Journal of Strafvordering:
https://nawalaeducation.com/index.php/JOSI/index
Journal of Criminal Law Vol.3 No.1, March 2026
E-ISSN:3046-8620
DOI : https://doi.org/10.62872/xjfjn579

Dark Side of Digital Economy: A Criminal Law Study of Economic Crimes on Digital Platforms

Harly Clifford Jonas Salmon✉
Universitas Pattimura, Indonesia
e-mail:* Harlyclifford@outlook.com

Entered :January 20, 2026 Revised :February 22, 2026
Accepted : March 16, 2026 Published : March 30, 2026

ABSTRACT

The development of the digital economy through various information technology-based platforms has created a major transformation in people's economic activities. On the other hand, this development has also given rise to various new forms of economic crime that exploit digital systems as a means to obtain unlawful profits. This situation poses challenges for the criminal law system in anticipating and addressing platform-based economic crimes. This study aims to analyze the criminal law construction for economic crimes on digital platforms and examine the ambiguity of norms regarding criminal liability for platform-based economic crimes. The research method used is normative legal research with a statutory and conceptual approach. Legal materials are analyzed qualitatively to identify the alignment between digital economic developments and applicable legal regulations. The results show that criminal law regulations related to digital economic activities in Indonesia are still partial and do not specifically regulate various forms of economic crimes on digital platforms. The ambiguity of norms regarding the responsibilities of platform providers, the determination of legal subjects, and electronic evidence-based evidentiary mechanisms creates legal uncertainty and has the potential to hamper the effectiveness of law enforcement. Therefore, a reformulation of criminal law policies is needed that is more responsive, integrative, and adaptive to developments in digital technology in order to create legal certainty and optimal protection for the community in the digital economy ecosystem.

Keywords: Digital Economic Crime, Digital Platform, Criminal Law, Criminal Liability.

INTRODUCTION

The transformation of the digital economy is a logical consequence of the increasingly rapid development of information and communication technology and the increasing penetration of the internet into modern society. These changes not only impact the technical aspects of economic activity but also alter the structure and patterns of legal relationships between businesses, consumers, and digital platform providers. Economic activities previously conducted conventionally have now shifted into the digital space, which is virtual, without territorial boundaries, and allows for real-time transactions.[1] This phenomenon has given rise to a new economic ecosystem known as the digital

[1] Mahera, R. M., & Suryadi, N. (2025). Transformasi mekanisme pasar dalam ekonomi berbasis teknologi digital. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *2*(11). https://www.ojs.daarulhuda.or.id/index.php/Socius/article/view/1558

economy, an economic system that relies on the use of digital technology as the primary means of producing, distributing, and consuming goods and services. Conceptually, the digital economy also reflects a paradigm shift in the global economic system, which is increasingly integrated with developments in information technology.[2]

The existence of digital platforms such as marketplaces, financial technology (fintech), online investment services, and electronic payment systems has expanded public access to various economic activities that were previously difficult to access. Digital platforms enable more efficient, transparent, and rapid economic interactions, thereby increasing productivity and national economic competitiveness. From the perspective of economic law theory, this development indicates a process of market digitalization that is shifting the structure of economic transactions from a conventional model to a platform-based one.[3] According to Don Tapscott in the concept of digital economy, digital technology has created a new economic space that is open, collaborative, and globally connected through the internet network.[4] Therefore, digital platforms not only function as a means of transaction, but also as economic infrastructure that facilitates various trading activities, investments, and financial services on a wider scale.

The growth of the digital economy in Southeast Asia has shown a very significant trend in recent years. A report by Google, Temasek, and Bain & Company indicates that the region's digital economy will surpass USD 200 billion by 2023, with Indonesia being the largest contributor to this growth.[5] These empirical facts demonstrate that the digital economy has become a crucial pillar of national economic development and a key driver of technology-based economic innovation. In economic law, this development confirms that the digital space has become a new arena for economic activity, requiring adequate legal regulation. Without an adaptive legal framework, the rapid growth of the digital economy has the potential to give rise to various complex legal issues in digital economic transactions.

While the digital economy offers numerous benefits for national economic development, it also presents significant risks. Ease of technological access, user anonymity, and the cross-border nature of the digital space create opportunities for various forms of economic malpractice. This demonstrates that technological development is not always accompanied by a legal system prepared to address the potential for abuse. From the perspective of modern criminological theory, technological development often creates new opportunities for crime previously unknown within the

---

[2] Amory, J. D. S., & Mudo, M. (2025). Transformasi ekonomi digital dan evolusi pola konsumsi: Tinjauan literatur tentang perubahan perilaku belanja di era internet. *Jurnal Minfo Polgan*, *14*(1), 28-37. https://doi.org/10.33395/jmp.v14i1.14608

[3] Ikhsan, M., bin Sapa, N., & Syatar, A. (2025). Ekonomi Digital dan Hukum Ekonomi Syariah: E-Commerce, Aset Digital dan Implikasi Hukumnya Menurut Hukum Islam. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *3*(1).

[4] Sulistyowati, R., Listiadi, A., Subroto, W. T., Ramadhani, S. N., Sarfita, D., Damayanti, F., ... & Weni, W. (2025). Pembelajaran Ekonomi Digital: Konsep, Transformasi Pasar Dan Kesiapan Teknologi. *Penerbit Tahta Media*.

[5] Utomo, A. P., Ibrohim, N. M., Ramadhani, N., Zidni, N. M., & Wahyuaristy, D. S. (2025). Konsep ideal regulasi identitas digital tunggal dalam konvergensi teknologi sebagai instrumen penguatan perdagangan digital berbasis ekonomi virtual. *Forschungsforum Law Journal*, *2*(02), 119-141. https://doi.org/10.35586/flj.v2i02.11161

conventional economic system.[6] Therefore, the development of the digital economy must be understood not only as an economic phenomenon, but also as a legal phenomenon that requires serious attention from the criminal law system.

One implication of the development of the digital economy is the emergence of various forms of economic crime that utilize digital platforms as both a means and object of criminal activity. Digital-based economic crime encompasses not only conventional fraud perpetrated through electronic media, but also more complex criminal methods such as digital transaction manipulation, misuse of platform algorithms, and the exploitation of personal data for illegal economic gain. In this context, digital platforms often provide a space where criminals can exploit technological loopholes to gain unlawful profits. This phenomenon demonstrates that the digitalization of the economy has created new forms of crime with characteristics distinct from traditional economic crime. Therefore, conventional criminal law approaches often struggle to address the rapidly evolving dynamics of digital economic crime.

Digital platform-based economic crime can be found in various forms of increasingly complex and organized illegal practices. Digital investment fraud, transaction manipulation in marketplaces, money laundering through electronic payment systems, and misuse of consumer data are just a few examples of crimes developing within the digital economy ecosystem.[7] Data from the Financial Transaction Reports and Analysis Center shows that suspicious transactions related to digital-based financial activities continue to increase every year.[8] This increase indicates that the digital space has become a strategic medium for economic criminals to disguise their illegal activities through complex electronic transaction systems. This situation demonstrates that the development of financial technology also carries the risk of increasing economic crimes that are difficult to detect through conventional surveillance mechanisms.

The characteristics of economic crimes on digital platforms are more complex than those of conventional economic crimes. The digital space allows criminals to operate anonymously, use false identities, and utilize encryption technology to conceal transaction traces. Furthermore, the cross-border nature of digital transactions often involves different jurisdictions, posing unique challenges to law enforcement. From the perspective of modern criminal law theory, this situation demonstrates that technological developments have fundamentally changed the structure and modus operandi of economic crimes.[9] Therefore, the criminal law system needs to develop a more adaptive approach to deal with the dynamics of crime that occur in the digital space.

Normatively, the Indonesian legal system already has a number of legal instruments that can be used to address economic crimes occurring in the digital space.

---

[6] Setiawan, D. A. (2024). Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa. *Masalah-Masalah Hukum*, *53*(1), 78-89. https://doi.org/10.14710/mmh.53.1.2024.78-89

[7] Muflikh, A. A. M., Ramadan, D. R. C., Silalahi, B. B. S., Martitah, M., & Sulistianingsih, D. (2025). Analisis Perlindungan Hukum Konsumen pada Perjanjian Transaksi E-Commerce terkait Investasi Kripto Ilegal via Media Sosial. *Bookchapter Hukum dan Politik dalam Berbagai Perspektif*, *4*, 106-133. https://bookchapter.unnes.ac.id/index.php/hp/article/view/609

[8] Farahdiva, A. T., Mulyana, S. L., & Asri, T. P. (2025). Implementasi Cyber Security Pada Sistem Transaksi Keuangan Digital. *Jurnal Ilmiah Ekonomi, Manajemen, Bisnis Dan Akuntansi*, *2*(4), 276-289. https://doi.org/10.61722/jemba.v2i4.1157

[9] Insani, N. S., Mulyana, R. N., & Hosnah, A. U. (2026). Dampak Perubahan Sosial Terhadap Pola Kejahatan: Perspektif Kriminologi. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(1), 3166-3176. https://doi.org/10.61104/alz.v4i1.3610

Some relevant regulations include Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, and Law Number 27 of 2022 concerning Personal Data Protection. These regulations are principally intended to provide legal protection for digital economic activities while also providing a legal basis for law enforcement against crimes that utilize information technology. From the perspective of the principle of legality in criminal law, the existence of clear legal norms is a primary requirement for effective law enforcement.[10] Therefore, regulations governing digital activities have an important role in maintaining legal order in the digital economic ecosystem.

Despite the development of various regulations, the rapid development of digital technology often outstrips the law's ability to adapt responsively. Many legal provisions are still formulated using conventional approaches, thus failing to fully address the ever-evolving dynamics of digital economic activity. From the perspective of the responsive legal theory put forward by Philippe Nonet and Philip Selznick, the law should be able to adapt to social changes occurring in society.[11] When the law fails to keep pace with the dynamics of technological development, a gap will emerge between legal norms and the social reality they regulate. This gap has the potential to create various problems in law enforcement practices regarding digital economic crimes.

A frequent problem in law enforcement practices for digital economic crimes is the lack of clarity in applicable legal regulations. Several existing criminal law provisions are still general and do not specifically address the forms of economic crimes that develop on digital platforms. This ambiguity is evident in the definition of criminal liability between perpetrators and digital platform providers, the classification of digital economic crimes within the criminal law system, and the mechanisms for proving evidence for complex digital transactions. From the perspective of the principle of legal certainty, unclear legal norms can lead to various interpretations in law enforcement practices. This situation has the potential to create legal uncertainty and hinder the effectiveness of combating economic crimes in the digital space.

The ambiguity of norms governing digital economic crimes also raises serious issues in determining the criminal liability of parties involved in the digital platform ecosystem. Digital platform providers often act as intermediaries in user transactions, raising questions about the extent of the platform's legal responsibility for illegal activities occurring within its system. Under the theory of corporate criminal liability, a legal entity can be held liable if there is a link between the illegal act and activities within the organization.[12] However, in digital economic practice, the boundaries between platform and user responsibility are often not clearly defined in legislation. This situation demonstrates that the criminal justice system still faces significant challenges in adapting the concept of criminal liability to developments in digital technology.

---

[10] Agustina, P. M. (2025). Implementasi Peraturan Kejaksaan Nomor 19 Tahun 2020 tentang Penyelesaian Uang Pengganti dalam Perspektif Asas Legalitas. *Lex Positivis*, *3*(2), 82-111. https://jtamfh.ulm.ac.id/index.php/jtamfh/article/view/170

[11] Djauzie, M. Z. (2025). Pancasila Sebagai Grundnorm Menurut Teori Hukum Murni Hans Kelsen Dan Teori Hukum Responsif Oleh Philippe Nonet Dan Philip Selznick. *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *11*(1), 239-252. https://doi.org/10.55809/tora.v11i1.456

[12] Harefa, S., & Nashir, M. A. (2025). SH Pertanggungjawaban Pidana Korporasi Dalam Kasus Pelanggaran Lingkungan Hidup Di Indonesia: Pertanggungjawaban Pidana Korporasi Dalam Kasus Pelanggaran Lingkungan Hidup Di Indonesia. *ADIL: Jurnal Hukum*, *16*(1), 36-60. https://doi.org/10.33476/ajl.v16i1.4966

Based on these various issues, the development of the digital economy not only presents opportunities for economic growth but also creates new challenges for the criminal justice system in addressing the phenomenon of digital platform-based economic crimes. Regulatory unpreparedness in responding to technological dynamics has the potential to create legal loopholes that criminals can exploit to conduct various illegal economic activities in the digital space. This situation raises fundamental questions about the extent to which current criminal law is able to address and address various forms of economic crimes on digital platforms. Furthermore, there is a need to critically examine how the legal system can address the unclear norms that arise in regulating digital economic crimes. Therefore, a criminal law study of the dark side of the digital economy is crucial for formulating a more comprehensive, adaptive, and responsive legal approach to technology-based economic developments.

METHODOLOGY

The research method used in this study is normative legal research, namely research that positions law as a system of norms analyzed through library studies of laws and regulations, legal doctrines, and various literature relevant to the problem being studied. Normative legal research essentially aims to examine law from a conceptual and normative aspect in order to discover principles, grounds, and legal constructions that can explain a particular legal phenomenon. According to Peter Mahmud Marzuki, normative legal research is research conducted to discover legal rules, legal principles, and legal doctrines to answer the legal issues faced.[13] This approach was used because the problem under study relates to the criminal law regulations for economic crimes on digital platforms, which require an analysis of applicable legal norms and the concept of criminal liability within the legal system. Therefore, this study seeks to systematically examine various legal provisions related to digital economic activities and the potential for economic crimes to arise within the digital platform ecosystem.

The research approaches used in this study include a statutory approach and a conceptual approach. The statutory approach is carried out by examining various laws and regulations related to digital economic crimes, while the conceptual approach is used to analyze various legal concepts and theories relevant to the issue of normative ambiguity in the regulation of digital platform-based economic crimes. The data used in this study is secondary data consisting of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations related to information technology, economic crimes, and personal data protection, while secondary legal materials include books, scientific journals, and the opinions of legal experts relevant to the research topic. According to Soerjono Soekanto, normative legal research is essentially based on the analysis of library materials or secondary data as the main source for understanding the applicable legal system.[14] All legal materials are then analyzed qualitatively using legal interpretation and argumentative analysis methods to obtain a comprehensive understanding of criminal law regulations regarding economic crimes on digital platforms.

---

[13] Arifuddin, Q., Riswan, R., HR, M. A., Bulkis, B., Latif, A., Salma, S., ... & Indah, N. (2025). *Metodologi penelitian hukum*. PT. Sonpedia Publishing Indonesia.

[14] Sukmawan, Y. A., & Damayanti, D. (2025). Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum. *Notary Law Journal*, *4*(3), 114-128. https://doi.org/10.32801/nolaj.v4i3.116

RESULTS AND DISCUSSION

Construction of Criminal Law on Economic Crimes in Digital Platforms from the Perspective of Legislation in Indonesia

The concept of economic crime from a modern criminal law perspective has evolved in line with the increasingly complex and technology-driven structure of the global economy. In criminal law doctrine, economic crime is no longer understood narrowly as a crime against property, but rather as an unlawful act that impacts the stability of the economic system, state finances, and public confidence in market mechanisms. These crimes are generally committed with the aim of obtaining illicit financial gain through manipulation of the economic system, abuse of authority, or manipulation of financial transactions.[15] Normatively, economic crimes often involve the misuse of legitimate economic instruments, such as trade transactions, banking activities, and investments. Therefore, economic crimes are often classified as specific crimes regulated by various laws and regulations outside the Criminal Code. In this context, criminal law serves as an instrument to protect the integrity of the economic system and as a means to address deviations that could undermine a healthy economic order.

The characteristics of economic crime differ fundamentally from conventional crime, which is generally direct and visible. Economic crime tends to be complex, systematic, and carried out through well-planned mechanisms that exploit loopholes in the economic system and existing regulations. Perpetrators of economic crime often hold relatively high social standing, whether as businesspeople, professionals, or officials with access to economic resources.[16] The impact of these crimes is often not immediately felt by individual victims, but they have far-reaching consequences for society and the state. The resulting losses can range from disrupted financial system stability, reduced public trust in economic institutions, to the potential for large-scale state financial losses. Therefore, economic crimes are viewed in modern criminal law as a serious threat that requires a more comprehensive and systematic approach to countermeasures.

One important concept in understanding economic crime was put forward by Edwin H. Sutherland through his theory of white-collar crime. Sutherland defined white-collar crime as crimes committed by individuals of high social status and respect in the course of their work.[17] This concept broadens the perspective of criminology by showing that crime is not only committed by lower-class groups but also by individuals occupying strategic positions within the economic structure. Within economic crime, the concept of white-collar crime encompasses various forms of deviance, such as corporate fraud, market manipulation, embezzlement, and violations of economic regulations.

---

[15] Suciana, H. E., Fardiansyah, A. I., & Tamza, F. B. (2025). UPAYA PENEGAKAN HUKUM TERHADAP KEJAHATAN EKONOMI DALAM SISTEM PERADILAN PIDANA. *Jurnal Pendidikan Sejarah dan Riset Sosial Humaniora*, *5*(2), 106-114. https://ejournal.penerbitjurnal.com/index.php/humaniora/article/view/1272

[16] Herawati, E., Mustopa, H., Sander, M., & Fujianti, P. J. (2025). Analisis Yuridis Terhadap Tanggung Jawab Korporasi Dalam Tindak Pidana Kejahatan Luar Biasa Di Bidang Ekonomi. *Jurnal Sosial Teknologi*, *5*(7), 2819-2831. https://doi.org/10.59188/jurnalsostech.v5i7.32225

[17] Rumahorbo, L., & Yusuf, H. (2025). Analisis Mendalam Perilaku Menyimpang White-Collar Crime (Studi Kasus melalui Lensa Teori Convenience). *Media Hukum Indonesia (MHI)*, *3*(3). https://ojs.daarulhuda.or.id/index.php/MHI/article/view/2195

Sutherland's perspective also critiques the tendency of the criminal justice system to treat white-collar crime more leniently than conventional crime.[18] This criticism shows that the losses caused by economic crimes are often much greater than those caused by conventional crimes, thus requiring more serious attention in criminal law policy.

The development of digital technology has expanded the scope of economic crime, giving rise to new forms previously unknown in conventional economic systems. The transformation of the digital economy has created various innovations in transaction mechanisms, but at the same time opened up opportunities for criminals to exploit technology as a means of committing unlawful acts. Economic crimes in the digital space are often committed through the manipulation of electronic transaction systems, the misuse of digital data, and the manipulation of electronic payment systems.[19] This phenomenon demonstrates that economic crimes are evolving in line with technological developments and changes in the global economic structure. Therefore, modern criminal law approaches must adapt to the increasingly complex dynamics of technological development. Without such adaptation, the legal system could potentially be left behind in addressing the ever-evolving forms of economic crime within the digital ecosystem.

In the digital economy, the relationship between cybercrime and economic crime is becoming increasingly close and conceptually difficult to separate. Cybercrime essentially refers to crimes committed using computer systems or internet networks as both a means and a target.[20] Meanwhile, economic crime focuses on the goal of illegally gaining economic advantage through various forms of manipulation of the economic system. In practice, many forms of modern economic crime utilize digital technology as the primary medium for their implementation. For example, digital investment fraud, transaction manipulation in marketplaces, and theft of financial data are then exploited for financial gain. This situation demonstrates that the development of digital technology has created a convergence between cybercrime and economic crime within a single, interconnected ecosystem.

The development of the digital economy has also given rise to a new ecosystem based on the existence of digital platforms as intermediaries in economic activities. Digital platforms such as marketplaces, financial technology, digital investment services, and payment gateways serve as infrastructure connecting various parties in the economic transaction process. The main characteristic of digital platforms lies in their ability to facilitate virtual transactions without requiring physical interaction between the parties involved. This system enables transactions to occur quickly, efficiently, and reach a wider area than conventional trading mechanisms. However, this characteristic also presents new challenges in the supervision and law enforcement aspects of economic activities occurring on digital platforms. This situation demands a legal framework capable of accommodating changing patterns of economic interaction in the digital era.

The digitalization of the economy has also transformed the legal structure of economic transactions, which previously involved only direct interactions between sellers and buyers. In the digital platform ecosystem, legal relationships have evolved into

[18] Gusmarani, R., & Zulyadi, R. (2025). *Kriminal VS Kriminologi*. Yayasan Tri Edukasi Ilmiah.

[19] Setiawan, D. A. (2024). Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa. *Masalah-Masalah Hukum*, *53*(1), 78-89. https://doi.org/10.14710/mmh.53.1.2024.78-89

[20] Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah Dan Hukum*, 40-55. https://doi.org/10.47498/maqasidi.v4i1.2966

tripartite relationships involving businesses, consumers, and platform providers as transaction intermediaries.[21] These legal relationships are generally formalized in electronic contracts containing the terms and conditions for using digital services. In this context, the concept of intermediary liability arises, relating to the extent to which platform providers are responsible for the activities carried out by users within their systems. Legal issues arise when digital platforms are used as a means to commit various forms of economic crimes, such as fraud, transaction manipulation, and misuse of personal data. Therefore, an in-depth legal analysis is required regarding the limits of digital platform liability within a technology-based economic ecosystem.

Legal regulation of digital economic activities in Indonesia is normatively based on a number of laws and regulations governing electronic transactions and technology-based financial activities. One key regulation is Law Number 11 of 2008 concerning Electronic Information and Transactions, which provides the legal basis for recognizing electronic information, electronic documents, and electronic transactions as legitimate legal acts. Furthermore, regulations regarding the potential for money laundering in digital economic activities are regulated in Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, which provides a legal framework for tracing the proceeds of crime through financial transaction mechanisms. In this context, digital platforms have the potential to be exploited as a means of money laundering through various instruments such as digital wallets, cryptocurrencies, and electronic payment systems. Therefore, institutions such as the Financial Transaction Reports and Analysis Center (PPATK) have a strategic role in analyzing suspicious transactions using a "follow the money" approach. The existence of this legal framework demonstrates that combating digital economic crime requires integration of information technology regulations and financial regulations within the national legal system.

Personal data protection is a fundamental aspect of the rapidly growing digital economy ecosystem, driven by the rise in information technology-based transactions. Within the national legal context, comprehensive regulations regarding personal data protection are enacted through Law Number 27 of 2022 concerning Personal Data Protection, which provides a legal framework for the collection, processing, storage, and utilization of personal data in various digital activities. Normatively, this law aims to guarantee individuals' rights to personal data protection while creating legal certainty for electronic system administrators in managing user data. This regulation also reflects the state's recognition that personal data is part of the right to privacy, which must be protected by law as a fundamental human right. In the digital economy, personal data protection is becoming increasingly important because nearly all digital platform-based economic activities depend on the processing of user data.[22] Therefore, the existence of a clear legal framework regarding personal data protection is an important prerequisite for maintaining public trust in the digital economic system.

From a digital economic perspective, personal data is no longer simply viewed as individual identity information but has evolved into an economic asset with strategic

[21] Sari, D. P., Safa, M. S., & Fahlevi, A. R. (2026). Perlindungan Hukum Konsumen dalam Transaksi E-Commerce di Indonesia: Perspektif Hukum Perdata dan Undang-Undang Perlindungan Konsumen. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *5*(1), 6311-6318. https://doi.org/10.31004/riggs.v5i1.6942

[22] Ramadhan, A., & Novitasari, K. (2023). Strategi pengembangan literasi ekonomi berbasis digital terhadap regulasi pemberdayaan perilaku sosial dan sumber daya manusia di era industri 4.0. *AB-JOIEC: Al-Bahjah Journal of Islamic Economics*, *1*(1), 14-25. https://doi.org/10.61553/abjoiec.v1i1.10

value for various digital platforms. User data collected by technology companies is often exploited for consumer behavior analysis, product development, and algorithm-based marketing strategies. This situation indicates that personal data has become commodified in the digital economy, where information about user preferences, habits, and activities can generate economic benefits for platform providers. In practice, many digital companies utilize data as a primary resource in developing technology-based business models. However, the commodification of personal data also raises serious legal issues if the data is managed without consent or exceeds the authority granted by the data owner. Therefore, legal regulations regarding the use of personal data are crucial to prevent data misuse in digital economic activities.

The misuse of personal data in the digital economy can be categorized as a form of modern economic crime with widespread impacts on society. Illegally obtained personal data can be exploited for various illegal economic activities, such as digital fraud, identity theft, financial transaction manipulation, and even illegal data trading on the digital black market.[23] In this context, personal data is not only the object of privacy violations but also an instrument used by criminals to gain illicit economic gain. This phenomenon demonstrates that the development of the digital economy has created a new dimension of economic crime based on the exploitation of digital data. Therefore, the criminal legal system needs to provide adequate protection for personal data as part of efforts to maintain the security and integrity of the digital economic system.

Regulations within the personal data protection legal framework also emphasize the importance of data controllers' responsibility to manage user information legally and responsibly. In the digital economy, data controllers are the parties with the authority to determine the purposes and methods of processing personal data collected through digital platforms.[24] These responsibilities include ensuring data security, preventing unauthorized access to user information, and ensuring that data processing is carried out in accordance with personal data protection principles. If a data controller fails to fulfill their obligations, resulting in data leakage or misuse, they may be held legally liable. Therefore, data controller responsibility is a crucial tool in maintaining data management accountability in an increasingly complex digital economy.

From a criminal law perspective, criminal liability is a fundamental principle that determines whether a person can be held accountable for an unlawful act. This concept stems from the basic principle that not every unlawful act automatically gives rise to criminal liability without any element of fault on the part of the perpetrator. Classical criminal law doctrine recognizes two primary elements that form the basis of criminal liability: actus reus and mens rea. Actus reus refers to the existence of an unlawful act, while mens rea relates to the presence of intent or fault accompanying the act.[25] These two elements must be proven cumulatively for someone to be found guilty of a crime. In digital economic crimes, proving these elements often faces various challenges because the criminal activity is conducted through complex technological systems.

---

[23] Faisal, N., Aswari, A., & Ilham, M. A. (2025). Penegakan Hukum Terhadap Eksistensi Tindak Pidana Pemalsuan Identitas di Era Digital. *LEGAL DIALOGICA*, *1*(1), 1-19. https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1672

[24] Afifah, N. (2024). Tanggung jawab hukum platform e-commerce terhadap keamanan data pribadi pengguna: Analisis berdasarkan UU PDP 2022. *Jurnal Legalitas*, *2*(1), 29-38. https://doi.org/10.58819/jle.v2i1.165

[25] Laila, N., Fatonah, M., & Rahmah, N. (2025). Seberapa Penting Terpenuhinya Unsur Mens Rea dalam Penetapan Perkara Pidana pada Kasus Korupsi di Indonesia. *Triwikrama: Jurnal Ilmu Sosial*, *10*(12), 141-150. https://doi.org/10.9963/8sj41q49

Individual criminal liability in digital economic activities faces various challenges related to the characteristics of the technology used in electronic transactions. Perpetrators of digital crimes often exploit the anonymity of internet networks, false identities, and encryption systems, which make it difficult to directly identify perpetrators. This situation makes it difficult for law enforcement officials to determine the legal entity responsible for a crime occurring in the digital space. Furthermore, digital economic crimes often involve multiple parties playing roles within complex technological systems, raising questions about who actually bears criminal responsibility for a crime. Therefore, a criminal law approach to digital economic crimes requires evidence-based methods that are more adaptive to developments in information technology.

In addition to individuals, modern criminal law systems also recognize the possibility of corporate criminal liability as perpetrators of economic crimes. Within digital platforms, technology companies providing electronic transaction services can act as corporate entities, bearing legal responsibility for the activities occurring within the systems they manage. The theory of corporate criminal liability developed to address the legal need to address economic crimes committed through corporate organizational structures.[26] Some concepts frequently used in this theory include strict liability and vicarious liability, which allow corporations to be held accountable for the actions of individuals within their organization. In the context of digital platforms, a frequently asked question is the extent to which platform providers can be held criminally liable for illegal activities carried out by users within their systems. This issue demonstrates that the development of the digital economy demands an adjustment to the concept of criminal liability within modern legal systems.

Law enforcement against economic crimes on digital platforms also faces challenges related to the limits of state authority within the international legal system. Digital transactions are generally transnational, allowing perpetrators to conduct illegal activities from jurisdictions different from those of the victim or the digital system being used. This situation raises questions about the legal jurisdiction authorized to prosecute perpetrators of digital economic crimes. International law recognizes the principle of territorial jurisdiction, which grants a state the authority to enforce the law against crimes occurring within its territory.[27] However, in the context of transnational digital crime, the principle of extraterritorial jurisdiction is often necessary to reach perpetrators located outside a country's territory. Therefore, combating digital economic crime requires international cooperation and harmonization of legal regulations to ensure effective law enforcement in addressing global economic crime.

Analysis of Normative Ambiguity in Criminal Liability for Digital Platform-Based Economic Crimes

The concept of legal norm ambiguity is a fundamental issue in legal theory, relating to the unclear formulation of a norm, thus opening up wide scope for

[26] Fridawati, T., Gunawan, K., Andika, R., Rafi, M., Ramadhan, R., & Isan, M. (2024). Perkembangan teori pertanggungjawaban pidana di Indonesia: Kajian pustaka terhadap literatur hukum pidana. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, *1*(3), 317-328. https://doi.org/10.71153/jimmi.v1i3.149

[27] Muhtadi, A., & Equity, B. (2026). Perkembangan dan Tantangan Penegakan Hukum Pidana Internasional dalam Menangani Kejahatan Lintas Negara. *Sinergi: Jurnal Ilmiah Multidisiplin*, *2*(1), 1264-1280. https://publikasi.ahlalkamal.com/index.php/sinergi/article/view/362

interpretation in its application. In legal doctrine, norm ambiguity occurs when a legal provision does not provide clear boundaries regarding the scope of behavior prohibited or permitted by law. This condition often arises from the use of general, non-operational terms, or the lack of clear parameters in the legislation. From the perspective of modern legal theory, norm clarity is a crucial element in establishing an effective and predictable legal system for society. Therefore, clarity in the formulation of norms is one of the main requirements for the formation of quality legislation. When a norm is formulated vaguely, it has the potential to create legal uncertainty and open up space for different interpretations in law enforcement practices.

The ambiguity of norms is closely related to the principle of legal certainty, a fundamental principle in a state based on the rule of law. Legal certainty requires that every legal rule be formulated clearly, firmly, and without ambiguity in its application. In criminal law, the principle of legal certainty is even more important because it directly relates to the protection of human rights against the potential abuse of power by the state.[28] Criminal law is inherently repressive because it empowers the state to impose sanctions on individuals deemed to have violated the law. Therefore, criminal law norms must be formulated strictly to avoid uncertainty about what actions can be categorized as criminal. If a criminal norm is formulated vaguely, there is a risk that law enforcement will be subjective and inconsistent.

Various legal experts emphasize the importance of clear norms in the criminal law system as part of protecting citizens' rights. One fundamental principle of criminal law is the principle of nullum crimen sine lege, which states that no act can be punished without first clearly defining it in law.[29] This principle requires that each criminal offense be formulated specifically so that the public can clearly understand the boundaries of behavior prohibited by law. Clarity of norms also serves as the basis for law enforcement officials in determining whether an act can be classified as a crime. When legal norms are formulated unclearly, there is the potential for differences in interpretation among law enforcement officials in interpreting a criminal provision. This situation has the potential to lead to inconsistencies in law enforcement, which can ultimately erode public trust in the legal system.

The implications of normative ambiguity extend beyond theoretical aspects of law to directly impact the effectiveness of law enforcement in practice. Law enforcement officials often face difficulties in determining whether a particular act constitutes a violation of the law when the norms governing it do not provide clear boundaries. In judicial practice, normative ambiguity can also lead to disparities in decisions, as judges have broad interpretive latitude in interpreting legal provisions. This can lead to inconsistent application of the law to cases with similar characteristics. In the long term, normative ambiguity can weaken the law's function as an instrument of social control, as society lacks certainty regarding the legal consequences of an action. Therefore, the formulation of clear and systematic legal norms is a crucial prerequisite for creating an effective legal system.

The problem of normative ambiguity can also be found in legal regulations related

[28] Ario, D., Situngkir, S. A., & Situngkir, F. (2025). Living Law, Kepastian Hukum, dan Hak Asasi Manusia: Politik Hukum dalam KUHP 2023 di Indonesia. *lentera*, *7*(1), 31-42. https://doi.org/10.32505/lentera.v7i1.13426

[29] Yamin, B., & Rachman, M. T. (2025). Problematik Yuridis Pasal 2 KUHP Baru Dalam Perspektif Prinsip-Prinsip Dasar Asas Legalitas. *Unizar Law Review*, *8*(2), 170-180. https://doi.org/10.36679/ulr.v8i2.106

to digital economic crimes. The rapid development of information technology is often not accompanied by adequate updates to legal regulations. Many legal provisions used to prosecute perpetrators of digital economic crimes were originally formulated to regulate conventional economic activities occurring in physical spaces. Consequently, the application of these legal norms in the context of digital activities often gives rise to various interpretation problems. Legal norms that are general in nature and do not specifically address the characteristics of technology-based crimes have the potential to create uncertainty in the law enforcement process. This situation indicates a gap between the development of digital technology and the development of existing legal regulations.

The mismatch between digital technology developments and prevailing legal regulations often gives rise to differing interpretations in law enforcement practices. Law enforcement officials frequently use general provisions to prosecute perpetrators of digital economic crimes, even though these norms do not explicitly regulate acts occurring in the digital space. This situation has led to differing interpretations of the boundaries of criminal acts in digital economic activities. These differences in interpretation occur not only among law enforcement officials but also in court decisions handling similar cases. This situation can ultimately create legal uncertainty for the public and businesses conducting economic activities through digital platforms. Therefore, regulatory clarity is a crucial factor in ensuring consistent law enforcement against digital economic crimes.

Regulatory ambiguity regarding the responsibilities of digital platform providers is one of the most prominent forms of normative ambiguity in the digital economy ecosystem. Digital platforms generally act as intermediaries, providing the technological infrastructure for transactions between businesses and consumers. However, the legal status of platforms as service providers often raises debate about the extent of their responsibility for user activities within the system. In some cases, digital platforms are viewed simply as technological providers and cannot be held accountable for illegal user activity.[30] On the other hand, there is a view that platforms have a specific responsibility to prevent abuse of the systems they manage. The debate over the concept of intermediary liability demonstrates that existing legal regulations do not yet provide clear boundaries regarding platform providers' responsibilities in addressing digital economic crime.

Another equally significant issue in digital platform-based economic crimes is the difficulty in determining criminal liability. The characteristics of digital technology allow perpetrators to conceal their identities through the use of anonymous accounts, virtual networks, and difficult-to-trace encryption technology. This makes the process of identifying perpetrators far more complex than with conventional crimes. Law enforcement officials often face difficulties in determining who is truly responsible for a crime occurring in a digital system. This situation is further complicated when criminal activity involves multiple parties located in different jurisdictions. As a result, the law enforcement process for digital economic crimes often faces significant obstacles, both during the investigation and prosecution stages, and during the evidentiary process in court.

The issue of proof is one of the main challenges in law enforcement against digital platform-based economic crimes. In the Indonesian criminal law system, proof is principally based on a negative statutory system of proof, which requires judges to base

[30] Rauf, A., Annah, A., & Djamro, R. A. (2025, March). Tanggung Jawab Hukum Penyedia Layanan Internet Terhadap Konten Ilegal Di Dunia Maya. In *SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi* (Vol. 14, No. 1, pp. 48-56). https://doi.org/10.36774/sisiti.v14i1.1674

their decisions on valid evidence and the judge's conviction. In digital crimes, the evidence used is no longer limited to conventional evidence such as witness testimony or physical documents, but also involves electronic evidence originating from information technology systems. The characteristics of electronic evidence differ from conventional evidence because it is digital, easily duplicated, and can be modified without leaving easily identifiable traces. This situation presents unique challenges in ensuring the authenticity and integrity of evidence presented in the judicial process. Therefore, the criminal law system needs a clear mechanism to ensure that electronic evidence used in the trial truly has accountable legal validity.

The validity of digital evidence in criminal justice is a crucial issue in handling technology-based economic crimes. The Indonesian legal system has recognized electronic evidence through the provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, which stipulates that electronic information and electronic documents can be used as valid legal evidence. This recognition of electronic evidence is a crucial step in adapting the legal system to developments in information technology. However, in judicial practice, various issues remain regarding the validity, authenticity, and integrity of digital evidence presented in court. Digital evidence can easily be manipulated or engineered through certain technologies, raising doubts about its validity. This situation requires stricter evidentiary standards and verification procedures to ensure that the digital evidence used truly reflects the actual facts.

The complexity of proving evidence in digital economic crimes is also related to the nature of digital transactions, which often involve various interconnected technological systems. Transaction activities on digital platforms involve more than one party but can involve various entities, such as users, platform providers, payment service providers, and financial institutions that process the transactions. These complex digital transaction chains often produce data trails spread across different systems and jurisdictions. In certain situations, tracing digital transaction flows requires in-depth technical analysis to determine the interconnections between the various digital activities. This complexity presents a challenge for law enforcement officials, who must be able to understand the technical aspects of information technology systems. Without adequate technical capabilities, the process of proving evidence in digital economic crimes can potentially encounter significant obstacles.

In the face of this complexity, digital forensics plays a crucial role in the process of proving digital economic crimes. Digital forensics is a scientific method used to identify, collect, analyze, and present digital evidence that can be used in legal proceedings.[31] Through digital forensics techniques, law enforcement officials can trace the digital activities of criminals, including transaction traces, electronic communications, and activity within digital systems. This process allows investigators to more accurately reconstruct the chronology of events in a digital crime case. However, the application of digital forensics also faces various challenges, particularly related to the limited human resources with technical expertise in this field. Therefore, strengthening the capacity of law enforcement institutions in the field of digital forensics is an urgent need in addressing technology-based economic crimes.

The ambiguity of norms governing digital economic crime also has a significant

[31] Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi peran digital forensik dalam penyidikan tindak pidana siber: Analisis kritis terhadap konstruksi hukum pidana di Indonesia. *Jurnal Tana Mana*, *6*(2), 289-296. https://doi.org/10.33648/jtm.v6i2.1194

impact on legal certainty for both businesses and users of digital platforms. When legal norms governing digital economic activities are not clearly formulated, businesses often face uncertainty regarding the limits of their legal responsibilities. This situation can raise concerns for technology companies conducting business activities through digital platforms. On the other hand, digital platform users also face potential uncertainty regarding the legal protection available if they become victims of digital economic crime. This legal uncertainty can hamper the development of the digital economy, as businesses and the public become hesitant to utilize digital technology optimally. Therefore, regulatory clarity is a crucial factor in creating a healthy and sustainable digital economic ecosystem.

Ambiguity of norms also potentially opens up opportunities for criminals to exploit legal loopholes to conduct illegal activities through digital platforms. When regulations do not clearly address forms of digital economic crime, criminals can easily exploit these gaps or ambiguities to avoid legal accountability. The dynamic and ever-evolving nature of digital technology creates room for the emergence of various new criminal modus operandi that have not yet been fully anticipated by the existing legal system.[32] This situation indicates that a legal system that is not adaptive to technological developments has the potential to lag behind the dynamics of digital economic crime. If this situation persists, the effectiveness of criminal law enforcement in tackling digital economic crime will further weaken. Therefore, updating legal regulations is a crucial step to close various legal loopholes that can be exploited by criminals.

Facing these challenges, reformulating criminal law policy is an unavoidable necessity in a modern legal system. The criminal policy approach emphasizes that criminal law must adapt to social, economic, and technological developments occurring in society. In the context of the digital economy, criminal law reformulation must consider the specific characteristics of technology-based economic activities, which differ from conventional economic activities. Integrating information technology regulations, digital economic policies, and criminal law is a strategic step in creating a more comprehensive legal system. This approach also requires stronger coordination between various state institutions authorized to regulate the digital economy sector. Thus, criminal law reform should not only focus on repressive aspects but also encompass preventive efforts to prevent digital economic crimes.

From the perspective of modern legal theory, a responsive legal approach is a relevant model for addressing the dynamics of digital economic development. The concept of responsive law emphasizes that the legal system must be able to adapt to social and technological changes occurring in society. In digital economic crimes, a responsive legal approach demands more specific and adaptive regulations that address the characteristics of digital platform-based economic activities. Clear regulations regarding platform provider responsibilities, user protection, and law enforcement mechanisms are crucial elements in creating legal certainty in the digital economy. Furthermore, strengthening criminal accountability mechanisms within the digital platform ecosystem is also necessary to ensure that all parties involved in digital economic activities can be held accountable for violations of the law. Thus, a responsive legal approach is expected to create a balance between public protection and the development of innovation in the digital economy.

[32] Andhitya, R., & Umam, J. (2025). Analisis Kritis Terhadap Penegakan Hukum Dalam Penanganan Kejahatan Siber Pada Kasus Data Breach Dalam Perspektif Hukum Pidana Indonesia. *Jurnal Hukum Lex Generalis*, *6*(7). https://doi.org/10.56370/jhlg.v6i7.1002

CONCLUSION

The development of the digital economy through information technology-based platforms has created new dynamics in economic activity and given rise to various forms of economic crime that are increasingly complex and difficult to address using conventional legal instruments. Normative analysis shows that the Indonesian criminal law system essentially has several regulatory instruments to address digital economic crime, but these regulations are scattered, general in nature, and do not specifically address the characteristics of crimes emerging within the digital platform ecosystem. The ambiguity of norms in various legal provisions raises issues in determining the limits of responsibility of perpetrators, platform providers, and evidentiary mechanisms in law enforcement processes, potentially creating legal uncertainty for both the public and digital businesses. This situation also demonstrates the gap between the rapid development of digital technology and the ability of legal regulations to anticipate the ever-evolving modes of economic crime. The complexity of electronic evidence-based evidence, issues of digital jurisdiction, and the ambiguity of platform responsibility demonstrate that the criminal law system still faces serious challenges in ensuring effective law enforcement in the digital space. This situation emphasizes the importance of reformulating criminal law policies that are more adaptive, integrative, and responsive to technological developments and the characteristics of the digital economy. These reforms need to be directed at establishing clearer regulations, strengthening criminal accountability mechanisms within the digital platform ecosystem, and increasing the capacity of law enforcement to address technology-based economic crimes in order to ensure legal certainty and protect the public in the digital economy era.

BIBLIOGRAPHY

Afifah, N. (2024). Tanggung jawab hukum platform e-commerce terhadap keamanan data pribadi pengguna: Analisis berdasarkan UU PDP 2022. Jurnal Legalitas, 2(1), 29-38. https://doi.org/10.58819/jle.v2i1.165

Agustina, P. M. (2025). Implementasi Peraturan Kejaksaan Nomor 19 Tahun 2020 tentang Penyelesaian Uang Pengganti dalam Perspektif Asas Legalitas. Lex Positivis, 3(2), 82-111. https://jtamfh.ulm.ac.id/index.php/jtamfh/article/view/170

Amory, J. D. S., & Mudo, M. (2025). Transformasi ekonomi digital dan evolusi pola konsumsi: Tinjauan literatur tentang perubahan perilaku belanja di era internet. Jurnal Minfo Polgan, 14(1), 28-37. https://doi.org/10.33395/jmp.v14i1.14608

Andhitya, R., & Umam, J. (2025). Analisis Kritis Terhadap Penegakan Hukum Dalam Penanganan Kejahatan Siber Pada Kasus Data Breach Dalam Perspektif Hukum Pidana Indonesia. Jurnal Hukum Lex Generalis, 6(7). https://doi.org/10.56370/jhlg.v6i7.1002

Arifuddin, Q., Riswan, R., HR, M. A., Bulkis, B., Latif, A., Salma, S., ... & Indah, N. (2025). Metodologi penelitian hukum. PT. Sonpedia Publishing Indonesia.

Ario, D., Situngkir, S. A., & Situngkir, F. (2025). Living Law, Kepastian Hukum, dan Hak Asasi Manusia: Politik Hukum dalam KUHP 2023 di Indonesia. lentera, 7(1), 31-42. https://doi.org/10.32505/lentera.v7i1.13426

Djauzie, M. Z. (2025). Pancasila Sebagai Grundnorm Menurut Teori Hukum Murni Hans Kelsen Dan Teori Hukum Responsif Oleh Philippe Nonet Dan Philip Selznick. Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat, 11(1), 239-252. https://doi.org/10.55809/tora.v11i1.456

Faisal, N., Aswari, A., & Ilham, M. A. (2025). Penegakan Hukum Terhadap Eksistensi Tindak Pidana Pemalsuan Identitas di Era Digital. LEGAL DIALOGICA, 1(1), 1-19. https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1672

Farahdiva, A. T., Mulyana, S. L., & Asri, T. P. (2025). Implementasi Cyber Security Pada Sistem Transaksi Keuangan Digital. Jurnal Ilmiah Ekonomi, Manajemen, Bisnis Dan Akuntansi, 2(4), 276-289. https://doi.org/10.61722/jemba.v2i4.1157

Fridawati, T., Gunawan, K., Andika, R., Rafi, M., Ramadhan, R., & Isan, M. (2024). Perkembangan teori pertanggungjawaban pidana di Indonesia: Kajian pustaka terhadap literatur hukum pidana. Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin, 1(3), 317-328. https://doi.org/10.71153/jimmi.v1i3.149

Gusmarani, R., & Zulyadi, R. (2025). Kriminal VS Kriminologi. Yayasan Tri Edukasi Ilmiah.

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjaun Yuridis Penegakkan Hukum Kejahatan Cyber Crime Studi Implementasi Undang-Undang Nomor 11 Tahun 2008. MAQASIDI: Jurnal Syariah Dan Hukum, 40-55. https://doi.org/10.47498/maqasidi.v4i1.2966

Harefa, S., & Nashir, M. A. (2025). SH Pertanggungjawaban Pidana Korporasi Dalam Kasus Pelanggaran Lingkungan Hidup Di Indonesia: Pertanggungjawaban Pidana Korporasi Dalam Kasus Pelanggaran Lingkungan Hidup Di Indonesia. ADIL: Jurnal Hukum, 16(1), 36-60. https://doi.org/10.33476/ajl.v16i1.4966

Herawati, E., Mustopa, H., Sander, M., & Fujianti, P. J. (2025). Analisis Yuridis Terhadap Tanggung Jawab Korporasi Dalam Tindak Pidana Kejahatan Luar Biasa Di Bidang Ekonomi. Jurnal Sosial Teknologi, 5(7), 2819-2831. https://doi.org/10.59188/jurnalsostech.v5i7.32225

Ikhsan, M., bin Sapa, N., & Syatar, A. (2025). Ekonomi Digital dan Hukum Ekonomi Syariah: E-Commerce, Aset Digital dan Implikasi Hukumnya Menurut Hukum Islam. Socius: Jurnal Penelitian Ilmu-Ilmu Sosial, 3(1).

Insani, N. S., Mulyana, R. N., & Hosnah, A. U. (2026). Dampak Perubahan Sosial Terhadap Pola Kejahatan: Perspektif Kriminologi. Al-Zayn: Jurnal Ilmu Sosial & Hukum, 4(1), 3166-3176. https://doi.org/10.61104/alz.v4i1.3610

Laila, N., Fatonah, M., & Rahmah, N. (2025). Seberapa Penting Terpenuhinya Unsur Mens Rea dalam Penetapan Perkara Pidana pada Kasus Korupsi di Indonesia. Triwikrama: Jurnal Ilmu Sosial, 10(12), 141-150. https://doi.org/10.9963/8sj41q49

Mahera, R. M., & Suryadi, N. (2025). Transformasi mekanisme pasar dalam ekonomi berbasis teknologi digital. Socius: Jurnal Penelitian Ilmu-Ilmu Sosial, 2(11). https://www.ojs.daarulhuda.or.id/index.php/Socius/article/view/1558

Muflikh, A. A. M., Ramadan, D. R. C., Silalahi, B. B. S., Martitah, M., & Sulistianingsih, D. (2025). Analisis Perlindungan Hukum Konsumen pada Perjanjian Transaksi E-Commerce terkait Investasi Kripto Ilegal via Media Sosial. Bookchapter Hukum dan Politik dalam Berbagai Perspektif, 4, 106-133. https://bookchapter.unnes.ac.id/index.php/hp/article/view/609

Muhtadi, A., & Equity, B. (2026). Perkembangan dan Tantangan Penegakan Hukum Pidana Internasional dalam Menangani Kejahatan Lintas Negara. Sinergi: Jurnal Ilmiah Multidisiplin, 2(1), 1264-1280. https://publikasi.ahlalkamal.com/index.php/sinergi/article/view/362

Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi peran digital forensik dalam penyidikan tindak pidana siber: Analisis kritis terhadap konstruksi hukum

pidana di Indonesia. Jurnal Tana Mana, 6(2), 289-296. https://doi.org/10.33648/jtm.v6i2.1194

Ramadhan, A., & Novitasari, K. (2023). Strategi pengembangan literasi ekonomi berbasis digital terhadap regulasi pemberdayaan perilaku sosial dan sumber daya manusia di era industri 4.0. AB-JOIEC: Al-Bahjah Journal of Islamic Economics, 1(1), 14-25. https://doi.org/10.61553/abjoiec.v1i1.10

Rauf, A., Annah, A., & Djamro, R. A. (2025, March). Tanggung Jawab Hukum Penyedia Layanan Internet Terhadap Konten Ilegal Di Dunia Maya. In SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi (Vol. 14, No. 1, pp. 48-56). https://doi.org/10.36774/sisiti.v14i1.1674

Rumahorbo, L., & Yusuf, H. (2025). Analisis Mendalam Perilaku Menyimpang White Collar Crime (Studi Kasus melalui Lensa Teori Convenience). Media Hukum Indonesia (MHI), 3(3). https://ojs.daarulhuda.or.id/index.php/MHI/article/view/2195

Sari, D. P., Safa, M. S., & Fahlevi, A. R. (2026). Perlindungan Hukum Konsumen dalam Transaksi E-Commerce di Indonesia: Perspektif Hukum Perdata dan Undang-Undang Perlindungan Konsumen. RIGGS: Journal of Artificial Intelligence and Digital Business, 5(1), 6311-6318. https://doi.org/10.31004/riggs.v5i1.6942

Setiawan, D. A. (2024). Strategi Penanggulangan Kejahatan Ekonomi Berbasis Teknologi: Studi Komparatif Antara Indonesia, Amerika, Dan Eropa. Masalah-Masalah Hukum, 53(1), 78-89. https://doi.org/10.14710/mmh.53.1.2024.78-89

Suciana, H. E., Fardiansyah, A. I., & Tamza, F. B. (2025). UPAYA PENEGAKAN HUKUM TERHADAP KEJAHATAN EKONOMI DALAM SISTEM PERADILAN PIDANA. Jurnal Pendidikan Sejarah dan Riset Sosial Humaniora, 5(2), 106-114. https://ejournal.penerbitjurnal.com/index.php/humaniora/article/view/1272

Sukmawan, Y. A., & Damayanti, D. (2025). Metode Penelitian Hukum Normatif dan Empiris sebagai Strategi Penguatan Perspektif Kajian Ilmu Hukum. Notary Law Journal, 4(3), 114-128. https://doi.org/10.32801/nolaj.v4i3.116

Sulistyowati, R., Listiadi, A., Subroto, W. T., Ramadhani, S. N., Sarfita, D., Damayanti, F., ... & Weni, W. (2025). Pembelajaran Ekonomi Digital: Konsep, Transformasi Pasar Dan Kesiapan Teknologi. Penerbit Tahta Media.

Utomo, A. P., Ibrohim, N. M., Ramadhani, N., Zidni, N. M., & Wahyuaristy, D. S. (2025). Konsep ideal regulasi identitas digital tunggal dalam konvergensi teknologi sebagai instrumen penguatan perdagangan digital berbasis ekonomi virtual. Forschungsforum Law Journal, 2(02), 119-141. https://doi.org/10.35586/flj.v2i02.11161

Yamin, B., & Rachman, M. T. (2025). Problematik Yuridis Pasal 2 KUHP Baru Dalam Perspektif Prinsip-Prinsip Dasar Asas Legalitas. Unizar Law Review, 8(2), 170-180. https://doi.org/10.36679/ulr.v8i2.106