Ilomata International Journal of Social Science



OPEN ACCESS

RECEIVED 8 December 2025
ACCEPTED 24 February 2026
PUBLISHED 30 April 2026

CITATION
Soraya J, Purborini VS, (2026). Regulating Fintech Abuse in Illegal Online Lending: A Criminal Law and Policy Approach International Journal of Social Science. 7 (2), 525-532.
doi: 10.61194/ijss.v7i2.2065

TYPE Original Research
PUBLISHED 30 April 2026
DOI 10.61194/ijss.v7i2.2065
VOL 7 Issue 2 April 2026



# Regulating Fintech Abuse in Illegal Online Lending: A Criminal Law and Policy Approach

Joice Soraya[1]*, Vivi Sylvia Purborini[2]
[1]Politeknik Negeri Malang, East Java, Indonesia
[2]Universitas Wisnuwardhana Malang, East Java, Indonesia
Correspondence: joice.soraya@polinema.ac.id[1]

## Abstract

The rapid expansion of financial technology (fintech) has transformed digital financial services, particularly in the online lending sector. However, this growth has been accompanied by the proliferation of illegal online lending platforms operating outside formal regulatory frameworks. These platforms often engage in abusive practices, including excessive interest rates, coercive debt collection, misuse of personal data, intimidation, and other forms of cyber-enabled economic crime. This article examines the regulatory and criminal law frameworks governing fintech-related abuses in illegal online lending in Indonesia, focusing on their coherence and limitations. Using a normative juridical approach, the study analyzes statutory regulations, policy instruments, and legal doctrines related to fintech regulation, consumer protection, cybercrime, and criminal liability. The findings reveal that, despite the existence of multiple regulatory and penal mechanisms, the legal framework remains fragmented and institutionally dispersed. Key challenges include overlapping regulatory mandates, weak coordination among supervisory and law enforcement bodies such as the Financial Services Authority (OJK), the Ministry of Communication and Information Technology, and criminal justice institutions and the increasingly transnational nature of digital financial crimes. This article proposes normative recommendations to enhance regulatory coherence, particularly through integrated regulatory supervision. This approach emphasizes structured coordination among relevant authorities, clearer division of institutional responsibilities, shared enforcement mechanisms, and harmonized regulatory standards. By clarifying structural and doctrinal gaps, this study contributes to strengthening consumer protection and improving legal certainty within Indonesia's fintech ecosystem.

KEYWORDS

fintech regulation; illegal online lending; criminal law; legal policy; consumer protection.

## Introduction

The rapid growth of digital financial technology has significantly transformed financial transactions and access to credit in Indonesia, particularly through online lending platforms. While fintech-based lending was initially promoted to expand financial inclusion and efficiency, its accelerated development has outpaced regulatory adaptation and enforcement capacity. This regulatory gap has been exploited by illegal online lending operators, who misuse digital platforms to engage in predatory practices, including excessive interest rates, abusive debt collection, and unlawful processing of personal data. As a result, fintech innovation in the lending sector has not only generated economic opportunities but has also created new forms of regulatory failure and criminal misuse that challenge existing frameworks of business law and criminal law governance (Afriana & Lestari, 2021).

The rapid development of financial technology (fintech) has fundamentally transformed the financial services industry by enabling faster, more efficient, and more inclusive access to financial products, particularly in the lending sector. Digital-based peer-to-peer (P2P) lending platforms have expanded financial inclusion by providing alternative financing for individuals and micro, small, and medium enterprises (MSMEs) that previously had limited access to conventional banking services (Arner, Barberis, &

Buckley, 2017; World Bank, 2020). In Indonesia, the fintech industry has experienced significant growth, supported by regulatory frameworks issued by the Financial Services Authority (Otoritas Jasa Keuangan/OJK), particularly OJK Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending Services(Arner et al., 2017).

However, alongside its positive contributions, the expansion of fintech has also generated serious legal challenges, particularly the proliferation of illegal online lending platforms operating outside the established regulatory framework. These illegal platforms frequently engage in abusive practices, including excessive interest rates, unlawful debt collection, intimidation, defamation, harassment, and the misuse of personal data obtained without valid consent(Atmasasmita, 2021) (Prayogo & Suryani, 2021) (Marzuki, P. M, 2021) Such practices give rise not only to economic harm but also to violations of legally protected rights, including the constitutional right to privacy and personal security under the 1945 Constitution of the Republic of Indonesia, statutory consumer protection guarantees, and data protection obligations under relevant electronic information and personal data protection laws. Consequently, victims of illegal online lending are subjected to systematic legal harms that implicate both individual rights and broader principles of human rights protection within Indonesia's legal system.

From a criminal law perspective, illegal online lending practices involve multiple layers of criminal conduct, including fraud, extortion, threats, identity theft, and unlawful access to electronic information and documents. Such acts fall within the scope of various criminal provisions, including the Indonesian Criminal Code (KUHP), the Law on Electronic Information and Transactions (Law No. 11 of 2008 as amended by Law No. 19 of 2016), and the Consumer Protection Law (Law No. 8 of 1999). Nevertheless, despite the existence of this normative framework, law enforcement against illegal fintech-based lending remains fragmented at multiple levels, including overlapping and inconsistently formulated regulatory norms, divided institutional authority among financial regulators, digital governance bodies, and criminal law enforcement agencies, as well as uneven enforcement practices across jurisdictions (Santoso, 2020) (Santoso, 2020). The complexity of fintech abuse is further aggravated by the transnational nature of digital financial crimes. Many illegal lending platforms operate through cross-border digital infrastructures, server anonymization, and the use of fake corporate identities, making detection, investigation, and prosecution increasingly difficult (UNODC, 2021). This condition exposes significant gaps in regulatory supervision, inter-agency coordination, and the capacity of criminal justice institutions to respond effectively to fintech-based economic crimes(Cruz, 2021).

In addition to the problem of enforcement, regulatory dualism also contributes to legal uncertainty. While fintech activities fall under the supervision of OJK and Bank Indonesia, criminal enforcement is handled by law enforcement agencies. Weak institutional coordination between regulators and criminal justice authorities often results in delayed enforcement, overlapping authority, and ineffective sanctions against perpetrators (Europol, 2022) (Sutedi, 2019). Consequently, the regulatory approach toward fintech abuse has not yet fully integrated preventive supervision with repressive criminal enforcement.

Previous studies have predominantly examined fintech-related disputes through the lenses of consumer protection and civil liability, emphasizing contractual imbalance, standard clauses, and regulatory compliance in digital lending transactions (Afriana & Lestari, 2021; Gomber, 2018). While a number of studies have touched upon criminal aspects of illegal online lending such as fraud, cybercrime, or data misuse these analyses tend to be fragmented and issue-specific, lacking a systematic criminal law and legal policy framework that integrates regulatory supervision, penal liability, and institutional enforcement dynamics (Marzuki, P. M, 2021; Santoso, 2020). Consequently, comprehensive doctrinal analyses that position illegal online lending as a distinct form of fintech-enabled criminality within Indonesia's criminal justice and regulatory systems remain limited.

This gap is particularly significant given the increasing number of victims and the growing economic and social losses caused by illegal online lending practices(Gunningham, 2019).

Therefore, this article aims to analyze the regulation of fintech abuse in illegal online lending from a criminal law and legal policy perspective. Specifically, this study seeks to examine: (1) the forms of criminal acts involved in illegal online lending practices; (2) the adequacy of existing criminal law and regulatory frameworks in addressing fintech abuse; and (3) the policy direction needed to strengthen law enforcement and consumer protection within Indonesia's digital financial ecosystem. By adopting this approach, the study is expected to contribute to the development of a more integrated, effective, and justice-oriented regulatory model for combating illegal fintech-based lending (Komnas HAM, 2022).

Rather than reiterating well-documented problems such as regulatory fragmentation, weak inter-agency coordination, and consumer victimization, this article departs from existing scholarship by advancing a doctrinal reorientation of illegal online lending as a form of *fintech-enabled criminality* that occupies an ambiguous space between administrative regulation and criminal law enforcement. While prior studies predominantly approach illegal online lending through consumer protection, civil liability, or regulatory compliance frameworks, this study situates the phenomenon within the structure of Indonesian criminal law and legal policy, focusing on how existing penal norms are conceptualized, fragmented, and operationalized in practice(Low & Teo, 2020).

The central analytical contribution of this article lies in its examination of the normative disjunction between preventive regulatory supervision and repressive criminal enforcement in Indonesia's fintech governance architecture. Instead of treating regulatory failure merely as an enforcement deficit, this study interrogates how overlapping mandates, sectoral legislation, and the absence of an integrated criminal policy framework shape the selective and inconsistent application of criminal liability to illegal online lending practices(Lubis, 2020). By mapping the interaction between fintech regulation, cybercrime provisions, and general criminal law doctrines, the article offers a systematic legal analysis that moves beyond descriptive accounts of abuse toward a clearer understanding of structural accountability gaps.

Accordingly, this research is not designed to evaluate the empirical effectiveness of sanctions or institutional coordination. Rather, it formulates normative legal arguments grounded in doctrinal analysis to clarify how criminal law can be more coherently positioned within fintech governance. In this context, the notion of an "integrated and justice-oriented regulatory model" is articulated not as a broad policy aspiration, but as a doctrinal proposition calling for clearer allocation of criminal responsibility, harmonization of regulatory and penal norms, and structured coordination between financial regulators and criminal justice institutions(Makarim, 2021).

Based on this analytical framework, the study addresses the following legal questions: (1) how illegal online lending practices are constructed as criminal acts under existing Indonesian criminal and cyber law regimes; (2) how regulatory and penal fragmentation affects the attribution of criminal liability; and (3) how criminal law policy can be normatively recalibrated to respond to fintech abuse without undermining legitimate financial innovation(Marshall, 2019). Through this

approach, the article seeks to contribute a more focused and conceptually grounded criminal law perspective to the evolving discourse on fintech regulation and digital economic crime(Muladi & Priyanto, 2018).

## Methods

This study employs a normative juridical research method, which focuses on the analysis of legal norms, principles, and regulations governing the misuse of financial technology (fintech) in illegal online lending practices. Normative juridical research is designed to examine law as a normative system by exploring statutes, legal doctrines, and court decisions in order to assess their coherence, effectiveness, and consistency in addressing a particular legal problem (Marzuki, P. M, 2021)(Marzuki, 2022; Soekanto & Mamudji, 2019).

The approach adopted in this study consists of three interrelated perspectives: the statutory approach, the conceptual approach, and the case approach. The statutory approach is used to examine relevant laws and regulations, including the Indonesian Criminal Code (KUHP), Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016, Law No. 8 of 1999 on Consumer Protection, and the Financial Services Authority Regulation (POJK) No. 77/POJK.01/2016 on Information Technology-Based Lending Services(OJK, 2024). These legal instruments are analyzed to identify the scope of criminalization, the elements of criminal liability, and the regulatory standards applicable to fintech-based lending activities(Nguyen, 2022).

The conceptual approach is employed to explore legal doctrines and theoretical concepts relating to criminal law, cybercrime, economic crime, and legal policy. This approach enables the researcher to critically assess the adequacy of existing criminal law principles such as legality, culpability, and proportionality—in addressing the unique characteristics of fintech abuse in the digital lending ecosystem(Prasetyo, 2020). In addition, this approach is used to evaluate the alignment between regulatory objectives and criminal law enforcement in protecting consumers and ensuring fairness in digital financial transactions(Prayogo & Suryani, 2021).

Furthermore, a case-based approach is employed to examine a limited number of selected court decisions and documented law enforcement practices related to illegal online lending and fintech-based financial crimes in Indonesia. The cases are selected based on their relevance to core forms of fintech abuse such as unlawful debt collection, data misuse, and cyber-enabled fraud and their significance in illustrating the application of criminal and regulatory norms(Rahardjo, 2022). The analysis focuses on decisions issued within the recent enforcement period following the expansion of fintech regulation, allowing the study to assess how existing legal frameworks are interpreted and applied in practice.The legal materials used in this research consist of primary, secondary, and tertiary legal materials. Primary legal materials include statutes and official regulations related to fintech, criminal law, cyber law, and consumer protection(Santoso, 2020). Secondary legal materials comprise books, journal articles, research reports, and expert opinions that discuss fintech regulation, cybercrime, criminal liability, and legal policy. Tertiary legal materials include legal dictionaries, encyclopedias, and indexing sources that support the interpretation of legal terms and concepts(Rahman, 2023).

All legal materials are analyzed using qualitative normative analysis, which involves systematic interpretation through legal reasoning, legal construction, and legal argumentation. The analysis is conducted through descriptive, analytical, and prescriptive stages(Satgas Waspada Investasi, 2023). The descriptive stage explains the existing regulatory framework governing fintech and illegal online lending. The analytical stage examines the weaknesses and gaps in the current criminal law and regulatory system. Finally, the prescriptive stage formulates policy recommendations aimed at strengthening criminal law enforcement and regulatory integration for combating fintech abuse in i(Sutedi, 2019)llegal online lending practices(Scholten, 2020).

Overall, this study employs a qualitative normative juridical method to analyze the coherence and adequacy of criminal and regulatory frameworks governing fintech abuse in illegal online lending. The analysis is confined to doctrinal and legal-normative evaluation and does not seek to empirically assess enforcement effectiveness, deterrence outcomes, or victim impact (Suryono, 2023). A statutory, conceptual, and case-based approach is applied in an integrated manner. The case analysis examines a limited number of purposively selected court decisions and documented law enforcement practices, chosen for their relevance to core forms of fintech abuse and their illustrative value in demonstrating the application of criminal and cyber law provisions. These cases are not intended to be statistically representative, but to support doctrinal interpretation. The study proceeds through descriptive, analytical, and prescriptive stages, with the prescriptive conclusions explicitly framed as normative legal arguments derived from doctrinal analysis rather than empirically tested policy solutions(World Bank, 2020; Zetzsche, 2017).

## Result and Discussion

### Typology of Fintech Abuse in Illegal Online Lending Practices

The findings of this study indicate, based on regulatory and doctrinal assessment, that illegal online lending in Indonesia constitutes a complex and highly adaptive form of fintech abuse that integrates financial exploitation. Statistical reports issued by the Financial Services Authority (OJK) and the Investment Alert Task Force indicate that tens of thousands of illegal fintech platforms have been blocked between 2019 and 2024, yet new platforms continue to reappear under different digital identities (OJK, 2024; Satgas Waspada Investasi, 2023).

Illegal fintech operators typically exploit digital infrastructure through unregistered mobile applications, overseas cloud servers, encrypted communication systems, and anonymous payment channels. The dominant forms of abuse include excessive and non-transparent interest rates, unauthorized access to borrowers' mobile data, digital harassment, intimidation, identity misuse, and extortion through threats of disseminating personal information to social networks(Prayogo & Suryani, 2021; Zhang, 2021)

From a criminal law perspective, these practices constitute multi-layered cyber-economic crimes, as they simultaneously violate property rights, personal security, privacy, and human dignity. This indicates that illegal online lending extends beyond civil contractual violations and involves patterns of digitally enabled criminal conduct that, from a criminological perspective, may be described as predatory and systematic.(Santoso, 2020; UNODC, 2021).

### Criminalization Framework under Indonesian Law Before and After the 2026 Criminal Code

Prior to the enactment of the new Indonesian Criminal Code, illegal online lending was prosecuted through fragmented criminal provisions, including fraud (Article 378 KUHP), extortion (Article 368 KUHP), threats (Article 369 KUHP), defamation (Articles 310–311 KUHP), and multiple criminal norms under the Law on Electronic Information and Transactions (Law No. 11 of 2008 as amended by Law No. 19

of 2016). Consumer losses were further addressed under the Consumer Protection Law (Law No. 8 of 1999) (Afriana & Lestari, 2021).

However, Law No. 1 of 2023 on the Indonesian Criminal Code, which will enter into force in 2026, introduces a more modern and systematic criminal policy framework. One of its most significant innovations is the formal recognition of corporate criminal liability. Under the new Code, corporations may be held criminally responsible for offenses committed within the scope of their business activities, including economic and digital crimes (Muladi & Priyanto, 2018; PwC Indonesia, 2025).

This reform directly strengthens the legal basis for prosecuting illegal fintech platforms that operate as structured digital enterprises. Under the previous regime, law enforcement authorities often targeted only operational actors such as debt collectors or system administrators, while the main controllers remained beyond effective prosecution. The 2026 Criminal Code narrows this structural gap by recognizing corporate and managerial criminal liability, while leaving unresolved practical challenges related to proof, attribution, and judicial capacity in fintech-related enforcement.

Criminal Liability and the Reconstruction of Mens Rea in Fintech-Based Crimes

One of the most complex issues in the prosecution of illegal fintech lending lies in establishing criminal intent (mens rea) within automated digital systems. Fintech platforms increasingly operate through algorithmic decision-making systems, outsourcing arrangements, and layered digital management structures, which complicate the identification of individual criminal intent. From the perspective of criminal jurisprudence, this condition raises questions of attribution and responsibility similar to those discussed in corporate crime and organizational liability doctrines, where intent is inferred through functional control rather than direct individual action. In parallel, scholarship on artificial intelligence ethics and algorithmic governance highlights the problem of "distributed agency," in which decision-making outcomes result from the interaction of human actors, automated systems, and institutional design rather than from a single intentional subject. These perspectives support the argument that traditional intent-based criminal frameworks face structural limitations when applied to fintech-enabled misconduct. (Arner et al., 2017; UNODC, 2021).

This study finds that under the conventional individual-based liability model, the burden of proof often results in selective enforcement against low-level operators rather than against system controllers. The new Criminal Code provides an opportunity to reconstruct criminal liability by adopting a functional corporate liability model. Under this approach, criminal intent (*mens rea*) may be attributed to a corporation through the actions, decisions, or omissions of its controlling organs or persons acting within the scope of their authority and for the benefit of the corporation. This model departs from strict identification theory by emphasizing functional control and organizational responsibility, while avoiding the evidentiary complexities associated with pure aggregation theory. Thus, the enforcement of criminal law against illegal online lending after 2026 is expected to shift from an individual-perpetrator focus toward a network-based and corporate accountability framework, which is more compatible with the technological reality of digital financial crimes.

Consumer Victimization and Human Rights Violations

Victims of illegal online lending suffer not only economic losses but also severe psychological, social, and reputational harm. Digital harassment, public shaming, mass dissemination of personal data, and continuous intimidation have become systematic debt collection methods used by illegal platforms (Komnas HAM, 2022; Prayogo & Suryani, 2021).

Such practices constitute serious violations of fundamental human rights, including the constitutional rights to personal security, privacy, and protection from intimidation as guaranteed under Article 28G of the 1945 Constitution of the Republic of Indonesia, as well as rights recognized in international human rights instruments such as the International Covenant on Civil and Political Rights, to which Indonesia is a State Party. From a victimological perspective, borrowers occupy a structurally vulnerable position due to information asymmetry, algorithmic opacity, and unequal bargaining power (World Bank, 2020).

The new 2026 Criminal Code strengthens the victim-centered orientation of Indonesian criminal law by emphasizing restitution, compensation, and restorative justice mechanisms. This development creates new opportunities for victims of illegal fintech lending to obtain meaningful redress, although strict differentiation must be maintained between small-scale disputes and organized economic crimes.

Regulatory Dualism and Institutional Fragmentation

Fintech regulation in Indonesia continues to operate under a dualistic governance structure involving the Financial Services Authority (OJK), Bank Indonesia, the Ministry of Communication and Informatics (Kominfo), and criminal law enforcement agencies. This institutional fragmentation often results in delayed enforcement, overlap of authority, loss of digital evidence, and weak coordination (OJK, 2024; Sutedi, 2019).

Illegal operators systematically exploit these regulatory gaps through rapid application migration, mirror-domain creation, and cross-border server relocation. Without integrated supervision and real-time cyber-financial monitoring, criminal enforcement remains reactive rather than preventive.

Transnational Dimension of Illegal Fintech Operations

The study further confirms that a significant portion of illegal online lending platforms operate as part of transnational cyber-financial networks. These platforms frequently employ offshore servers, nominee shareholders, and cross-border financial intermediaries to evade national jurisdiction(UNODC, 2021).

Although international mutual legal assistance mechanisms exist, their procedural rigidity and slow response time are incompatible with the rapid mobility of digital financial crimes. This creates a condition of structural enforcement asymmetry, where domestic victims remain fully exposed while transnational perpetrators remain partially shielded.

Penal Policy Effectiveness under the 2026 Criminal Code

Under the 2026 Criminal Code, the Indonesian penal system undergoes a significant paradigm shift from a retributive model toward a corrective–restorative–rehabilitative framework (Atmasasmita, 2021). Criminal sanctions are no longer limited to imprisonment and fines, but may also include restitution, corporate sanctions, business activity restrictions, rehabilitation measures, and probationary supervision.

This diversification of sanctions increases the capacity of criminal law to address illegal fintech lending in a more comprehensive manner. However, the findings of this study indicate that criminal sanctions alone remain insufficient without complementary regulatory, technological, and institutional reforms. Without effective digital surveillance, asset tracing, and cross-agency coordination, the deterrent effect of criminal law will remain limited.

Restorative Justice and the Limits of Settlement in Fintech Crimes

In response to the limitations of both purely retributive and overly restorative approaches, this study briefly considers alternative sanctioning models that seek to preserve punitive integrity while ensuring meaningful victim restitution. One such option is hybrid sentencing, in which custodial or corporate penalties are combined with legally enforceable restitution orders, thereby maintaining the expressive and deterrent functions of criminal law while directly addressing victim harm. Another possibility lies in suspended or conditional corporate sanctions, whereby fines, license restrictions, or operational prohibitions are deferred on the condition of full restitution compliance, regulatory reform, and demonstrable internal control improvements. From a criminal law policy perspective, these models offer a more balanced response to large-scale fintech abuse by integrating accountability, deterrence, and victim redress without reducing criminal enforcement to purely compensatory mechanisms.

The restorative justice orientation of the 2026 Criminal Code introduces a policy space for victim recovery through restitution and negotiated settlement. While this approach may be appropriate for minor fintech disputes involving unlicensed small-scale lenders, it carries serious risks when applied to organized digital economic crimes.

Normatively, and drawing on criminological theory, an overreliance on restorative mechanisms in large-scale illegal fintech cases may diminish the symbolic and deterrent functions of criminal law. (Atmasasmita, 2021). Therefore, this study argues that restorative justice must be selectively applied, and should never replace strict punitive enforcement against organized fintech crime networks.

Comparative Regulatory Models and International Best Practices

Comparative experience from jurisdictions such as China, Singapore, and the European Union demonstrates the effectiveness of centralized fintech supervision, real-time algorithm auditing, integrated cyber-financial intelligence units, and explicit criminalization of illegal digital lending (Arner et al., 2017; World Bank, 2020).

Indonesia has not yet fully adopted such an integrated supervisory and penal model. The 2026 Criminal Code provides a strong normative foundation, but its success will depend on the alignment of financial regulation, cyber governance, and criminal justice institutions.

Toward an Integrated Criminal Law and Fintech Governance Model

Based on the findings and the 2026 Criminal Code reform, this study proposes an integrated regulatory and penal model consisting of:

1. Explicit criminalization of illegal online lending as a specialized cyber-economic offense;
2. Full implementation of corporate criminal liability for fintech enterprises;
3. Integrated real-time digital supervision involving OJK, Kominfo, and law enforcement agencies;
4. Strengthened cross-border cyber-financial cooperation;
5. Victim-centered digital protection and restitution mechanisms.

Such an integrated model aligns criminal law enforcement with digital economic governance and strengthens legal certainty, justice, and the sustainability of Indonesia's fintech ecosystem. The phenomenon of illegal online lending in Indonesia cannot be adequately explained solely as a violation of financial regulations or as isolated criminal conduct. It represents a structural transformation of economic crime in the digital era, where technology is no longer a neutral instrument but an intrinsic part of the criminal architecture itself. Illegal fintech lending operates through algorithmic systems, data-driven surveillance, psychological coercion, and transnational financial engineering. Therefore, the traditional criminal law paradigm which is predominantly reactive, offender-oriented, and territorially bound—faces serious structural limitations.

The enactment of the 2026 Indonesian Criminal Code marks a progressive normative shift, particularly through the recognition of corporate criminal liability, restorative justice, and diversified sanctions. However, from a critical standpoint, this reform still carries a latent risk of normative lag behind technological acceleration. Digital financial crimes evolve faster than statutory criminal provisions. If the criminal law is not continuously updated through adaptive interpretation, judicial innovation, and regulatory synchronization, it will remain one step behind fintech-based criminality.

The author argues that illegal online lending should no longer be framed merely as a derivative offense under fraud, extortion, or cybercrime provisions. Instead, it must be reconstructed as a distinct category of cyber-economic organized crime, characterized by (1) digital infrastructure dependency, (2) automated victim targeting, (3) data-driven coercion, and (4) cross-border profit circulation. Without such a conceptual reconstruction, criminal law enforcement will continue to suffer from fragmented qualification, evidentiary complexity, and disproportionate sentencing.

Furthermore, the author critically observes that Indonesia's current law enforcement orientation still prioritizes tactical repression rather than structural disruption. The continuous blocking of illegal applications, scattered arrests of field operators, and reactive prosecution of individual offenders have not significantly reduced the market supply of illegal online lending services. This indicates that enforcement has not yet fully targeted the economic command structure of illegal fintech enterprises, including digital financiers, data brokers, system designers, and offshore controllers.

The rapid development of financial technology (fintech) has revolutionized access to financial services by providing speed, flexibility, and inclusivity. Digital lending platforms in particular have expanded rapidly by utilizing mobile applications, big data analytics, and automated credit scoring systems (Arner et al., 2017; Gomber et al., 2018). However, this expansion has also generated significant risks, particularly the emergence of illegal online lending platforms operating without regulatory authorization.

Illegal online lending represents a new form of digital economic crime, characterized by algorithm-based exploitation, excessive interest rates, and abusive debt collection prkaractices (Prayogo & Suryani, 2021; Santoso, 2020). Unlike conventional loan sharking, illegal fintech lending operates through data extraction, cyber intimidation, and mass digital surveillance of borrowers (World Bank, 2020). Borrowers in illegal online lending are structurally vulnerable due to information asymmetry, economic pressure, and algorithmic opacity (Makarim, 2021; World Bank, 2020). Studies show that most victims lack legal literacy and are unaware of the distinction between licensed and illegal platforms at the time of borrowing (Afriana & Lestari, 2021). From a victimological perspective, the harms suffered extend beyond financial loss to include depression, job loss, family conflict, public shaming, and even suicide in extreme cases (Komnas HAM, 2022; Rahman, 2023). This confirms that illegal online lending must be treated as a serious human rights-related economic crime, not merely a contractual irregularity. Before the enactment of the new Indonesian Criminal Code, prosecution relied on fragmented provisions of fraud, extortion, threats, defamation, and cybercrime (Afriana & Lestari, 2021; Prasetyo, 2020). This

fragmented construction weakened deterrence and complicated evidentiary procedures.

Comparative research in China, Singapore, and the European Union demonstrates that specific criminalization of illegal digital lending significantly increases enforcement effectiveness (Arner et al., 2017; Zetzsche, 2017). Indonesia's previous reliance on general offenses created regulatory ambiguity and enforcement inconsistency (Sutedi, 2019).

One of the most critical weaknesses in fintech crime enforcement lies in the absence of effective corporate criminal liability models prior to the 2026 Criminal Code (Muladi & Priyanto, 2018)(Muladi & Priyanto, 2018). Illegal fintech platforms operate as structured digital corporations with layered control systems, nominee owners, and offshore financial channels (UNODC, 2021)(UNODC, 2021). Without recognizing corporate responsibility, law enforcement tends to target only low-level operators such as debt collectors or marketing agents, while the true controllers remain legally insulated (Atmasasmita, 2021; PwC Indonesia, 2025). Indonesia's fintech governance structure involves multiple authorities, including OJK, Bank Indonesia, Kominfo, and law enforcement agencies. Although this multi-agency model is intended for checks and balances, in practice it produces institutional fragmentation and slow enforcement responses (OJK, 2024; Sutedi, 2019).

Illegal platforms exploit this fragmentation by migrating servers, replicating applications, and shifting payment gateways across jurisdictions (Satgas Waspada Investasi, 2023). Similar patterns have also been documented in Vietnam and the Philippines (Cruz, 2021; Nguyen, 2022)(Nguyen, 2022; Cruz, 2021).

Illegal online lending increasingly operates through transnational cyber-crime networks involving offshore servers, cryptocurrency laundering, and nominee ownership structures(Europol, 2022; UNODC, 2021) (UNODC, 2021; Europol, 2022). This creates a structural mismatch between national jurisdiction and globalized digital crime.

Mutual legal assistance treaties remain slow and bureaucratic when applied to real-time cyber-financial crimes (Scholten, 2020)(Scholten, 2020). As a result, domestic victims remain fully exposed while transnational offenders enjoy partial protection through jurisdictional complexity.

The shift toward restorative justice in modern criminal law has opened opportunities for victim recovery through restitution and compensation mechanisms (Atmasasmita, 2021; Marshall, 2019). However, scholars warn that restorative justice must not be applied indiscriminately to organized economic crimes (Braithwaite, 2018)(Braithwaite, 2018). In fintech crimes, excessive reliance on settlement risks transforming systematic digital exploitation into a negotiable offense (Rahardjo, 2022). Victims often accept settlements due to desperation rather than genuine justice. China criminalized illegal peer-to-peer lending with explicit penal sanctions, including asset confiscation and platform shutdowns, which significantly reduced illegal fintech operations after 2020 (Zhang, 2021). Singapore applies a strict licensing and criminal enforcement regime, enabling rapid prosecution of illegal digital lenders (Low & Teo, 2020)(Low & Teo, 2020). The European Union integrates consumer protection, data protection (GDPR), financial supervision, and criminal sanctions into a single digital governance architecture (Gomber, 2018; Zetzsche, 2017). The literature consistently shows that illegal online lending cannot be effectively controlled through fragmented criminal provisions and reactive enforcement (Prayogo & Suryani, 2021) Instead, successful jurisdictions adopt:

1. Explicit criminalization of illegal fintech lending,
2. Strong corporate liability regimes,
3. Real-time digital supervision,
4. Integrated victim restitution systems, and
5. Transnational cyber-financial cooperation (UNODC, 2021; World Bank, 2020).

Thus, the global literature supports the argument that fintech abuse represents a new structural form of digital economic crime requiring integrated criminal–regulatory governance.

Scholars classify fintech abuse in illegal lending into several dominant forms:

(1) unauthorized data harvesting
(2) excessive and non-transparent interest imposition,
(3) digital harassment and intimidation, and
(4) cross-platform cyber defamation (Lubis, 2020; Rahardjo, 2022).

Empirical studies in Southeast Asia show that illegal fintech platforms systematically exploit application permissions to access contacts, photographs, location data, and communication history, which are later used as tools of coercion (Suryono, 2023; UNODC, 2021). This transforms borrowers into digitally controlled debt subjects, where financial dependency is maintained through psychological pressure rather than contract enforcement.

From a policy perspective, the author contends that the effectiveness of the 2026 Criminal Code in addressing illegal fintech lending will depend on three key conditions. First, the integration of criminal law with real-time digital financial supervision must be institutionalized through permanent cyber-financial task forces combining OJK, Kominfo, police cyber units, prosecutors, and financial intelligence agencies. Second, asset tracing and confiscation mechanisms must be technologically strengthened to follow the digital money trail, including the use of blockchain forensics and AI-based transaction monitoring. Without dismantling the economic incentives of illegal fintech operators, criminal sanctions will remain symbolically strong but materially weak.

Third, the author emphasizes that victim protection must be repositioned as the core objective of criminal fintech governance. The current punitive orientation still prioritizes the interests of public order rather than the recovery of victims' dignity, privacy, and economic survival. Under the new Criminal Code, restitution and rehabilitation must not be treated as complementary measures but as central indicators of enforcement success. The absence of effective restitution will perpetuate social distrust toward both digital finance and state law enforcement.

The author also critically reflects on the ambivalence of restorative justice in fintech-related crimes. While restorative mechanisms offer humane and participatory solutions for minor disputes, their indiscriminate application to organized illegal fintech operations risks transforming economic crime into negotiable wrongdoing. From a criminological standpoint, this would normalize systemic digital exploitation and weaken the moral authority of criminal law. Therefore, restorative justice in illegal fintech lending must be selectively limited to cases without organized networks, data exploitation, or mass victimization.

Indonesia currently stands at a strategic legal crossroads. One trajectory continues the existing pattern of fragmented regulation, reactive enforcement, and largely symbolic criminalization. An alternative and more realistic path lies in the gradual development of integrated digital criminal governance through institutionally feasible reforms, such as clearer delineation of authority between financial regulators and criminal justice agencies, formalized inter-agency coordination mechanisms, and the incremental use of joint task forces for fintech-related investigations. Within existing political and administrative constraints, this approach does not require the creation of new institutions, but rather the strengthening of coordination frameworks, data-sharing protocols, and cross-border cooperation instruments already recognized in

Indonesian law. The 2026 Criminal Code provides a strong normative gateway toward this second path, but without intellectual courage in judicial interpretation, institutional reform, and political commitment, it risks becoming a progressive legal text with minimal transformative impact.

In conclusion, from the author's viewpoint, the regulation of fintech abuse in illegal online lending must move beyond the logic of prohibition and punishment toward a comprehensive architecture of digital economic justice, where criminal law functions not only as a tool of repression but as an instrument of structural correction, victim restoration, and ethical governance of the digital economy.

Rather than merely reaffirming widely recognized characteristics of illegal online lending, this study advances a more nuanced doctrinal analysis by examining how existing criminal law concepts are structurally strained when applied to fintech-enabled misconduct. The discussion demonstrates that regulatory fragmentation is not only an institutional weakness but also a doctrinal problem, reflected in the inconsistent construction of criminal liability, evidentiary thresholds, and attribution of intent across regulatory and penal regimes. While the recognition of corporate criminal liability under the 2026 Criminal Code marks a significant normative development, this study critically highlights unresolved challenges related to proof of corporate intent, functional attribution, and judicial capacity in complex digital finance cases. Similarly, the classification of illegal online lending as implicating human rights is not treated as a rhetorical label, but as a legal claim that requires meeting constitutional and international law thresholds concerning privacy, security, and protection from coercion. Finally, the critique of restorative justice is framed not as an empirical assessment of outcomes, but as a normative legal argument grounded in criminal law theory, emphasizing the limits of restorative mechanisms in addressing systemic, profit-driven digital crimes that implicate public legal order. Through this approach, the analysis seeks to move beyond descriptive confirmation and contribute a more critical and doctrinally grounded perspective to the legal governance of fintech abuse.

## Conclusion

This study concludes that the rapid expansion of financial technology has fundamentally transformed the structure of economic crime, particularly through the proliferation of illegal online lending practices in Indonesia. Illegal fintech lending has evolved into a complex form of cyber-economic organized crime, characterized by algorithmic exploitation, data-driven coercion, digital intimidation, and transnational financial operations. These characteristics demonstrate that illegal online lending can no longer be treated merely as a derivative offense of fraud or cybercrime, but must be understood as a distinct and systemic digital crime phenomenon.

The findings also confirm that, prior to the enactment of the new Indonesian Criminal Code, law enforcement relied on fragmented criminal provisions scattered across the Criminal Code, the Electronic Information and Transactions Law, and sectoral regulations. This fragmentation resulted in weak deterrence, selective enforcement, and limited recovery of victims' rights. The enactment of Law No. 1 of 2023 on the Indonesian Criminal Code, which will come into force in 2026, introduces a significant paradigm shift through the recognition of corporate criminal liability, diversification of criminal sanctions, and the strengthening of restorative justice and victim restitution mechanisms. Normatively, this reform provides a much stronger legal foundation for prosecuting illegal fintech enterprises as structured corporate offenders rather than merely targeting individual operators.

However, this study also concludes that normative reform alone is insufficient to effectively combat illegal online lending. Without structural integration between criminal law enforcement, real-time digital financial supervision, cyber surveillance, and cross-border cooperation, the 2026 Criminal Code risks functioning only as a progressive legal text with limited practical impact. The transnational nature of illegal fintech operations, the rapid mobility of digital platforms, and the sophistication of financial evasion techniques demand a comprehensive governance model that goes beyond conventional law enforcement strategies.

From a victim-centered perspective, this study affirms that the harms caused by illegal online lending extend far beyond economic loss, encompassing severe violations of privacy, human dignity, psychological security, and social reputation. Therefore, the success of criminal law enforcement in this field should not be measured solely by conviction rates, but primarily by the effectiveness of victim protection, restitution, and rehabilitation. Restorative justice, while normatively strengthened under the new Criminal Code, must be applied selectively and should not replace punitive enforcement against organized and systematic fintech crimes.

In conclusion, this study asserts that the future regulation of fintech abuse in illegal online lending in Indonesia must be directed toward an integrated model of digital criminal governance, which combines: (1) explicit criminalization of illegal fintech lending as a cyber-economic offense; (2) full implementation of corporate criminal liability; (3) technologically reinforced asset tracing and confiscation; (4) permanent inter-agency cyber-financial coordination; and (5) strong victim-oriented restitution mechanisms. An integrated regulatory and criminal law approach has the potential to strengthen the role of criminal law beyond repression, including its contribution to consumer protection and ethical governance in the digital economy.

In conclusion, this study advances a normative and doctrinal argument that illegal online lending in Indonesia may be analytically understood as a form of cyber-enabled economic crime that exhibits certain organized characteristics, rather than asserting its reconstruction as a distinct and inevitable legal category. The proposed model of integrated digital criminal governance is presented as one possible normative framework among several regulatory approaches, and its feasibility remains conditioned by institutional capacity, political commitment, and resource constraints within Indonesia's legal system. Consistent with the limits of normative juridical research, this study does not empirically assess enforcement effectiveness, deterrent impact, or victim recovery outcomes, but instead focuses on clarifying doctrinal tensions and regulatory gaps. Accordingly, future research is needed to complement this analysis through empirical studies on enforcement practices, judicial interpretation of corporate liability under the 2026 Criminal Code, and the practical operation of hybrid sanctioning models in fintech-related cases.

## Author contributions

Joice Soraya conceptualized the study, developed the theoretical framework, conducted the primary legal and policy analysis, and drafted the main sections of the manuscript, including the introduction, results, and discussion. Joice Soraya also led the interpretation of findings and formulated the core policy recommendations.

Vivi Sylvia Purborini contributed to the research methodology design, data and legal material collection, and analysis of statutory regulations and comparative legal sources. Vivi Sylvia Purborini also participated in manuscript editing, critical revision for intellectual content, and final approval of the version to be published. Both authors have read

and agreed to the published version of the manuscript..

## Acknowledgements

The authors would like to express their sincere gratitude to all parties who have contributed to the completion of this research. Special appreciation is extended to colleagues and reviewers who provided valuable insights and constructive feedback that helped improve the quality of this manuscript. The authors also gratefully acknowledge institutional support that facilitated the research process.

## Conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this article. The research was conducted independently, without any financial, institutional, or personal relationships that could inappropriately influence the content, analysis, or interpretation of the results.

## References

Afriana, A., & Lestari, R. (2021). Consumer protection in fintech lending. *Yuridika*, *36*(2), 345–362.
Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *FinTech and financial regulation*. *Northwestern JILB*. *37*(3), 371–413.
Atmasasmita, R. (2021). Restorative justice reform. *Jurnal Hukum IUS QUIA IUSTUM*, *28*(1), 1–21.
Braithwaite, J. (2018). Restorative justice and responsive regulation. *Regulation & Governance*, *12*(3), 371–385.
Cruz, R. (2021). Digital lending risks in Southeast Asia. *Asian Economic Journal*, *35*(4), 401–420.
Europol. (2022). *Internet organized crime threat assessment*.
Gomber, P. (2018). Fintech revolution. *Journal of Management Information Systems*, *35*(1), 220-265.
Gunningham, N. (2019). Smart regulation theory. *Law & Policy*, *41*(1).
Komnas HAM. (2022). *Human rights and online lending*.
Low, K., & Teo, E. (2020). Regulating fintech in Singapore. *Singapore Journal of Legal Studies*, *2020*(1), 34–57.
Lubis, T. (2020). Digital consumer exploitation. *Jurnal Hukum & Teknologi*, *1*(2).
Makarim, E. (2021). Cyber law and fintech risks. *Jurnal Legislasi Indonesia*, *18*(3).
Marshall, T. (2019). Restorative justice theory. *Oxford Journal of Criminology*, *59*(4).
Marzuki, P. M. (2021). *Penelitian Hukum (Edisi Revisi)*. Kencana.
Muladi, & Priyanto. (2018). Corporate criminal liability. *Jurnal Hukum Pidana*, *14*(2).
Nguyen, T. (2022). Illegal fintech in Vietnam. *Asian Journal of Law and Society*, *9*(1).
OJK. (2024). *Indonesian fintech lending statistics 2024*. Financial Services Authority.
Prasetyo, T. (2020). Cybercrime enforcement. *Jurnal Hukum & Peradilan*, *9*(1).
Prayogo, S., & Suryani, T. (2021). Online lending victims. *Journal of Financial Crime*, *28*(3).
PwC Indonesia. (2025). *New Criminal Code*.
Rahardjo, S. (2022). Cyber victimology. *Jurnal Hukum Progresif*, *10*(2).
Rahman, F. (2023). Psychological impacts of fintech debt. *Journal of Social Psychology*, *41*(2).
Santoso, T. (2020). Cyber economic crime. *Indonesia Law Review*, *10*(2).
Satgas Waspada Investasi. (2023). *National illegal fintech report*.
Scholten, K. (2020). Cross-border cyber enforcement. *European Journal of Crime Policy*, *26*(4).
Suryono, R. (2023). Data exploitation in fintech. *Information Systems Frontiers*, *25*(2).
Sutedi, A. (2019). Financial regulation law. *Jurnal Regulasi Keuangan*, *5*(1).
UNODC. (2021). *Cybercrime and fintech*.
World Bank. (2020). *Consumer protection and fintech*.
Zetzsche, D. (2017). Fintech regulation in the EU. *Journal of Financial Regulation*, *3*(1).
Zhang, W. (2021). China's P2P crackdown. *China Law Review*, *19*(3).