Indonesian Journal of Law and Justice Volume: 3, Number 2, 2025, *Page*: 1-9

Corporate Criminal Liability in Digital Economic Crimes: an Analysis of Legal Developments in Indonesia

Nanin Koeswidi Astuti

Universitas Kristen Indonesia

DOI:
https://doi.org/10.47134/ijlj.v3i2.5013
*Correspondence: Nanin Koeswidi Astuti
Email: naninkoeswidi@uki.ac.id

Received: 28-10-2025
Accepted: 28-11-2025
Published: 28-12-2025

Abstract: This study analyzes the evolution of legal frameworks and the implementation of corporate criminal liability in digital economic crimes in Indonesia. Using a normative juridical method supported by empirical data, the research examines statutory regulations, official institutional reports, and relevant case studies involving digital corporate offenses such as illegal fintech operations, e-commerce fraud, and cryptocurrency-based money laundering. The findings reveal that despite the recognition of corporations as subjects of criminal law under the 2023 Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and the Anti-Money Laundering Law (TPPU Law), law enforcement remains focused on individual offenders and rarely addresses systemic organizational fault. Comparative analysis shows that Indonesia has not yet adopted the corporate culture liability model widely applied in international jurisdictions, which evaluates structural negligence and corporate ethical culture. The study concludes that a reformulation of Indonesia's criminal law policy is required to emphasize comprehensive corporate accountability and to enhance law enforcement mechanisms in addressing digital economic crimes effectively.

Keywords: Corporate Criminal Liability, Corporation, Digital Economy, Indonesian Criminal Law

Introduction

The rapid advancement of digital technology has fundamentally transformed the global economic landscape, including that of Indonesia. According to the We Are Social and Meltwater Report (2024), Indonesia recorded 221 million internet users, representing approximately 79.5% of the population, with the digital economy projected to reach a value of USD 110 billion by 2025 (Google, Temasek, Bain, 2024). The exponential growth of electronic transactions, financial technology (fintech), crypto assets, and digital marketplaces has created tremendous economic efficiency, yet simultaneously opened new vulnerabilities to digital economic crimes such as online fraud, data manipulation, identity theft, and cyber laundering (Nugroho, 2022) (Sembiring, 2022).

Empirical data from the Cybercrime Directorate of the Indonesian National Police (Bareskrim Polri, 2023) recorded more than 16,500 cybercrime cases in 2023 increase of approximately 32% compared to the previous year. Approximately 40% of these cases were associated with digital economic activities, including unauthorized online lending, crypto fraud, and digital payment misuse (Kementerian Kominfo, 2024). In parallel, the Financial Services Authority Otoritas Jasa Keuangan reported that more than 1,700 illegal fintech entities were blocked between 2020 and 2024 for legal violations, resulting in consumer losses amounting to IDR 5.9 trillion (CNBC Indonesia, 2024; DetikFinance, 2024). These

cases highlight that perpetrators of digital economic crimes are no longer confined to individuals but increasingly involve corporate entities operating through complex digital infrastructures (Rahman, 2023). From a regulatory perspective, Indonesia already possesses several legal instruments providing a normative basis for corporate criminal liability, such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments, Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering (TPPU Law), and the 2023 Criminal Code (KUHP), which explicitly recognizes corporations as subjects of criminal law (Hamzah, 2012; Hiariej, 2021; Muladi & Priyatno, 2010). Nonetheless, the principal challenge lies in implementation and evidentiary proof, particularly in establishing corporate fault and attributing mens rea to a non-natural legal entity (Moeljatno, 2008; Prakoso, 2020; Setiyono, 2021). Law enforcement institutions often remain hesitant or lack technical capacity to apply collective culpability within the hierarchical and policy-based decision structures of corporations (Harahap, 2020) (Mahfud, 2023).

This implementation gap reflects a persistent doctrinal orientation toward individual liability rather than the broader systemic or cultural accountability of corporations. Such limitations contrast with jurisdictions such as the United States, United Kingdom, and Australia, which have developed more progressive doctrines respondeat superior, corporate manslaughter, and corporate culture liability allowing liability to be attributed to organizational failures, permissive cultures, or deficient internal controls (Clarkson, 2015) (Fisse & Braithwaite, 1993) (Gobert & Punch, 2003) (U.S. Department of Justice, 2023) (Wells, 2020). These comparative frameworks demonstrate that effective enforcement of corporate criminal liability requires the integration of structural and cultural factors within legal evaluation, rather than solely focusing on individual acts (Parker, 2021). In the context of a globalized digital economy, the absence of robust corporate accountability mechanisms threatens Indonesia's economic security, undermines investor confidence, and erodes public trust in digital transactions (Rahardjo, 2021) (Santoso, 2022). Therefore, strengthening corporate criminal liability both normatively and practically is crucial for establishing a just, preventive, and adaptive criminal justice system capable of addressing cross-sectoral and transnational digital economic crimes (Hartono, 2024).

Accordingly, this study aims to analyze the conceptual evolution and practical implementation of corporate criminal liability in Indonesia's digital economic crimes. It will explore the interplay between national regulations and enforcement realities, compare them with international practices, and propose a model suited to Indonesia's socio-legal context. The findings are expected to contribute theoretically to the modernization of corporate criminal law and practically to policy recommendations for harmonizing national law with global best practices in the digital era (Asshiddiqie, 2022) (Harahap, 2020) (Marzuki, 2023).

Methodology

This study employs a normative juridical (doctrinal legal research) approach, complemented by limited empirical observations to strengthen contextual validity. The normative juridical approach is used because the core issue lies in examining positive legal norms, doctrinal interpretations, and juridical constructs that govern corporate criminal liability within the framework of Indonesia's criminal law system (Ishaq, 2019) (Marzuki, 2017) (Soekanto & Mamudji, 2015). This approach emphasizes the law in books perspective, which allows systematic evaluation of how corporate criminal liability is formulated, interpreted, and implemented within Indonesia's codified and special legislation (Asshiddiqie, 2022) (Hiariej, 2021). Within this framework, the research conducts a doctrinal analysis focusing on the internal consistency of statutory provisions and their interpretative coherence in academic and judicial discourse (Muladi & Priyatno, 2010) (Prakoso, 2020). Primary legal materials include Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments, Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering (TPPU Law), and Law No. 1 of 2023 concerning the new Criminal Code (KUHP). These are analyzed alongside implementing regulations, OJK circulars, and Supreme Court decisions to evaluate how the legislative intent is operationalized in corporate criminal cases (Hartono, 2024) (Mahfud, 2023) (Setiyono, 2021).

Secondary legal materials consist of authoritative doctrinal commentaries, peer-reviewed journal articles, and textbooks that elaborate on theories of corporate mens rea and the moral foundations of organizational liability (Hamzah, 2012) (Hiariej, 2021) (Muladi & Priyatno, 2010) (Rahardjo, 20210 (Santoso, 2022). Through this analysis, the research identifies the conceptual transformation from individual culpability (individual mens rea) to collective or systemic fault that arises within a corporate structure (Fisse & Braithwaite, 1993) (Gobert & Punch, 2003) (Wells, 2020). To enrich the normative analysis, this study adopts a comparative jurisprudence approach, examining models of corporate criminal liability in the United States, United Kingdom, and Australia. These jurisdictions were chosen because each represents a distinct doctrinal trajectory: respondeat superior (vicarious liability) in the U.S., identification theory and corporate manslaughter in the U.K., and the corporate culture model in Australia (Clarkson, 2015) (U.S. Department of Justice, 2023) (Wells, 2020). Comparative analysis helps assess the transferability and adaptability of these foreign models into Indonesia's civil-law system, considering differences in legal philosophy, prosecutorial discretion, and enforcement infrastructure (Asshiddiqie, 2022) (Park et al, 2022).

Furthermore, to bridge the law in books and law in action, a limited empirical component is integrated to demonstrate how digital economic crimes manifest in practice. Three representative case studies were purposively selected: (1) illegal fintech operations investigated by the Financial Services Authority; (2) e-commerce fraud handled by the Cybercrime Directorate of the Indonesian National Police (Bareskrim Polri, 2023); and (3) cryptocurrency-based money-laundering cases reported by the Financial Transaction Reports and Analysis Center. These cases reveal the complexity of attributing corporate fault where digital infrastructures obscure responsibility among shareholders, directors, and algorithmic systems (Sembiring, 2022).

By combining doctrinal, comparative, and empirical elements, this research constructs an integrative framework for understanding how corporate criminal liability operates in Indonesia's digital economic ecosystem. This hybrid methodology provides both theoretical depth and pragmatic insight—linking legal principles, institutional practices, and governance challenges (Hartono, 2024) (Rahman, 2023). Ultimately, it offers a normative-empirical synthesis that can guide future legal reform and institutional strengthening, ensuring Indonesia's criminal justice system remains adaptive, just, and responsive to transnational digital crimes (Asshiddiqie, 2022) (Harahap, 2020) (Marzuki, 2023).

Result and Discussion

Overview of Digital Economic Crimes Involving Corporate Entities

An examination of data from the Financial Services Authority (OJK), the Financial Transaction Reports and Analysis Center (PPATK), the Cybercrime Directorate of the Indonesian National Police (Bareskrim Polri), and the Ministry of Communication and Information Technology (Kominfo) for the period 2020-2024 reveals that digital economic crimes involving corporate entities have become increasingly complex and cross-sectoral in nature. These cases not only cause significant financial losses to the public but also undermine the stability of the national financial system and erode public trust in Indonesia's digital economy.

The table below illustrates that the implementation of corporate criminal liability remains weak in practice, as the majority of cases conclude with sanctions imposed solely on individual offenders, while the corporate entities themselves are rarely prosecuted as subjects of criminal law. This evidences a persistent enforcement gap between normative recognition of corporate criminal liability and its actual application within Indonesia's legal framework.

Table 1. Types and Data of Digital Economic Crimes Involving Corporate Entities (2020–2024)

No	Type of Crime	Number of Cases (2020-2024)	Estimated Financial Losses (IDR)	Relevant Authorities:	Status of Legal Enforcement
1	Illegal fintech operations and fraudulent investment schemes	1,700 entities blocked	± IDR 5.9 trillion	Financial Services Authority (OJK); Ministry of Communication and Information Technology (Kominfo)	45 cases under police investigation; 5 corporate entities prosecuted before the court
2	*E-commerce fraud and customer data manipulation*	365 cases reported	± IDR 1.2 trillion	Cybercrime Directorate, Indonesian National Police	Predominantly prosecuted against individual offenders;

No	Type of Crime	Number of Cases (2020-2024)	Estimated Financial Losses (IDR)	Relevant Authorities:	Status of Legal Enforcement
				(Bareskrim Polri)	corporate entities have not yet been subjected to criminal liability proceedings
3	*Cryptocurrency-based money laundering*	425 suspicious transaction reports (STRs) related to money laundering activities	± IDR 2.8 trillion	Indonesian Financial Transaction Reports and Analysis Center (PPATK)	Under ongoing cross-border monitoring and coordination with international financial intelligence units
4	Personal data breaches and illicit data sales	240 reported incidents	Unquantifiable (non-financial losses related to privacy and reputational harm)	Ministry of Communication and Information Technology (Kominfo)	Law enforcement actions limited to individual perpetrators; corporate entities involved have not been subjected to prosecution

Source: Bareskrim Polri (2023), Kementerian Kominfo (2024)

Normative Analysis of National Regulations

Within the framework of Indonesia's positive law, corporate criminal liability has been explicitly recognized under the new Criminal Code (Law No. 1 of 2023). Articles 45 to 52 stipulate that a corporation may be held criminally liable when:

1. The criminal act is committed by a manager or a person having a working relationship with the corporation;
2. The act is carried out within the scope of the corporation's business activities; and
3. The act provides benefit or advantage to the corporation.

Despite this recognition, no structural assessment mechanism currently exists to evaluate systemic corporate fault, such as failures in internal supervision, compliance negligence, or corporate culture deficiencies. Consequently, law enforcement practices remain individual centered, focusing primarily on personal liability rather than organizational culpability. This limitation is evident in recent cases involving illegal fintech

operations and customer data breaches, where only individual perpetrators were prosecuted while the corporate entities themselves escaped criminal responsibility.

Empirical Analysis of Representative Cases

An analysis of several representative cases reveals that law enforcement practices concerning digital economic crimes involving corporate entities in Indonesia remain partial and predominantly individualistic. The illegal fintech case "PinjamCepat" (Bareskrim Polri, 2024) demonstrates how a foreign-registered corporation operating without authorization from the Financial Services Authority (OJK) engaged in intimidatory debt collection practices through digital platforms. However, law enforcement efforts targeted only local operators, leaving the parent corporate entity beyond prosecution. This situation highlights weaknesses in cross-border jurisdiction and the absence of a transnational corporate liability framework.

The e-commerce fraud case "TokDeal" (Bareskrim Polri, 2023) further illustrates this issue. Manipulation of product prices and user transaction data was perpetrated by the company's IT division to obtain financial gain. Nevertheless, the corporation itself was not held criminally liable on the grounds that the acts were committed by individual employees without managerial knowledge. From the perspective of vicarious liability, however, the corporation should still bear responsibility, as the wrongful act occurred within the scope of employment and for the benefit of the corporate entity.

The cryptocurrency-based money laundering case also exposes deficiencies in internal compliance and monitoring systems within digital asset companies. The lack of robust due diligence mechanisms enabled anonymous cross-border transactions to be used as instruments of money laundering. This condition underscores the relevance of adopting the Corporate Culture Model, in which culpability is attributed not only to individual actions but also to organizational culture and systemic negligence in internal control mechanisms.

Overall, these three cases demonstrate that corporate criminal liability in Indonesia's digital economic crimes remains ineffective, as the current legal approach does not yet accommodate the collective, structured, and cross-jurisdictional nature of digital criminal conduct.

Comparative Analysis of Corporate Liability Models (Indonesia vs International Jurisdictions)

A comparative examination of corporate criminal liability systems between Indonesia and several other jurisdictions reveals fundamental differences in how corporate fault is assessed. In Indonesia, under the Criminal Code, the Electronic Information and Transactions Law (ITE Law), and the Anti Money Laundering Law (TPPU Law), corporations have been formally recognized as subjects of criminal law. However, the implementation of these provisions continues to focus primarily on individual managerial wrongdoing, without adequately addressing systemic organizational failures. In contrast, the United States applies the principle of vicarious liability, under which a corporation may

be held criminally responsible if an employee commits an offense in the course of employment and for the benefit of the corporation. The United Kingdom, through the Corporate Manslaughter and Corporate Homicide Act 2007, emphasizes structural or managerial failures within the organization as the basis of corporate culpability. Meanwhile, Australia adopts the corporate culture model, which attributes liability to a corporation based on its internal culture, ethical climate, and negligence in maintaining effective internal control and compliance mechanisms. From this comparison, it becomes evident that Indonesia remains in the early stage of developing a mature framework for corporate criminal liability. The country's legal system should move toward adopting the corporate culture model, as implemented in Australia, because it provides a more comprehensive and contextually appropriate foundation for assessing corporate responsibility in digital economic crimes that are collective, systemic, and technology driven.

The results of the analysis indicate that corporate criminal liability in digital economic crimes in Indonesia continues to face significant challenges, both in terms of regulatory framework and practical implementation. Although the Criminal Code (KUHP, 2023), the Electronic Information and Transactions Law (ITE Law), and the Anti Money Laundering Law (TPPU Law) formally recognize corporations as subjects of criminal law, their enforcement in practice remains largely centered on individual managerial responsibility, rather than on the corporate entity as a collective offender. Cases such as illegal fintech operations, e-commerce fraud, and cryptocurrency-based money laundering clearly demonstrate weaknesses in establishing systemic fault and in ensuring effective internal corporate oversight. In comparison with other jurisdictions, Indonesia still lags behind in developing mechanisms to assess structural or organizational culpability. The United States and the United Kingdom have long implemented the principles of vicarious liability and organizational failure, respectively, while Australia emphasizes the corporate culture model, which evaluates the ethical climate and institutional negligence within the organization. Accordingly, for Indonesian criminal law to become more adaptive to the evolving digital economy, it is imperative to reformulate the concept of corporate criminal liability. Such reform should not only impose sanctions on individuals but also assess the moral, cultural, and institutional responsibility of corporations in preventing and mitigating digital economic crimes.

Conclusion

Corporate criminal liability in digital economic crimes in Indonesia has made significant normative progress through the 2023 Criminal Code (KUHP), the ITE Law, and the Anti-Money Laundering Law (TPPU), which explicitly recognize corporations as subjects of criminal law. Nevertheless, the practical enforcement of these provisions remains limited due to the continued focus on individual liability, weak inter-agency coordination, and the absence of clear procedural frameworks for prosecuting corporate entities in digital contexts. To strengthen the system, policymakers should prioritize developing comprehensive prosecutorial guidelines, enhancing digital forensic capacity, and fostering institutional collaboration among law enforcement, financial authorities, and cyber regulators. Furthermore, future research should explore the empirical effectiveness of the

Corporate Culture Liability model in Indonesian legal practice, particularly in assessing how organizational behavior, governance structures, and internal compliance systems influence corporate culpability in digital crimes. This approach would not only refine theoretical understanding but also inform the formulation of evidence-based reforms to ensure corporate accountability in Indonesia's rapidly evolving digital economy.

References

Asshiddiqie, J. (2022). *Hukum dalam Perspektif Globalisasi Digital*. Rajawali Press.

Bareskrim Polri. (2023). Laporan Kejahatan Siber Tahun 2023. *Mabes Polri*.

Bareskrim Polri. (2024). *Laporan Tahunan Direktorat Siber 2023*. Mabes Polri.

Clarkson, C. M. (2015). *Corporate Manslaughter and Regulatory Reform*. Oxford University Press.

CNBC Indonesia. (2024). *OJK Blokir 1.700 Fintech Ilegal, Kerugian Capai Triliunan*.

DetikFinance. (2024). *Kejahatan Ekonomi Digital Meningkat 32% di 2023*.

Fisse, B., & Braithwaite, J. (1993). *Corporations, Crime and Accountability*. Cambridge University Press.

Gobert, J., & Punch, M. (2003). *Rethinking Corporate Crime*. Butterworths.

Google, Temasek, Bain. (2024). *The Future of Southeast Asia's Digital Economy*.

Hamzah, A. (2012). *Asas-Asas Hukum Pidana*. Rineka Cipta.

Harahap, Y. (2020). *Hukum Acara Pidana Indonesia*. Sinar Grafika.

Hartono, S. (2024). *Hukum Siber dan Tanggung Jawab Korporasi di Indonesia*. Gadjah Mada University Press.

Hiariej, E. O. S. (2021). *Prinsip-Prinsip Hukum Pidana*. Erlangga.

Ishaq. (2019). *Metode Penelitian Hukum Normatif*. Refika Aditama.

Kementerian Kominfo. (2024). Laporan Statistik Kejahatan Siber Indonesia 2023. *Kementerian Kominfo*.

Mahfud, M. D. (2023). *Reformasi Sistem Hukum Pidana Nasional*. Alumni.

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi*. Kencana.

Marzuki, P. M. (2023). *Metodologi Penelitian Hukum*. Kencana.

Moeljatno. (2008). *Asas-Asas Hukum Pidana*. Rineka Cipta.

Muladi, & Priyatno, D. (2010). *Corporate Criminal Responsibility*. Refika Aditama.

Nugroho, A. (2022). Cybercrime dan Transformasi Digital Ekonomi. In *Airlangga University Press*.

Park, S., Yoon, H. J., & Jang, S. (2022). Cybersecurity concerns in hotel management systems: Post-pandemic insights. *Computers & Security*, *114*, *102615*. https://doi.org/10.1016/j.cose.2021.102615

Parker, C. (2021). *Corporate Compliance Systems and the Law*. Cambridge University Press.

Prakoso, D. (2020). *Korporasi sebagai Subjek Hukum Pidana*. Setara Press.

Rahardjo, S. (2021). *Hukum Progresif dalam Perspektif Globalisasi Ekonomi*. Kompas.

Rahman, H. (2023). *Keuangan Digital dan Kejahatan Ekonomi Baru*. Pustaka Setia.

Santoso, T. (2022). *Hukum dan Teknologi Finansial di Indonesia*. Rajawali Press.

Sembiring, M. (2022). *Kejahatan Siber dan Perlindungan Konsumen Digital*. USU Press.

Setiyono, B. (2021). *Corporate Criminal Responsibility and Governance Reform in Indonesia*. FH-UII Press.

Soekanto, S., & Mamudji, S. (2015). *Penelitian Hukum Normatif*. RajaGrafindo Persada.

U.S. Department of Justice. (2023). *Evaluation of Corporate Compliance Programs*.

Wells, C. (2020). *Corporations and Criminal Responsibility* (3rd ed.). Oxford University Press.