be held directly criminally liable, or whether it must first be proven that an individual offender within the corporate structure is responsible. This ambiguity hampers the effective use of criminal law as a control mechanism.

A risk-based criminal policy approach indicates that the crypto-asset sector, given its high level of exposure to cybercrime and money laundering, ought to be prioritised in the formulation of specific offences concerning the misuse of personal data. Research data show that the use of crypto-assets as instruments of crime and as a medium for obscuring transactional trails places retail users in a

vulnerable position, not only in terms of asset loss but also in terms of the fragility of their personal data, which are recorded across multiple layers of transactions and ancillary services. In the absence of specific offences, criminal law tends to arrive too late and operates only once harm has materialised on a large scale, while its preventive function against poor data-governance practices becomes suboptimal. This strengthens the argument that offence reformulation is not merely a matter of adding new provisions, but of recalibrating the priority of the legal interests that the law seeks to protect.

From a human rights theoretical perspective, the normative gaps identified in this study may be read as an indication that the protection of personal data as a fundamental right has not yet been fully internalised within crypto-asset regulatory policy. Although the PDP Law marks an important shift, its integration into sectoral regulations and the supervisory practices of the Financial Services Authority (OJK) remains in a formative stage. As a result, the rights to privacy and personal data protection of crypto-asset users are easily subordinated to other interests, such as market growth, technological innovation, or formal compliance with AML/CFT standards. When data breaches or cases of data misuse occur, policy responses tend to focus on system stability and the restoration of market confidence, rather than on the restoration of data subjects' rights and the enforcement of criminal accountability for such violations.

The foregoing findings also show that Friedman's legal system theory is relevant in explaining why the offence gap persists. Relatively advanced substantive law in the PDP Law is not automatically translated into robust protective practice because of a fragmented institutional structure and a legal culture that does not yet regard personal data breaches as serious crimes. In the crypto-asset context, this is reflected in the scarcity of published cases, the limited number of court decisions that can serve as jurisprudence, and the tendency to resolve data violations through non-penal mechanisms. When the legal system fails to send a clear signal that the misuse of personal data in the crypto sector constitutes a serious offence with criminal consequences, business actors are not compelled to adopt the highest standards of data protection, and users remain in a vulnerable position.

Accordingly, this discussion confirms that the normative construction of offences involving the misuse of personal data within Indonesia's crypto-asset ecosystem is still partial and fragmented. Positive law provides a foundation in the form of the PDP Law, the ITE Law, and sectoral regulations on digital financial assets, but has not yet crystallised into specific offences that explicitly address the unique relationships, risks, and modes of operation in the crypto sector. The gap between the theoretical recognition of personal data as an object of protection under criminal law and the absence of a specific offence design generates uncertainty in law enforcement, weakens the preventive function, and risks reducing the right to personal data protection to a mere normative slogan. It is from this point that the urgency of reformulating criminal offences concerning the misuse of personal data in Indonesia's crypto-asset ecosystem becomes evident, while at the same time opening room for the subsequent sub-discussion to propose a more coherent and responsive normative model.

A Model for Reformulating Criminal Offences on the Misuse of Personal Data in the Crypto-Asset Ecosystem: A Comparative Analysis and Legal-Theoretical Approach

Findings

The reformulation of criminal offences concerning the misuse of personal data within the crypto-asset ecosystem becomes crucial because the research findings reveal an imbalance between the level of risk generated by data processing in crypto activities and the offence design currently available in Indonesian positive law. On the one hand, the Personal Data Protection Law and the Electronic Information and Transactions Law have laid the groundwork for criminalising acts of unlawfully obtaining, disclosing, and using personal data, yet their formulations are general in nature and have not specifically captured the crypto-asset context, which is characterised by a combination of cross-border features, blockchain technology, large-scale KYC practices, and the involvement of business actors operating in the form of digital platforms.[39] On the other hand, sectoral regulations on crypto-

[39] Meriyati Meriyati et al., "Hukum Dan Eksistensi Jual Beli Crypto Untuk Investasi Dalam Perspektif Ekonomi Islam Dan Ekonomi Sosial 'Studi Literasi Dan Komparasi Pada Masyarakat,'" *Jurnal Justisia Ekonomika: Magister Hukum Ekonomi Syariah* 7, no. 2 (December 20, 2023): 869–81, https://doi.org/10.30651/justeko.v7i2.20456.

assets under the financial services authority place greater emphasis on market stability and the financial protection of investors, so that the protection of users' personal data rights has not yet been normatively articulated in the form of specific offences that are commensurate with the risks involved.

From a comparative perspective, this study finds that jurisdictions such as the European Union situate the issue of personal data protection in the crypto-asset ecosystem within an integrative framework that links data protection regulation (such as the GDPR) with crypto market regulation (such as MiCA).[40] That integration is not merely a matter of administrative coordination, but also involves a sanctions framework that allows serious violations of data protection in the crypto sector to result in corporate criminal liability and liability of corporate managers, alongside administrative sanctions and civil liability. This pattern indicates that offence reformulation in Indonesia needs to move towards an explicit recognition that the misuse of personal data in the crypto ecosystem constitutes a form of crime that infringes the legal interests of privacy and data security, while at the same time undermining market integrity and public trust in the digital financial system.

Theoretically, the principal foundation of this offence-reformulation model rests on human rights theory, which views the right to privacy and the protection of personal data as fundamental rights that must be guaranteed by the state,[41] including when those rights are "objectified" in the form of digital traces and KYC databases of crypto-asset users. Using this framework, personal data must not be reduced to a mere commodity that can be traded by business actors, but must instead be regarded as an extension of individual dignity and autonomy. Consequently, the ideal offence formulation must clearly position any collection, processing, and transfer of data beyond legitimate purposes as conduct that potentially violates human rights and is therefore deserving of criminal sanctions, particularly when carried out on a large scale, in a systematic manner, or with far-reaching impacts on data subjects.

The legal system theory provides a second framework for constructing the reformulation model. From this perspective, offence reformulation cannot be confined to merely adding or modifying statutory provisions; it must also be harmonised with the institutional structure and legal culture that will enforce them.[42] The findings show that the involvement of various institutions such as the Financial Services Authority, the Data Protection Authority, the Ministry responsible for the digital sector, and law enforcement agencies requires an offence design that clearly determines who constitutes the subject of law, how the lines of responsibility between corporations and individuals are allocated, and how inter-agency coordination in enforcement is to be carried out. A sound reformulation model will contain norms that stipulate the active obligations of crypto-asset service providers to prevent data misuse, the obligation to report breach incidents to the authorities and data subjects, and a graduated sanctions scheme that links violations of these obligations to criminal liability.

Criminal policy theory and a risk-based regulation approach serve as the third analytical lens justifying the need for sector-specific offences. The research shows that the crypto-asset ecosystem has a high-risk profile in relation to cybercrime and money laundering, and demands heightened sensitivity to data protection given the volume and types of data collected.[43] Within this framework, criminal law is positioned as an *ultimum remedium* that is applied selectively to the most harmful forms of conduct,[44] for example, the misuse of personal data by business actors who deliberately monetise data beyond legitimate purposes, data breaches resulting from gross negligence in system security design, or collusion with offenders who exploit user data for subsequent fraud schemes. An

[40] Tauda, Omara, and Arnone, "Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union."
[41] Tauda, Omara, and Arnone.
[42] Priyo Hutomo and Markus Marselinus Soge, "PERSPEKTIF TEORI SISTEM HUKUM DALAM PEMBAHARUAN PENGATURAN SISTEM PEMASYARAKATAN MILITER," *Legacy: Jurnal Hukum Dan Perundang-Undangan* 1, no. 1 (March 4, 2021): 46–68, https://doi.org/10.21274/legacy.2021.1.1.46-68.
[43] Septhian Eka Adiyatma and Dhita Fitria Maharani, "Cryptocurrency's Control in the Misuse of Money Laundering Acts as an Effort to Maintain the Resilience and Security of the State," *Lex Scientia Law Review* 4, no. 1 (May 8, 2020): 75–88, https://doi.org/10.15294/lesrev.v4i1.38257.
[44] Beby Suryani Fithri, Riswan Munthe, and Anggreni Atmei Lubis, "Asas Ultimum Remedium/The Last Resort Principle Terhadap Pelaku Usaha Dalam Hukum Perlindungan Konsumen," *DOKTRINA: JOURNAL OF LAW* 4, no. 1 (April 30, 2021): 69–84, https://doi.org/10.31289/doktrina.v4i1.4918.

offence reformulation grounded in risk analysis makes it possible to delineate the scope of criminalised conduct in a more proportionate and calibrated manner.

At a more concrete level, the normative and comparative analysis points to the need to formulate an offence that explicitly targets the misuse of crypto-asset users' personal data by service providers and third parties cooperating with them. The elements of such an offence should clearly encompass forms of conduct such as collecting and processing data for purposes beyond those permitted, granting access to third parties without a legal basis, transferring data abroad without adequate safeguards, and failing to implement minimum technical and organisational measures to prevent data breaches that may be qualified as gross negligence.[45] This formulation must be accompanied by a clear designation of corporations and their management as subjects of law, with provisions that allow corporate fault to be proven without always having to identify a single individual perpetrator on the ground.

The reformulation model also needs to clarify the relationship between this specific offence and the existing offences in the PDP Law, the ITE Law, and the general provisions of the Criminal Code, in order to prevent overlap or gaps in application. In an ideal design, the specific offence of misuse of personal data in the crypto-asset ecosystem would operate as *lex specialis* in relation to general data protection offences where the conduct is committed by or through crypto-asset service providers. This would provide clearer guidance for law enforcement authorities as to which provisions should be prioritised, while at the same time reducing the risk of disparities in case handling. Clarifying this relationship is in line with legal system integration theory, which emphasises the importance of coherence and consistency among sub-systems so that the law can function effectively and predictably.

An analytical approach to judgments and enforcement practices in more advanced jurisdictions also shows that offence reformulation must be accompanied by strengthened evidentiary mechanisms and victim protection. In cases of personal data misuse in the crypto sector, proof often depends on digital traces, system logs, and transaction records that can only be accessed through close cooperation between the authorities and business actors.[46] A sound offence model must therefore be accompanied by provisions requiring service providers to securely retain logs for a specified period, to provide access to law enforcement authorities in accordance with legal procedures, and to furnish technical support for the investigative process.[47] On the other hand, victims must be afforded a strong legal position to claim redress and compensation, so that criminal law functions not only in a repressive, but also in a restorative manner.

Overall, this sub-discussion concludes that a model for reformulating criminal offences concerning the misuse of personal data in the crypto-asset ecosystem must be built upon a synergy between human rights theory, legal system theory, and risk-based criminal policy, with comparative reference to international best practices. Reformulation is not merely a matter of drafting new statutory provisions, but an effort to recalibrate the relationships between the state, business actors, and users within the digital economy, so that personal data protection does not remain empty rhetoric but is guaranteed through offence designs that are clear, enforceable, and capable of producing a tangible deterrent effect. Accordingly, the findings of this study provide a conceptual and normative foundation for legislative reform efforts that are more responsive to the evolving dynamics of personal data misuse in Indonesia's crypto-asset sector.

Discussion

This sub-discussion on the model for reformulating criminal offences concerning the misuse of personal data in the crypto-asset ecosystem departs from the core finding that there is an imbalance between the level of risk generated by data collection and processing practices in crypto activities and the offence structure available in Indonesian positive law. Normative data drawn from the

[45] Marlia Hafny Afrilies et al., "Ensuring Construction Workers Legal Protection: A Legal Analysis of Construction Competency Certificates under the Law on Personal Data Protection and Blockchain Frameworks," *Jurnal Pamator : Jurnal Ilmiah Universitas Trunojoyo* 16, no. 4 (January 15, 2024): 810–25, https://doi.org/10.21107/pamator.v16i4.23948.
[46] Dhimas Candra Andrianto, "Perlindungan Hukum Dan Pengenaan Pajak Bagi Investor Cryptocurrency Di Indonesia," *Jurnal Ilmiah Universitas Batanghari Jambi* 22, no. 1 (February 19, 2022): 140, https://doi.org/10.33087/jiubj.v22i1.2014.
[47] Ferdy Arliyanda Putra and Lucky Dafira Nugroho, "Perlindungan Hukum Terhadap Penyalahgunaan Akun Dalam Transaksi Elektronik Melalui Traveloka," *INICIO LEGIS* 2, no. 1 (June 30, 2021), https://doi.org/10.21107/il.v2i1.11081.

Personal Data Protection Law, the ITE Law, and sectoral regulations on crypto-assets show that existing criminalisation remains general in nature, whereas empirically the crypto ecosystem exhibits a configuration of legal relationships that is far more complex than that of conventional digital services. This imbalance affirms the initial hypothesis that, in the absence of an offence design that specifically anticipates the characteristics of crypto-assets, legal protection for users' personal data will tend to lag behind the technological dynamics.

When these analytical results are linked to human rights theory, it becomes apparent that the position of personal data as a manifestation of the right to privacy and individual autonomy is not yet fully reflected in the existing offence construction. Conceptually, human rights theory requires that any form of data processing that exceeds legitimate purposes be regarded as a threat to the dignity and self-determination of the data subject.[48] However, a systematic reading of the criminal provisions in the PDP Law shows that emphasis still lies predominantly on administrative compliance and fine-based sanction mechanisms, while the criminal dimension has not yet been explicitly linked to high-risk situations such as the misuse of KYC data on crypto platforms. At this point, offence reformulation is required not merely to increase criminal penalties, but to harmonise the offence structure with the human-rights conception of the fundamental importance of personal data protection.

The comparative findings with legal regimes in the European Union and Japan reinforce the conclusion that an integrative model linking data protection regulation with crypto-sector regulation is capable of producing a more responsive offence structure. In those jurisdictions, serious data breaches in the crypto sector are not treated merely as administrative violations, but can trigger criminal liability for corporations and their management. This finding does not simply reflect a difference in the "strictness" of regulation, but provides empirical grounds for the view that integrating data protection and crypto-asset regulatory regimes can close gaps which, in the Indonesian context, remain wide. Accordingly, the offence-reformulation model proposed in this study is aligned with that trend, while still needing to be adapted to the civil law tradition and the principle of legality within the national legal system.

Within the framework of legal system theory, the processing of normative and institutional data indicates that the substantive law on data protection and crypto-assets in Indonesia remains fragmented, while the law enforcement structure is dispersed across several authorities whose coordination mechanisms have not yet been firmly institutionalised.[49] This explains why the offences that are textually available have not yet been fully operationalised in cases of data misuse, including those related to digital financial and crypto services. The proposed offence reformulation therefore cannot be understood in isolation from the need to recalibrate inter-institutional relationships, for example by clarifying the roles of the data protection authority, the Financial Services Authority, and law enforcement agencies in investigating and prosecuting data-misuse cases in the crypto sector. Without structural improvements, the introduction of new offences risks producing "dead" norms that are difficult to apply.

A risk-based criminal policy approach helps explain why the crypto-asset sector deserves special treatment in offence design. Based on processed data concerning the characteristics of crypto-assets relative anonymity, cross-border nature, transaction speed, and the volume of KYC data it can be concluded that this sector carries a risk of large-scale, systematic, and cross-jurisdictional misuse of personal data. This distinguishes it from conventional digital services, where the scale and complexity of data networks are relatively easier to map and supervise. Accordingly, the reformulation of offences specifically targeting data misuse within the crypto ecosystem does not amount to over-criminalisation, but rather constitutes a rational strategy to focus criminal law on high-risk areas that have the potential to cause widespread harm to many parties.

At a more operational level, the normative data analysed in this study point to the need for an offence formulation that clearly specifies the object of protection (the personal data of crypto-asset

[48] Imas Novita Juaningsih et al., "Rekonsepsi Lembaga Pengawas Terkait Perlindungan Data Pribadi Oleh Korporasi Sebagai Penegakan Hak Privasi Berdasarkan Konstitusi," *SALAM: Jurnal Sosial Dan Budaya Syar-I* 8, no. 2 (March 5, 2021): 469–86, https://doi.org/10.15408/sjsbs.v8i2.19904.
[49] Muhamad Rizqi Yudha Pratama, Chairul Muriman, and Surya Nita, "Establishing the Legal Basis for Crypto Asset Confiscation: A Critical Study on the Challenges of Cybercrime Law Enforcement in Indonesia," *POLICY LAW NOTARY AND REGULATORY ISSUES (POLRI)* 4, no. 2 (May 14, 2025): 284–98, https://doi.org/10.55047/polri.v4i2.1679.

users and its derivatives), the subjects of law (service-provider corporations, their management, and cooperating third parties), the forms of conduct that are criminalised, as well as the relevant forms of culpability and causal relationships. The object of protection encompasses not only traditional identity data, but also financial data and transactional behaviour data which, if misused, can generate both financial and social harm. By articulating these elements explicitly, the resulting offence will be aligned with human rights theory, which underscores the dimension of personal data as an integral part of personal integrity and individual freedom in the digital sphere.

At the level of the conduct element, the processed comparative materials indicate that a number of acts warrant specific criminalisation, including the collection and processing of personal data beyond legitimate purposes, the transfer of data to third parties or across borders without a legal basis and adequate safeguards, and gross negligence in the operation of security systems resulting in large-scale data breaches. These elements can be distinguished from general data protection offences by linking them to the status of the perpetrator as an operator of the crypto ecosystem or as a party that directly exploits crypto-asset users' data for commercial or criminal purposes. In this way, the proposed offence-reformulation model creates space for a clear differentiation between ordinary administrative violations and criminal acts that threaten the important *rechtsgut* constituted by users' personal data.

The examination of corporate criminal liability practices in various jurisdictions also indicates that schemes which only target individual technical perpetrators are inadequate for addressing systemic data misuse. The data analysed in this study show that many incidents of data breaches and misuse stem from managerial decisions, system designs that disregard the *privacy by design* principle, or business strategies that consciously exploit user data.[50] Accordingly, the proposed offence-reformulation model positions the corporation as the principal subject of liability, with members of management incurring personal liability where it can be shown that they consented to, ordered, or wilfully allowed the conduct to occur. This approach is consistent with legal system theory, which underscores the importance of linking legal responsibility to the actual centres of decision-making within an organisation.

In the evidentiary context, the analysis of cybercrime patterns shows that the misuse of personal data in the crypto sector is highly dependent on digital traces, system logs, and transaction records that are entirely under the technical control of service providers. Without explicit obligations to retain, secure, and provide limited access to such data for law enforcement authorities, even newly formulated offences will be difficult to prove. Therefore, the offence reformulation model developed in this study requires integration between the elements of the offence and the procedural obligations of service providers, such as incident reporting, log retention, and cooperation in investigations. This establishes a direct connection between criminal norms and data-governance design, and ensures that the human-rights-based theory of personal data protection can be realised through operational law-enforcement mechanisms.

The comparative data analysis also shows that the offence reformulation model must be balanced with safeguards for technological innovation and the healthy development of markets. Criminal policy theory cautions that excessive criminalisation may create a chilling effect, whereby business actors are reluctant to innovate for fear of criminal liability. To maintain this balance, the proposed offence model clearly distinguishes between ordinary faults that can be addressed through administrative sanctions and serious faults that reflect a high degree of negligence or intent. Criminal offences are positioned as an *ultimum remedium* that is activated only where there are serious breaches of data protection obligations causing significant harm or exhibiting a pattern of systemic misuse.

In relation to previous research, the synthesis presented in this sub-discussion is not intended to negate the contributions of studies that have examined data protection or crypto-asset regulation in a partial manner, but rather to process those diverse findings into a more integrated conceptual model. Whereas part of the prior literature tends to regard data protection as an administrative issue and consumer protection as a civil or market issue, this study brings both within a criminal-law framework that places the misuse of personal data in the crypto ecosystem at its core. In other words,

[50] Muhammad Na'im Al Jum'ah, "Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi," *Cyber Security Dan Forensik Digital* 1, no. 2 (March 12, 2019): 39–44, https://doi.org/10.14421/csecurity.2018.1.2.1370.

the proposed offence-reformulation model both supports theories that treat data as an autonomous legal interest and corrects the prevailing tendency to rely excessively on non-penal approaches in a high-risk sector.

Finally, this sub-discussion affirms that the proposed model for reformulating criminal offences concerning the misuse of personal data in the crypto-asset ecosystem should be understood as the outcome of an integrated processing of normative, empirical, and theoretical data that mutually reinforce one another. The findings on the imbalance between risk and offence structure, the best practices observed in other jurisdictions, and the frameworks of human rights theory, legal system theory, and criminal policy together form a coherent argument that Indonesia requires a specific offence integrated with data protection and crypto-asset regulation. Thus, the proposed reformulation is not merely an abstract idea, but a recommendation grounded in the practical needs of law enforcement and the conceptual imperative to place personal data protection at the heart of legal protection in a digital economy driven by crypto-assets.

Conclusion

This study concludes that the construction of criminal offences relating to the misuse of personal data within Indonesia's crypto-asset ecosystem remains inadequately balanced when measured against the level of risk generated by data collection and processing practices and the available normative design. Positive law through the regimes on personal data protection, cybercrime, and sectoral regulation of crypto-assets does in fact provide a foundation for criminalisation, but it remains general, fragmented, and has yet to specifically internalise the technological, economic, and institutional characteristics of the crypto ecosystem. By linking normative, empirical, and comparative findings through the lenses of human rights theory, legal system theory, and risk-based criminal policy, this study demonstrates that the reformulation of a specific offence concerning the misuse of personal data in the crypto-asset ecosystem constitutes both a conceptual and practical necessity for strengthening the protection of the legal interests attached to users' personal data.

From the perspective of doctrinal development and practice, this study contributes by proposing a conceptual model for offence reformulation that not only adds new statutory provisions, but also recalibrates the way the state positions personal data as an object of criminal law protection amid the transformation of digital finance. Its principal novelty lies in the analytical focus that explicitly links three domains that have often been treated separately personal data protection, crypto-asset regulation, and criminal law and integrates them into a single, measurable normative framework grounded in legal theory. For policymakers and supervisory authorities, this model can serve as a reference for designing legislative instruments and implementing regulations that are more responsive to risk patterns in the crypto sector; for the academic community, it opens space for further enrichment of theories on the status of personal data as an autonomous *rechtsgut* in contemporary criminal law.

Nevertheless, this study has several limitations that should be noted as a basis for further research. First, the predominantly normative–doctrinal and comparative character of the research means that the depth of analysis is highly dependent on the availability of legal materials and secondary reports, so that the empirical mapping of law-enforcement practice and case patterns of personal data misuse on domestic crypto platforms has not been fully uncovered. Second, the limited number of court decisions that explicitly address personal data misuse in the context of crypto-assets constrains the possibility of testing the proposed offence-reformulation model against concrete judicial practice. Going forward, follow-up studies that combine normative approaches with empirical research, case-law analysis, and cross-sectoral examinations (taxation, AML/CFT, and consumer protection) constitute an important agenda for testing, refining, and implementing the offence-reformulation model proposed in this article.

References

Adiyatma, Septhian Eka, and Dhita Fitria Maharani. "Cryptocurrency's Control in the Misuse of Money Laundering Acts as an Effort to Maintain the Resilience and Security of the State." *Lex Scientia Law Review* 4, no. 1 (May 8, 2020): 75–88. https://doi.org/10.15294/lesrev.v4i1.38257.

Admiral, Admiral, and Mega Ardina Pauck. "Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services." *Lex Scientia Law Review* 7, no. 2 (November 30, 2023): 995–1048. https://doi.org/10.15294/lesrev.v7i2.77881.

Afrilies, Marlia Hafny, Angie Angel Lina, Maria Theresia, Efendi Simanjuntak, Yuris Tri Naili, Evis Garunja, and Burhanuddin Bin Mohd Aboobaider. "Ensuring Construction Workers Legal Protection: A Legal Analysis of Construction Competency Certificates under the Law on Personal Data Protection and Blockchain Frameworks." *Jurnal Pamator : Jurnal Ilmiah Universitas Trunojoyo* 16, no. 4 (January 15, 2024): 810–25. https://doi.org/10.21107/pamator.v16i4.23948.

Aliman. "Criminal Law Implications of Personal Data Misuse in the Digital Age ." *International Journal of Health, Economics, and Social Sciences (IJHESS)* 7, no. 2 SE-Articles (April 30, 2025): 986–991. https://doi.org/10.56338/ijhess.v7i2.8300.

Andrianto, Dhimas Candra. "Perlindungan Hukum Dan Pengenaan Pajak Bagi Investor Cryptocurrency Di Indonesia." *Jurnal Ilmiah Universitas Batanghari Jambi* 22, no. 1 (February 19, 2022): 140. https://doi.org/10.33087/jiubj.v22i1.2014.

Arbina, Maria, and M Ilham F Putuhena. "Tata Kelola Pembentukan Regulasi Terkait Perdagangan Mata Uang Kripto (Cryptocurrency) Sebagai Aset Kripto (Crypto Asset)." *Mahadi: Indonesia Journal of Law* 1, no. 1 (February 10, 2022): 33–57. https://doi.org/10.32734/mah.v1i1.8314.

Ariani, Okta, and Aji Lukman Ibrahim. "Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia." *JURNAL USM LAW REVIEW* 7, no. 1 (December 31, 2023): 30–44. https://doi.org/10.26623/julr.v7i1.8027.

Astrakhantseva, Irina, Roman Astrakhantsev, and Alexey Los. "Cryptocurrency Fraud Schemes Analysis." Edited by A.D. Nazarov. *SHS Web of Conferences* 106 (May 18, 2021): 02001. https://doi.org/10.1051/shsconf/202110602001.

Benson, Vladlena, Bogdan Adamyk, Anitha Chinnaswamy, and Oksana Adamyk. "Harmonising Cryptocurrency Regulation in Europe: Opportunities for Preventing Illicit Transactions." *European Journal of Law and Economics* 57, no. 1–2 (April 4, 2024): 37–61. https://doi.org/10.1007/s10657-024-09797-w.

Busser, Els De. "EU-US Digital Data Exchange to Combat Financial Crime: Fast Is the New Slow." *German Law Journal* 19, no. 5 (October 6, 2018): 1251–67. https://doi.org/10.1017/S2071832200023026.

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (September 28, 2021): 177. https://doi.org/10.25072/jwy.v5i2.460.

Fithri, Beby Suryani, Riswan Munthe, and Anggreni Atmei Lubis. "Asas Ultimum Remedium/The Last Resort Principle Terhadap Pelaku Usaha Dalam Hukum Perlindungan Konsumen." *DOKTRINA: JOURNAL OF LAW* 4, no. 1 (April 30, 2021): 69–84. https://doi.org/10.31289/doktrina.v4i1.4918.

Garnita, Camiliya Fakhriyah, and Kuswandi Kuswandi. "Analisis Kriminologi Dalam Tindak Pidana Pencurian Data Pribadi Di Era Digital." *Indonesian Journal of Law and Justice* 3, no. 2 (December 28, 2025): 11. https://doi.org/10.47134/ijlj.v3i2.5288.

Gilbert, Chris, and Mercy Gilbert. "Patterns and Vulnerabilities of Cryptocurrency-Related Cybercrimes." *SSRN Electronic Journal*, 2025. https://doi.org/10.2139/ssrn.5196069.

Gustryan, Muhammad, and Zainal Arifin Hoesein. "Peran Undang-Undang ITE Dan Undang-Undang Perlindungan Data Pribadi Dalam Perlindungan Data Dan Privasi Di Era Ekonomi Digital." *Jurnal Minfo Polgan* 14, no. 2 (December 26, 2025): 3333–43. https://doi.org/10.33395/jmp.v14i2.15746.

Hamsin, Muhammad Khaeruddin, Abdul Halim, and Rizaldy Anggriawan. "Addressing Cybercrime in the Sharia Digital Wallet Industry: A Legal Perspective in the Indonesian Context." Edited by D. Mutiarin, M. Alam, D. Cahill, J. Sharifuddin, M. Senge, A. Robani, P. Saiyut, and A. Nurmandi. *E3S Web of Conferences* 440 (November 1, 2023): 04016. https://doi.org/10.1051/e3sconf/202344004016.

Huda, Uu Nurul, Dian Rachmat Gumelar, and Alwi Al Hadad. "Fortifying Democracy: Deploying Electoral Justice for Robust Personal Data Protection in the Indonesian Election." *Khazanah Hukum* 6, no. 1 (March 1, 2024): 24–33. https://doi.org/10.15575/kh.v6i1.30734.

Hutomo, Priyo, and Markus Marselinus Soge. "Perspektif Teori Sistem Hukum Dalam Pembaharuan Pengaturan Sistem Pemasyarakatan Militer." *Legacy: Jurnal Hukum Dan Perundang-Undangan* 1, no. 1 (March 4, 2021): 46–68. https://doi.org/10.21274/legacy.2021.1.1.46-68.

Juaningsih, Imas Novita, Rayhan Naufaldi Hidayat, Kiki Nur Aisyah, and Dzakwan Nurirfan Rusli. "Rekonsepsi Lembaga Pengawas Terkait Perlindungan Data Pribadi Oleh Korporasi Sebagai Penegakan Hak Privasi Berdasarkan Konstitusi." *SALAM: Jurnal Sosial Dan Budaya Syar-I* 8, no. 2 (March 5, 2021): 469–86. https://doi.org/10.15408/sjsbs.v8i2.19904.

Jum'ah, Muhammad Na'im Al. "Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi." *Cyber Security Dan Forensik Digital* 1, no. 2 (March 12, 2019): 39–44. https://doi.org/10.14421/csecurity.2018.1.2.1370.

Knetsch, Jonas. "The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases." *Journal of European Tort Law* 13, no. 2 (August 4, 2022): 132–53. https://doi.org/10.1515/jetl-2022-0008.

Kurniawan, Kukuh Dwi, Deassy J. A. Hehanussa, Rahmat Setiawan, Indah Susilowati, Sopian, and Desmarani Helfisar. "Criminal Sanctions and Personal Data Protection in Indonesia." *Lex Publica* 11, no. 2 (December 3, 2024): 221–47. https://doi.org/10.58829/lp.11.2.2024.255.

Lestariningtyas, Twotik, and Muhammad Roqib. "Perlindungan Data Pribadi Pengguna Sistem Layanan Perizinan Berusaha Terintegrasi Secara Elektronik OSS 1.1 DAN OSS RBA (RISK BASIC APPROACH)." *Jurnal Jendela Hukum* 8, no. 2 (September 15, 2021): 25–34. https://doi.org/10.24929/fh.v8i2.1576.

Mayuna, I K. O., R. Dewantara, and P. A. Ruslijanto. "Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia." *Journal of Digital Technologies and Law* 3, no. 2 (July 6, 2025): 275–303. https://doi.org/10.21202/jdtl.2025.12.

Meriyati, Meriyati, Imamul Arifin, Dimas Fahrul Putra Arismanto, Muhammad Rizal, and Mustamiruddin Mustamiruddin. "Hukum Dan Eksistensi Jual Beli Crypto Untuk Investasi Dalam Perspektif Ekonomi Islam Dan Ekonomi Sosial 'Studi Literasi Dan Komparasi Pada Masyarakat.'" *Jurnal Justisia Ekonomika: Magister Hukum Ekonomi Syariah* 7, no. 2 (December 20, 2023): 869–81. https://doi.org/10.30651/justeko.v7i2.20456.

Muradyan, S. V. "Digital Assets: Legal Regulation and Estimation of Risks." *Journal of Digital Technologies and Law* 1, no. 1 (March 15, 2023): 123–51. https://doi.org/10.21202/jdtl.2023.5.

Norval, Chris, Heleen Janssen, Jennifer Cobbe, and Jatinder Singh. "Data Protection and Tech Startups: The Need for Attention, Support, and Scrutiny." *Policy & Internet* 13, no. 2 (June 7, 2021): 278–99. https://doi.org/10.1002/poi3.255.

Nur Luthiya, Adik, Benny Irawan, and Rena Yulia. "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi." *Jurnal Hukum Pidana Dan Kriminologi* 2, no. 2 (September 22, 2021): 14–29. https://doi.org/10.51370/jhpk.v2i2.43.

Nurmansyah, Gunsu, Rudi Natamiharja, and Ikhsan Setiawan. "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach." *Pancasila and Law Review* 6, no. 1 (August 25, 2025): 15–44. https://doi.org/10.25041/plr.v6i1.4138.

Olushola, Akinlemi, and S. P. Meenakshi. "Cybersecurity Crimes in Cryptocurrency Exchanges (2009–2024) and Emerging Quantum Threats: The Largest Unified Dataset of CEX and DEX Incidents." *Frontiers in Blockchain* 8 (November 27, 2025). https://doi.org/10.3389/fbloc.2025.1713637.

Poulle, Jean-Baptiste, Arut Kannan, Nicolas Spitz, Sandra Kahn, and Anastasia Sotiropoulou. "Markets in Crypto-Assets (MiCA) Regulation." In *EU Banking and Financial Regulation*, 662–69. Edward Elgar Publishing, 2024. https://doi.org/10.4337/9781035301959.00100.

Pratama, Muhamad Rizqi Yudha, Chairul Muriman, and Surya Nita. "Establishing the Legal Basis for Crypto Asset Confiscation: A Critical Study on the Challenges of Cybercrime Law Enforcement in Indonesia." *POLICY LAW NOTARY AND REGULATORY ISSUES (POLRI)* 4, no. 2 (May 14, 2025): 284–98. https://doi.org/10.55047/polri.v4i2.1679.

Putra, Ferdy Arliyanda, and Lucky Dafira Nugroho. "Perlindungan Hukum Terhadap Penyalahgunaan Akun Dalam Transaksi Elektronik Melalui Traveloka." *INICIO LEGIS* 2, no. 1 (June 30, 2021). https://doi.org/10.21107/il.v2i1.11081.

Sevim, Hasret Ozan. "European Union's Approach to Crypto-Assets and Distributed Ledger Technologies." *Studia Sieci Uniwersytetów Pogranicza* 6 (2022): 139–47. https://doi.org/10.15290/sup.2022.06.10.

Simbolon, Valentina Ancillia, and Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (December 30, 2022): 178. https://doi.org/10.31314/pjia.11.2.178-190.2022.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (March 25, 2021): 38. https://doi.org/10.47268/sasi.v27i1.394.

Soemitro, Dian Purwaningrum, Muhammad Arvin Wicaksono, and Nur Aini Putri. "Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore." *SIGn Jurnal Hukum* 5, no. 1 (July 31, 2023): 155–67. https://doi.org/10.37276/sjh.v5i1.272.

Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. "TATA KELOLA PERLINDUNGAN DATA PRIBADI DI ERA METAVERSE (TELAAH YURIDIS UNDANG-UNDANG

PERLINDUNGAN DATA PRIBADI).” *Masalah-Masalah Hukum* 52, no. 1 (March 31, 2023): 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106.

Syailendra, Moody Rizqy. “Personal Data Protection Law In Indonesia: Challenges And Opportunities.” *Indonesia Law Review* 14, no. 2 (August 31, 2024). https://doi.org/10.15742/ilrev.v14n2.4.

Tauda, Gunawan A., Andy Omara, and Gioia Arnone. “Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and European Union.” *BESTUUR* 11, no. 1 (August) (April 12, 2023): 1. https://doi.org/10.20961/bestuur.v11i1.67125.

Vidianto, Dominic Imanuel, Aloysius Mardiana, Nurul Hikmah, and Aliif Ahmad Akbar. “Legal Protection for Consumers Who Lose Assets on Crypto Exchange Platforms in Indonesia: A Case Study of Hacking and Rug Pull.” *Justice Voice* 4, no. 2 (December 31, 2025): 83–93. https://doi.org/10.37893/jv.v4i2.1204.

Wijaya, Glenn. “PELINDUNGAN Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum.” *Law Review* 19, no. 3 (August 12, 2020): 326. https://doi.org/10.19166/lr.v19i3.2510.

Yanuar, Muh Afdal. “Risiko Dan Posibilitas Penyalahgunaan Aset Kripto Dalam Kejahatan Pencucian Uang: Risks and Possibilities of Misuse of Crypto Assets in Money Laundering Crimes.” *Majalah Hukum Nasional* 52, no. 2 (2022): 169–88.