Indonesian Journal of Law and Justice Volume: 3, Number 3, 2026, *Page*: 1-11

Juridical Construction of Causality in Cyber-Threatening Crimes Resulting in Victim Death: A Critical Study of Fintech Peer-to-Peer Lending Debt Collection

Adrianus Herman Henok

Universitas Kristen Indonesia

DOI: https://doi.org/10.xxxxx/xxxxx
*Correspondence: Adrianus Herman Henok
Email: adrianus.henok@uki.ac.id

Received: 24-12-2025
Accepted: 24-01-2026
Published: 24-02-2026

Abstract: This research examines the complexity of proving the causal link in cyber-threatening crimes resulting in victim death, with a specific focus on debt collection practices by Fintech Peer-to-Peer (P2P) Lending providers. The central issue in this discourse is the difficulty of legally linking psychological pressure exerted through digital media to physical outcomes such as death (often in the form of suicide). The research method employed is normative legal research with statutory and conceptual approaches. The results indicate that the construction of causality in conventional criminal law needs to be reassessed through the theory of adequacy to address the realities of cybercrime. Aggressive collection practices that violate legal norms often serve as a conditio sine qua non for the loss of the victim's life. This article concludes that there is an urgent need for policymakers to clarify the criteria for corporate and personal criminal liability within the fintech ecosystem to counter the fatal impacts of cyber-harassment.

Keywords: Causality, Cyber-Threatening, Fintech, P2P Lending, Criminal Liability

Introduction

Addressing the "paralysis" of criminal law in linking digital threats to physical death, this research argues that the approach to causation must no longer be confined to physical contact alone (Bagaskara, 2025). In cases of fintech debt collection, we must employ the Adequacy Theory (Von Kries). (Marble & Yanakiev, 2020). Juridically, "threatening words on a phone screen" are not merely text; they are instruments of assault against an individual's honor and psychological state. When a collector engages in doxing (disseminating personal data) to all of the victim's contacts, the perpetrator has consciously created a condition of extreme social pressure, or "social death". From a legal perspective, if the collection methods are objectively deemedaccording to general experience capable of causing severe depression, then the causal link between the cyber threat and the victim's death is established, even if the victim committed suicide of their own volition (Branzoli & Supino, 2020).

Building upon this repositioning of causation, the argument can be further tested using the conditio sine qua non parameter to observe the direct link between the perpetrator's actions and the victim's fatal decision (Budisusanto, 2025). Utilizing the "but-for" test, the reality becomes clear: had there been no cyber threats and massive

dissemination of private data by the collector, the victim would not have experienced the psychological pressure that led to the decision to end their life. The persistent ambiguity in causal construction occurs because law enforcement often severs the chain of causation at the moment the victim decides to commit suicide. (Muchamad, 2023). However, in cybercrimes, the victim's action is a direct response to the "digital terror" orchestrated by the perpetrator. Consequently, perpetrators should not merely be charged under Article 27B of the ITE Law regarding threats, but must be brought into the construction of aggravated offenses (gequalificeerde delicten), analogous to maltreatment resulting in death (Daeng & Levin et al, 2023).

This construction of aggravated offenses ultimately leads to a fundamental conclusion: legal liability must no longer stop at the administrative level or with individual collectors, but must reach the realm of substantive corporate criminal liability (Daud & Jaya, 2022). To date, many P2P Lending providers have only faced administrative sanctions from the OJK or minor ITE charges, under the assumption that the collectors were merely "rogue elements" or third parties (Manurung, 2025). However, through a robust construction of causation, fintech companies can be held criminally liable if they are proven to have a collection system that permits or encourages cyber-intimidation. (Najaf, Subramaniam & Atayah, 2022). The bridge between the "phone screen" and "physical death" is found in the concept of Foreseeability (Suwondo, 2021). A collector who intensively terrors a victim ought to foresee that their actions would permanently damage the victim's mental health. Thus, sanctions are no longer sufficient if limited to administrative fines; they must enter the realm of substantive criminal law regarding the loss of human life. As a synthesis of the aforementioned arguments, it is evident that the juridical courage to link "threats on a screen" with the "loss of life" is the primary key to dismantling the impunity previously enjoyed by predatory fintech providers (Fitri, 2024).

Methodology

This study is conducted using normative legal research, which treats law as a cohesive system of norms. (Johan, S. 2022) The primary approach employed to dissect the issue is the statute approach, aimed at examining the synchronization of regulations within the Indonesian Criminal Code (KUHP), Law No. 1 of 2024 (the Second Amendment to the ITE Law), and sectoral regulations under OJK Regulation (POJK) No. 22 of 2023. (Rusadi & Benuf, 2020). (Rusadi & Benuf, 2020) To deepen the analysis of causation doctrine, the researcher also adopts a conceptual approach, referencing both classical and contemporary criminal law doctrines (Williams, 2021). This is further reinforced by a case approach toward the phenomenon of aggressive fintech debt collection that has resulted in fatalities in Indonesia (Khalbi, Maulani & Monica, 2025).

All data utilized are sourced from primary legal materials, consisting of statutory regulations, as well as secondary legal materials, which include legal literature, academic journals, and relevant prior research (Prawira, 2023). Data collection was performed through library research, subsequently analyzed qualitatively using deductive logic. Through this analytical framework, the researcher connects the general principles of causation with the specific facts of cyber-threats to produce a comprehensive juridical

construction regarding criminal liability within the digital financial ecosystem (Kritzinger, 2021).

This research employs a normative legal method, utilizing a statute approach to synchronize Indonesian regulations and a conceptual approach to reconstruct criminal law doctrines. The following steps establish the juridical construction of causality :

1. Identifying Juridical Paralysis

The first step involves diagnosing the "legal paralysis" in current law enforcement regarding cyber-threats. Traditional application of the Conditio Sine Qua Non theory often absolves perpetrators because a victim's suicide is viewed as an intervening act of free will that severs the causal chain.

2. Transitioning to Psycho-Normative Causality

The analysis shifts from a physical-mechanistic view to a psycho-normative approach using Von Kries' Adequacy Theory. Under this doctrine, an act is a legal cause if it objectively possesses a general tendency to produce the fatal result based on human experience. Persistent cyber-intimidation and doxing are identified as adequate causes for extreme psychological pressure.

3. Reclassifying Offense Qualifications

The study reconstructs "threats on a screen" as aggravated offenses (gequalificeerde delicten). Rather than treating these cases as mere administrative violations or simple threats under Article 27B of the ITE Law, they are positioned as "disguised material offenses" where the death is a foreseeable consequence of the digital assault.

4. Expanding the Scope of Evidence

To bridge the gap between digital actions and physical death, the doctrinal analysis integrates digital evidence with forensic psychology. Digital footprints—such as doxing narratives and abnormal call frequencies—are classified as instruments of crime (instrumentum delicti) with destructive power equivalent to physical weapons.

5. Attributing Liability through Corporate Fault

The final step addresses accountability by applying the doctrines of Vicarious Liability and Corporate Fault. If a fintech provider designs a system or sets targets that encourage intimidatory collection, the corporation possesses an organizational mens rea (guilty mind) and must be held criminally liable for the fatal outcomes.

In analyzing this juridical construction of causality, the researcher applies three primary interpretative methods to address normative gaps and legal ambiguities :

- Systematic Interpretation links various regulations cohesively by aligning Article 27B of the ITE Law regarding digital threats with National Criminal Code (KUHP) offenses related to the loss of life. Through this method, violations of debt collection ethics in OJK Regulation (POJK) No. 22 of 2023 are no longer viewed as mere administrative breaches but as the fundamental causa triggering substantive criminal liability.

- Teleological Interpretation is utilized to explore the purpose of the law in providing genuine protection for consumers within the digital ecosystem against the phenomenon of "social death" resulting from doxing. This method directs the law to evolve from a physical-mechanistic approach toward a psycho-normative approach, ensuring that justice prevails amidst the reality of digital terror that empirically triggers fatal impulses in victims.
- Comparative Interpretation is conducted by dissecting the doctrinal differences between the rigid Conditio Sine Qua Non theory and Von Kries' Adequacy Theory to find the most relevant causality parameters for cybercrimes. Furthermore, this method compares individual liability with the doctrines of Vicarious Liability and Corporate Fault to prove the existence of an organizational mens rea in fintech corporations that facilitate intimidatory collection systems.

The argument construction in this study follows a deductive logical flow that connects abstract legal theories with the empirical reality of cybercrimes. The logical stages are as follows :

1. Major Premise: Reconstruction of Causality Doctrine
   - Paradigm Shift: The argument begins by asserting that the doctrine of causation must shift from a physical-mechanistic approach to a psycho-normative approach.
   - Adoption of Adequacy Theory: Utilizing Von Kries' Adequacy Theory, an act is legally considered a cause if it objectively possesses a general tendency to produce a fatal result according to reasonable human experience.
   - Foreseeability: A collector who intensively terrors a victim ought to foresee that their actions would permanently damage the victim's mental health or lead to a fatal outcome.
2. Minor Premise: Empirical Reality of Digital Terror
   - Instruments of Crime (Instrumentum Delicti): Threatening words on a phone screen are not merely text but are instruments of assault against an individual's honor and psychological state.
   - The "Social Death" Phenomenon: Doxing and the massive dissemination of private data create a condition of extreme social pressure that empirically triggers severe depression and fatal impulses.
   - Factual Causality: Based on the conditio sine qua non parameter, had there been no cyber-threats and dissemination of private data, the victim would not have experienced the psychological pressure leading to the decision to end their life.
3. Synthesis: Offense Qualification and Liability
   - Aggravated Offenses (Gequalificeerde Delicten): Cyber-threatening resulting in death must be qualified as an aggravated offense, analogous to physical maltreatment resulting in death, rather than a minor ITE charge.
   - Corporate Criminal Liability: Legal liability must extend beyond individual collectors to fintech corporations through the doctrines of Vicarious Liability and Corporate Fault if the company permits or encourages intimidatory systems.
4. Juridical Conclusion: Regulatory Harmonization and Justice

- Evidence Integration: Proving psychological causality requires integrating digital evidence with forensic psychological testimony through a "psychological autopsy" approach.
- Ultimate Objective: The juridical courage to link "threats on a screen" with the "loss of life" is the primary key to dismantling impunity for predatory fintech providers and ensuring justice in the digital economy.

Result and Discussion

Causality Theory Analysis in Cyberspace: Shifting from Physical to Psycho-Normative

The research results indicate that the legal paralysis in prosecuting cyber-threatening perpetrators stems from an overly rigid application of causality theory. In conventional criminal law, prosecutors often rely on the Conditio Sine Qua Non theory, where every factor is deemed a cause. However, in fintech debt collection cases leading to suicide, this theory frequently absolves the perpetrator because the victim's conscious act of ending their life is viewed as an intervening cause that breaks the causal chain. Therefore, this study proposes a reconstruction through Von Kries' Adequacy Theory. Based on this theory, an act is considered a cause if it objectively possesses a general tendency to produce such a result. In the context of fintech collection, persistent intimidation, doxing (disseminating personal data to relatives), and the digital degradation of dignity have empirically proven capable of creating extreme psychological pressure. Juridically, such cyber-threats must be viewed as an adequate cause for the victim's fatal decision.

Critical Study of P2P Lending Debt Collection and Offense Qualification

(Laia, 2025). Debt collection practices by rogue elements or third-party agents often exceed the boundaries set by the ITE Law and OJK Regulation No. 22 of 2023. The research finds a legal loophole where perpetrators are merely charged under Article 27B paragraph (1) of Law No. 1 of 2024 concerning threats. Yet, considering the resulting impact (death), these acts should be classified as offenses aggravated by their results (gequalificeerde delicten). The appropriate juridical construction is to position cyber-threats as "disguised material offenses." The victim's death is not a coincidence but a foreseeable consequence when the perpetrator launches a massive psychological assault. Law enforcement must begin utilizing psychological autopsy approaches to prove that without the digital pressure from the fintech party, the victim would have had no motive for such a fatal act. Thus, criminal sanctions should no longer be limited to fines or short-term imprisonment but should be equated with crimes against human life **(**Maknun, 2024).

Corporate Criminal Liability and Vicarious Liability

The discussion further addresses accountability. Often, fintech companies hide behind the status of "rogue" collectors or third-party agents. However, through a reconstructed doctrine of causality, corporations can be held liable via Vicarious Liability and Corporate Fault doctrines. If a company provides the system or permits threatening collection methods to operate for the sake of meeting collection targets, the corporation is

legally deemed to possess organizational mens rea (guilty mind). Juridical causality links repressive corporate policies to the field actions of collectors, which ultimately results in the victim's death. This demands law enforcement that targets not only the individual executors but also the business entities that facilitate such practices.

Transformation of Digital Evidence in Proving Psychological Causality

A crucial challenge in implementing this juridical construction lies in the aspect of proof (bewijslevering). In conventional criminal procedure, evidence of death is usually based on a physical visum et repertum. However, in deaths resulting from cyber-threats, an expansion of the meaning of evidence is required by integrating digital evidence with forensic psychological testimony. Digital footprintssuch as recordings of intimidatory messages, abnormal call frequencies, and narratives of public shamingconstitute material evidence showing an assault on the victim's mental state. Through a scientific crime investigation approach, the causal link can be proven by demonstrating the escalation of the victim's psychological distress recorded in their digital behavior shortly before death. Law enforcement must no longer view digital evidence partially as a communication tool, but as an instrument of crime (instrumentum delicti) with destructive power equivalent to physical weapons.

The Urgency of Regulatory Harmonization: ITE Law, Criminal Code, and OJK Regulations

The analysis reveals regulatory overlaps and gaps often exploited by P2P Lending providers. Although OJK Regulation No. 22 of 2023 strictly prohibits collection involving threats and intimidation, the sanctions remain predominantly administrative. Conversely, the ITE Law focuses on information transmission but does not yet specifically address cyber-delicts causing fatalities. Consequently, this juridical construction demands penal policy harmonization. Law enforcement must not stop at the revocation of business licenses by the OJK but must proceed to substantive criminal law by linking the violation of collection procedures as the primary cause (causa) of the threat to the consumer's life. This harmonization is essential to prevent a disconnection between consumer protection in the financial services sector and the human right to life in cyberspace.

Fintech Debt Collection Violation Statistics

Based on consumer protection data trends in the financial services sector, there has been a significant increase in categories involving unethical debt collection behavior.

Table 1. Categories involving unethical debt collection behavior

Violation Category	Form of Action	Psychological/Physical Impact
Cyber-Harassment	Threats of violence, insults, and intimidation via instant messaging (WhatsApp/SMS).	Trauma, excessive anxiety, and depression.
Doxing	Dissemination of personal data or photos to all of the debtor's phone contacts.	Social Death (social isolation), job loss, and loss of dignity.

Physical Intimidation	Threats to visit the debtor's residence or workplace publicly.	Extreme fear triggering fatal impulses (suicide).

Regulatory Framework (Juridical Data)

The following is a comparison of existing sanctions, which serves to critique the current "legal paralysis" in addressing these cases:

Table 2. Serves to critique the current "legal paralysis" in addressing these cases

Regulation	Violation Focus	Primary Sanction	Legal Loopholes
UU ITE (Art. 27B)	Transmission of threats/extortion	Imprisonment / Fines	Does not yet cover fatalities as a direct consequence.
POJK 22/2023	Debt collection ethics & data protection	Administrative (Warnings / Revocation of License)	Does not address criminal liability regarding loss of life.
National Criminal Code (KUHP)	Crimes against life/physical integrity	Imprisonment	Difficulty in proving cyber-physical causality without theoretical reconstruction.

Discussion

This study reveals that law enforcement regarding deaths resulting from fintech debt collection in Indonesia is currently in a state of "juridical paralysis". These findings hold broad significance, both theoretically within the doctrine of criminal law and practically for digital consumer protection policies.

Transcending the Limits of Physical-Mechanistic Causation

The primary significance of this study is the urgent need to reposition the doctrine of causation. Juridical ambiguity persists because prosecutors and judges often remain tethered to a rigid application of the Conditio Sine Qua Non theory. In the traditional view, a victim's decision to end their life is regarded as an intervening act of free will that severs the causal chain from the perpetrator. However, this research demonstrates that in the cyber ecosystem, the victim's action is not an isolated event but a direct response to the "digital terror" orchestrated by the collector. By employing Von Kries' Adequacy Theory, this study offers a new interpretation: threatening words on a phone screen must be viewed as instruments of assault against honor and psychological well-being. Objectively, practices such as doxing and continuous intimidation are adequate causes that are foreseeable to result in severe depression and, ultimately, fatality.

Validation of Digital Instruments and "Social Death"

This study confirms the proposition that cyber-attacks can produce tangible physical outcomes through extreme psychological pressure. The phenomenon of social deathresulting from the dissemination of private data to a debtor's entire contact listis a form of massive destruction of human dignity. Data trends indicate that cyber-harassment and doxing empirically trigger trauma and excessive anxiety. Consequently, digital evidence such as recorded intimidatory messages must not be viewed merely as

communication tools but as instrumentum delicti (instruments of crime) with destructive power equivalent to physical weapons.

Practical Consequences for Criminal Liability

Practically, these findings demand a shift in the qualification of offenses. Law enforcement should no longer rely solely on Article 27B of the ITE Law, which carries relatively light sanctions. The more appropriate juridical construction is to classify these acts as aggravated offenses (gequalificeerde delicten) due to the fatal consequences. Furthermore, this discussion emphasizes the doctrines of Vicarious Liability and Corporate Fault. Fintech companies often attempt to evade responsibility by blaming "rogue" agents or third parties. However, if a corporation provides the system or sets targets that indirectly encourage intimidatory practices, the entity possesses an organizational mens rea and must be held liable for substantive criminal acts, moving beyond mere administrative fines from the OJK.

The Urgency of Justice in the Digital Era

Ultimately, this issue is crucial as it concerns the protection of the right to life within cyberspace. Failing to link "threats on a screen" to the "loss of life" perpetuates impunity for predatory fintech providers. Juridical courage and the harmonization of penal policy are required to ensure that sanctions address the loss of human life, allowing the law to retain its essence of justice in the digital economy era.

Comparative Doctrinal Analysis

Traditional criminal law widely applies the Conditio Sine Qua Non theory. This theory treats all contributing factors equally. It fails to address digital ecosystems effectively because courts view a victim's suicide as an independent act. Von Kries' Adequacy Theory provides a more precise legal framework. It measures the objective tendency of an act to cause a specific result. The Conditio Sine Qua Non theory relies on rigid physical links. Conversely, the Adequacy Theory successfully evaluates the severe psychological impacts of persistent cyber-intimidation. This doctrinal comparison validates the urgent need to shift from physical-mechanistic causality to psycho-normative causality.

Policy Implications

Policymakers must immediately revise existing digital consumer protection frameworks. Currently, the Financial Services Authority (OJK) relies predominantly on administrative sanctions for unethical debt collection. The government must explicitly criminalize lethal debt collection practices. Legislators should harmonize the Information and Electronic Transactions (ITE) Law with the National Criminal Code (KUHP). This regulatory harmonization ensures prosecutors can charge fintech companies under the Corporate Fault doctrine. Furthermore, law enforcement agencies must legally recognize digital footprints as direct instruments of crime rather than mere communication tools.

Research Limitations

This study primarily utilizes normative legal research. It relies heavily on statutory frameworks and conceptual approaches to build the causality argument. Consequently, the research lacks extensive quantitative data regarding victim psychology. It does not comprehensively analyze court rulings because prosecutors rarely bring these specific aggravated charges to trial. Additionally, the scope focuses strictly on the Indonesian legal and regulatory context, limiting its direct applicability to foreign jurisdictions.

Future Research Directions

Future researchers should conduct empirical socio-legal studies to validate these findings. Scholars need to analyze the exact psychological mechanisms linking cyber-threats to suicide using primary clinical data. Researchers must also explore international comparative law to evaluate how other jurisdictions handle fintech corporate criminal liability. Subsequent studies should examine the role of artificial intelligence in automating debt collection intimidation and its implications for legal accountability.

Conclusion

(Stern, Makinen & Qian, 2017). Based on the analysis and discussion presented above, this research concludes two fundamental points. First, the legal paralysis in linking cyber-threats to a victim's death can be overcome by reconstructing the doctrine of causation, shifting from a physical-mechanistic approach to a psycho-normative approach. By employing the Adequate Theory, fintech debt collection practices that are intimidating and dignity-destroying (such as doxing) must be classified as an adequate cause for a victim's fatal decision; this is because the resulting psychological impact is objectively foreseeable to lead to fatality (Sulastri & Janssen, 2023).

(Sunardi & Purwana, 2022). Second, the juridical construction of criminal liability must not be confined to administrative sanctions or minor threat offenses under the ITE Law. Law enforcement needs to apply the qualification of aggravated offenses (gequalificeerde delicten) and extend liability to the corporate level through the doctrine of Vicarious Liability. This is crucial to ensure fintech companies are held accountable for the debt collection ecosystems they create. Without the juridical courage to bridge the gap between "threats on a screen" and the "loss of life," law enforcement in the digital economy era will continue to lose its essence of justice (Suryono, Budi & Purwandari, 2021).

References

Bagaskara, G. B. A. (2025). Tindak Pidana Pengancaman Melalui Media Sosial: Tinjauan Hukum Pidana Terhadap Penanganan Oleh Penyidik Polres Tomohon. Menulis: Jurnal Penelitian Nusantara, 1(10), 297-308.

Branzoli, N., & Supino, I. (2020). Fintech credit: A critical review of empirical research literature. *Bank of Italy Occasional Paper*, (549).

Budisusanto, E. (2025). Rekonstruksi Regulasi Peran Amicus Curiae Dalam Pembuktian Pidana Fintech Ilegal Yang Berbasis Keadilan Pancasila (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Budisusanto, E. (2025). Rekonstruksi Regulasi Peran Amicus Curiae Dalam Pembuktian Pidana Fintech Ilegal Yang Berbasis Keadilan Pancasila (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., ... & Virgio, V. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan siber di indonesia. Innovative: Journal Of Social Science Research, 3(6), 1135-1145.

Daud, B. S., & Jaya, N. S. P. (2022). Kebijakan Hukum Pidana dalam Tindak Pidana Pencucian Uang di Pasar Modal. Journal of Judicial Review, 24(1), 59-80.

Fitri, D. (2024). Tindak Pidana Pengancaman Melalui Media Elektronik Dalam Perspektif Kebijakan Hukum Pidana (Doctoral dissertation, University's Malikussaleh).

Johan, S. (2022). Financial Technology Company's Debt Collection Method: A Legal Aspect. Unnes Law Journal, 8(1), 1-20.

Khalbi, V. T., Maulani, D. G., & Monica, D. R. (2025). Kajian Normatif Dan Yuridis Terhadap Putusan Penyebaran Informasi Elektronik Bermuatan Kesusilaan Dan Ancaman. Causa: Jurnal Hukum dan Kewarganegaraan, 12(12), 51-60.

Kritzinger, E. (2021). Roles and responsibilities for school role players in addressing cyber incidents in South Africa. Eurasian Journal of Social Sciences.

Laia, E. (2025). The role of peer-to-peer (P2P) lending in developing countries: a systematic literature review. International Journal of Innovation Science.

Maknun, L. (2024). Sanksi Pidana Terhadap Pelaku Tindak Pidana Pengancaman Melalui Media Elektronik Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. Disiplin: Majalah Civitas Akademika Sekolah Tinggi Ilmu Hukum sumpah Pemuda, 30(1), 21-28.

Manurung, M. L. (2025). Analisis Hukum Penagihan Pinjaman Online Melalui Media Elektronik "(Studi Kasus Putusan No. 438/Pid. Sus/2020/PN. Jkt. Utr)" (Doctoral dissertation, Universitas Kristen Indonesia).

Marble, J., TRAEBER-BURDIN, S., & Yanakiev, Y. (2020). Human Systems Integration Approach to Cyber Security (Démarche d'intégration humain-systèmes appliquée à la cybersécurité) Final Report of Research Task Group HFM-259. Distribution and Availability on Back Cover. Human Systems Integration Approach to Cyber Security (Démarche d'intégration humain-systèmes appliquée à la cybersécurité). Final Report of Research Task Group HFM-259.

Muchamad, M. K. (Ed.). (2023). Kejahatan Siber Ancaman dan Permasalahannya: Tinjauan Yuridis pada Upaya Pencegahan dan Pemberantasannya di Indonesia. Syiah Kuala University Press.

Najaf, K., Subramaniam, R. K., & Atayah, O. F. (2022). Understanding the implications of FinTech Peer-to-Peer (P2P) lending during the COVID-19 pandemic. Journal of Sustainable Finance & Investment, 12(1), 87-102.

Prawira, M. Y. (2023). Rekonstruksi Regulasi Sanksi Pidana Dalam Perkara Tindak Pidana Financial Technology Berbasis Keadilan Pancasila (Doctoral dissertation, UNIVERSITAS ISLAM SULTAN AGUNG).

Rusadi, F. A. R. P., & Benuf, K. (2020). Fintech peer to peer lending as a financing alternative for the development MSMEs in Indonesia. Legality: Jurnal Ilmiah Hukum, 28(2), 232-244.
Rusadi, F. A. R. P., & Benuf, K. (2020). Fintech peer to peer lending as a financing alternative for the development MSMEs in Indonesia. Legality: Jurnal Ilmiah Hukum, 28(2), 232-244.
Stern, C., Makinen, M., & Qian, Z. (2017). FinTechs in China–with a special focus on peer to peer lending. Journal of Chinese Economic and Foreign Trade Studies, 10(3), 215-228.

Sulastri, R., & Janssen, M. (2023, July). Challenges in designing an inclusive Peer-to-peer (P2P) lending system. In Proceedings of the 24th Annual International Conference on Digital Government Research (pp. 55-65).

Sunardi, R., Hamidah, H., Buchdadi, A. D., & Purwana, D. (2022). Factors determining adoption of fintech peer-to-peer lending platform: an empirical study in Indonesia. The Journal of Asian Finance, Economics and Business, 9(1), 43-51.

Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. Heliyon, 7(4).

Suwondo, D. (2021). Rekonstruksi Regulasi Perlindungan Hukum Terhadap Konsumen Financial Technology Dalam Perjanjian Pinjam-Meminjam Pada Peer To Peer Lending Yang Berbasis Nilai Berkeadilan. Universitas Islam Sultan Agung (Indonesia).

Williams, L. (2021). *US Cybersecurity Implications Trending Into Wireless Power Transfer: An Exploratory Qualitative Case Study* (Doctoral dissertation, Colorado Technical University).