AL RISALAH: Jurnal Ilmu Syariah dan Hukum

VOLUME 26 NO 2, NOVEMBER 2026
P-ISSN: 2252-8334 / E-ISSN: 2550-0309
This work is licensed under a Creative Commons Attribution 4.0 International License
https://doi.org/10.24252/al-risalah.v26i2.68664

Attributing Criminal Liability for AI-Based Credit Scoring Misuse in Digital Lending: A Juridical Qualification Analysis

Nynda Fatmawati Octarina[1*], Fany Dwi Hariyanto[2]
[1]*E-mail: ninda.fatmawati@narotama.ac.id*
[2]*E-mail: fanydwi57@yahoo.com*
[1,2]*Universitas Narotama, Indonesia*
*corresponding author

Article history:
Received in revised form: 02 June 2026
Acceptance date: 07 July 2026
Available online: 19 July 2026

Keywords:
Artificial Intelligence; AI Governance; Financial Technology; Digital Lending; Cybercrime; Electronic Evidence; Corporate Criminal Liability.

How to Cite:
Octarina, N. F., & Hariyanto, F. D. (2026). Attributing Criminal Liability for AI-Based Credit Scoring Misuse in Digital Lending: A Juridical Qualification Analysis. Al-Risalah Jurnal Ilmu Syariah Dan Hukum, 26(2). https://doi.org/10.24252/al-risalah.v26i2.68664

License:
Copyright (c) The authors (2026)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Abstract

The rapid digital transformation of Indonesia's banking sector has accelerated the adoption of Artificial Intelligence (AI)-based credit scoring systems to improve lending efficiency and risk assessment. While previous studies have predominantly examined AI implementation from technological, consumer protection, or financial regulatory perspectives, limited attention has been devoted to the legal qualification of AI-based credit scoring abuse as a criminal offence and the attribution of criminal liability within Indonesia's digital lending framework. This study addresses this gap by analyzing the legal qualification of such misconduct and examining the attribution of criminal liability through the ratio decidendi of Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr. Employing normative legal research with statutory, conceptual, and case approaches, this study finds that the manipulation of AI-based credit scoring constitutes a hybrid criminal offence that simultaneously violates Article 49 paragraph (1) letter a of the Indonesian Banking Law and Article 35 of the Electronic Information and Transactions Law. The study further demonstrates that criminal liability remains attributable to natural persons (natuurlijke persoon) possessing mens rea, whereas AI functions solely as an instrument of the offence rather than as a legal subject. This research contributes to the development of Indonesian criminal law by providing a legal framework for classifying AI-assisted financial crimes and clarifying the attribution of criminal liability in technology-driven financial services. Practically, the findings support the strengthening of AI governance, regulatory harmonization, digital evidence management, and risk supervision within Indonesia's digital financial ecosystem following the enactment of Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector.

INTRODUCTION

The modernization of state financial governance in the contemporary era must be based on the constitutional corridor as mandated by Article 23 of the 1945 Constitution of the Republic of Indonesia.[1] These provisions are implemented through organic regulations that demand the use of the state budget in an accountable, transparent, and efficient manner.[2] In line with these principles, the banking world is overhauling its operations through the adoption of cutting-edge technology in the form of *Artificial Intelligence* to cut rigid bureaucratic lines.[3] Nevertheless, the phenomenon of illegal intervention on *credit scoring mechanisms* based on intelligent computing has triggered a complicated polemic due to the regulatory gray area between cyber law and banking criminal law.[4] Data irregularities in online creditworthiness assessments raise the urgency of legal certainty: whether this crime is purely a conventional banking crime or is it transformed into a cyber computer crime because the main object is in the form of manipulation of electronic documents.[5] This conceptual void is prone to give birth to disparities in law enforcement in prosecuting crimes in the digital financial sector.[6] The development of *the digital lending* industry in Indonesia has shown a significant increase in recent years in line with the increasing use of *Artificial Intelligence* (AI) technology in the creditworthiness analysis process. This technology allows financial service providers to conduct risk assessments quickly through an algorithm-based *credit scoring* mechanism . However, these developments are also followed by an increased risk of data manipulation, misuse of electronic systems, and irregularities in the credit decision-making process. This condition shows that digital transformation not only brings efficiency, but also creates new challenges for criminal law enforcement in the financial services sector.

On the other hand, the problem of criminal liability in the use of AI presents a complex doctrinal puzzle, especially regarding the placement of legal errors in autonomous systems.[7] When financial valuation data is changed to pass a credit facility that is of poor quality, the limitation on the legal subject who bears criminal responsibility becomes

---

[1] Article 23 *of the Constitution of the Republic of Indonesia in 1945*.
[2] *Law Number 17 of 2003 concerning State Finance*.
[3] Sutan Remy Sjahdeini, *Digital Banking: Legal and Risk Perspectives* (Jakarta: Kencana, 2020), 120.
[4] Ahmad M. Ramli, *Cyber Law and Legal Dilemmas in the Digital Era* (Jakarta: PT RajaGrafindo Persada, 2022), 82.
[5] *Law Number 10 of 1998 concerning Banking*.
[6] Edmon Makarim, *Compendium of Telematics Law* (Jakarta: PT RajaGrafindo Persada, 2015), 143.
[7] Muladi and Dwidja Priyatno, *Corporate Criminal Liability in Criminal Law* (Bandung: Bandung College of Law, 2015), 66.

biased.[8] This spectrum of juridical errors can target individual operators who tamper with databases, fintech corporations through the doctrine of *vicarious liability*, and software developers if they are sniffed out intentional motives from the beginning of system design.[9] Through a practical lens, the construction of judicial law in Decision Number 438/Pid.sus/2020/PN Jkt.Utr is an important instrument to dissect the interaction between digital *evidence* and criminal element proof.[10] The consideration of the panel of judges (*ratio decidendi*) in the case needs to be critically examined to assess the depth of the judicial institution's understanding of the working mechanism of fintech and the position of AI as a tool of crime (*instrumentum delicti*). The combination of cyber proof and the judge's conviction will reveal the parameters of current economic criminal law enforcement facing algorithm-based crime.[11]

Research on the use of *Artificial Intelligence* in the financial services sector has been conducted. Most of the research discusses AI from the perspective of technology governance (*AI Governance*), personal data protection, consumer protection, and risk management in *financial technology* services. These studies place AI as an instrument to improve the efficiency of financial services, but have not comprehensively examined the consequences of criminal law arising from the misuse of *credit scoring* algorithms. Another study examines cybercrime and banking crime as two independent legal regimes. In fact, the abuse of AI-based *credit scoring* features has characteristics that are at the intersection of banking law and cyber law. Therefore, an approach that uses only one legal regime has not been able to provide a complete legal construction of these forms of crime.

Another study examines cybercrime and banking crime as two independent legal regimes. In fact, the abuse of AI-based *credit scoring* features has characteristics that are at the intersection of banking law and cyber law. Therefore, an approach that uses only one legal regime has not been able to provide a complete legal construction of these forms of crime. This research offers novelty in two aspects. First, this study builds a legal construction regarding the misuse of AI-based *credit scoring* features as a hybrid crime that integrates banking and cyber law legal regimes. Second, this study analyzes the attribution of criminal liability through *the ratio decidendi* of Decision Number 438/Pid.Sus/2020/PN Jkt.Utr so as to provide a perspective on the limits of accountability between perpetrators, corporations, and AI as a technological instrument.

[8] Sutan Remy Sjahdeini, *Corporate Criminal Liability* (Jakarta: Kencana Prenada Media Group, 2017), 104.
[9] *Ibid.*, 107.
[10] *North Jakarta District Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr*.
[11] Shidarta, *Law of Reasoning and Legal Reasoning* (Jakarta: Kencana, 2013), 112.

Thus, this research is expected to contribute to the development of criminal law in the field of digital financial crimes as well as a recommendation for the formation of legal policies in the AI-based financial services sector.

Based on this description, this study aims to analyze the juridical qualifications of the abuse of *Artificial* Intelligence-based *credit scoring features in* digital lending *schemes* as a banking crime and analyze the attribution of criminal liability based on *ratio decidendi* Decision Number 438/Pid.Sus/2020/PN Jkt.Utr. Unravelling juridical anomalies in the modern banking sector that has *highly regulated characteristics*.[12] By mapping the limits of delicacies, the imposition of errors, and court precedents, this research is expected to be able to contribute solutive thinking for the reform of banking criminal law.[13] This effort is crucial to realize monetary stability and a safe and credible cyber financial ecosystem in the future.[14] The convergence of classical banking law and dynamic information technology law is the main foundation in this normative research.[15] An integrative legal umbrella is absolutely necessary because online lending activities have jumped the physical boundaries of traditional bank operations.[16] Synchronization between regulations is the main prerequisite so that there is no vacuum in the legal norms of state administration when intelligent algorithms malfunction or are abused.[17]

Law Number 10 of 1998 remains the main compass to measure violations of the principle of banking prudence.[18] However, the existence of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law) presents a new paradigm in monitoring the Financial Sector Technology Innovation (ITSK) cluster.[19] This latest law emphasizes the portion of responsibility of fintech operators while strengthening the protection of customer rights.[20] From the cyber aspect, manipulative actions on the scoring feature refer to the latest ITE Law.[21] This cyber regulation focuses sanctions on the aspect of protecting the integrity of the electronic

---

[12] Mariam Darus Badrulzaman, *Banking Law in a Digital Perspective* (Bandung: Citra Aditya Bakti, 2021), 101.
[13] Romli Atmasasmita, *Integrative Legal Theory: Reconstruction of Development Law Theory and Progressive Legal Theory* (Jakarta: Kencana, 2012), 91.
[14] Ahmad M. Ramli, "Legal Protection of Banking Data Integrity in the AI Era," *Transnational Law Journal* 14, no. 2 (2023): 55.
[15] Makarim, *Compendium of Telematics Law*, 155.
[16] Badrulzaman, *Banking Law in a Digital Perspective*, 105.
[17] Ramli, *Cyber Law*, 90.
[18] *Law Number 10 of 1998 concerning Banking*.
[19] *Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law).*
[20] Article 50 of *the P2SK Law*.
[21] *Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions*.

financial system.[22] Clauses on unauthorized access and modification of electronic data are the main juridical weapons to ensnare actors who manipulate program code for illegal gain.[23]

In addition to the law, operational corridors are also controlled by the Financial Services Authority Regulation (POJK).[24] This sectoral regulation outlines cyber risk management obligations for all digital finance industry actors.[25] This standard of administrative compliance serves as an early indicator for judges to test for the existence of individual malicious intent (*mens rea*) or corporate systemic wrongdoing.[26] Based on the description of the background of the problem, the formulation of the problem in this study is: What is the juridical qualification for the misuse of *Artificial Intelligence* (AI) - *based* credit scoring features in *digital lending* schemes as a banking crime according to laws and regulations in Indonesia? And what is the criminal liability and analysis of the judge's legal considerations (*ratio decidendi*) in Decision Number 438/Pid.sus/2020/PN Jkt.Utr related to the misuse of the *Artificial Intelligence* (AI)-*based* credit scoring feature?

METHODS

This research is a normative legal research that focuses on the analysis of positive legal norms related to the abuse of Artificial Intelligence (AI)-based credit scoring features in digital lending services. The approaches used include the statute approach, the case approach, and the conceptual approach.[27] The legislative approach is carried out by examining various relevant regulations, including Law Number 10 of 1998 concerning Banking, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector.

The case approach was carried out through an analysis of the North Jakarta District Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr in order to identify the judge's legal considerations (ratio decidendi) in determining the qualification of the criminal act and the criminal responsibility of the perpetrator. Decision Number 438/Pid.Sus/2020/PN Jkt.Utr was chosen as the object of study because it is one of the decisions that represents the misuse of data in the process of granting credit through electronic systems so that it has relevance to the issue of *credit scoring* abuse based on

[22] Makarim, *Compendium of Telematics Law*, 162.
[23] Ramli, *Cyber Law*, 95.
[24] Badrulzaman, *Banking Law in a Digital Perspective*, 110.
[25] Sjahdeini, *Digital Banking*, 135.
[26] Sjahdeini, *Corporate Criminal Liability*, 118.
[27] Peter Mahmud Marzuki, *Legal Research* (Jakarta: Kencana, 2021), p. 55.

Artificial Intelligence. The decision provides an overview of the application of criminal law to the manipulation of electronic data in the banking sector as well as contains judges' legal considerations that can be analyzed to determine the construction of criminal liability in technology-based crimes. Meanwhile, a conceptual approach is used to examine criminal law doctrines regarding criminal liability, mens rea, cyber crime, corporate criminal liability, and electronic system protection. The legal materials used consist of primary, secondary, and tertiary legal materials. The collection of legal materials is carried out through library research. [28] All legal materials are analyzed qualitatively using prescriptive legal analysis methods. Prescriptive analysis is used to provide arguments regarding the application of legal norms to the problem being studied as well as formulate recommendations for legal settlement based on the principles, theories, and provisions of applicable laws and regulations. Deductive reasoning is used because this research departs from general legal norms and is then applied to concrete problems in the form of the abuse of *Artificial* Intelligence-based *credit scoring* features and the judge's legal considerations in Decision Number 438/Pid.Sus/2020/PN Jkt.Utr. The use of this method is expected to produce legal arguments that are systematic, consistent, and academically accountable.

RESULTS AND DISCUSSION

1. Juridical Qualification of Abuse of Artificial Intelligence-Based Credit Scoring Feature in Digital Lending Scheme as a Banking Crime

Digital transformation in the financial services sector has changed the credit analysis mechanism from a conventional system to a system based on artificial intelligence algorithms (*Artificial Intelligence*). In *digital lending* practice, AI technology is used to assess the risk profile of prospective debtors through automatic data processing based on certain parameters that have been determined by financial service providers. The use of technology is basically a form of innovation that is in line with the principles of efficiency and effectiveness of financial services. However, when the algorithm or data on which decision-making is based is deliberately manipulated to produce a credit score that does not match the actual conditions, then the action has gone beyond the realm of administrative violations and entered the criminal jurisdiction.[29]

Juridically, manipulation of the AI-based credit scoring system can be qualified as an unlawful act because it contains elements of intentionality to create conditions that are

[28] Soerjono Soekanto and Sri Mamudji, *Normative Law Research: A Brief Review* (Jakarta: RajaGrafindo Persada, 2015), p. 13.
[29] Andi Hamzah, *Speciale Delicten in the Criminal Code* (Jakarta: Sinar Grafika, 2016), p. 45.

not in accordance with the actual facts. From a criminal law perspective, these acts meet the characteristics of *fraudulent conduct* which aims to obtain unlawful profits through the misuse of electronic systems. The act of entering incorrect data, changing credit scoring parameters, or modifying the database used by the AI system is a form of information engineering that causes the system to produce wrong decisions. As a result, credit can be given to parties who actually do not meet the eligibility requirements, thus causing losses to financial institutions and threatening the stability of the banking system as a whole.[30]

Research on the misuse of AI technology in the financial sector generally places system manipulation as part of *cybercrime* or technological governance violations. However, most studies have not examined the relationship between banking crime and cybercrime in one integrated legal construction. This study shows that AI-based *credit scoring* manipulation not only attacks the integrity of electronic systems, but also affects the validity of recording and the credit granting process so that it meets the characteristics of hybrid criminal acts.

In Indonesia's positive legal framework, these acts have the characteristics of being a hybrid criminal act because they simultaneously touch the banking law regime and cyber law. From the perspective of banking law, data manipulation that is the basis for recording credit transactions can be categorized as a form of false recording as stipulated in Article 49 paragraph (1) letter a of Law Number 10 of 1998 concerning Banking. The element of "making or causing false records" is not only limited to physical documents, but also includes electronic data used as the basis for bookkeeping and decision-making in the modern banking system. Thus, any intervention in data that affects the results of credit analysis ultimately has the potential to result in financial statements that do not reflect the actual conditions.[31]

On the other hand, the manipulation of data processed by AI systems also meets the elements of criminal acts as stipulated in Article 35 of the Electronic Information and Transaction Law. The provision prohibits any person from intentionally and without rights from manipulating, creating, altering, deletion, or destroying electronic information with the aim of making such information considered as authentic data. In the context of *credit scoring*, the modified data will be processed by the AI system and produce outputs that formally look legitimate, even though they are built on pre-engineered information. Therefore, the object of legal protection in the provision is not

[30] Edmon Makarim, *Introduction to Telematics Law* (Jakarta: RajaGrafindo Persada, 2005), p. 132.
[31] Article 49 paragraph (1) letter a of Law Number 10 of 1998 concerning Banking.

only in the form of electronic data, but also public trust in the integrity of electronic systems used in the financial sector.[32]

Regulation	Protected Objects	Forms of Violation	Relevance to AI Abuse
Banking Law Article 49	Administrative integrity of the bank	False Loggings	Credit data manipulation
ITE Law Article 35	Electronic information	Electronic data manipulation	Perubahan data credit scoring
P2SK Law	Financial sector stability	Technology governance	Strengthening AI surveillance

Based on the theory of protected legal interests (*rechtsbelang theorie*), the act of manipulation of AI-based *credit scoring* actually attacks two legal interests at once. First, legal interests in the form of the integrity of electronic systems are protected by the cyber law regime. Second, legal interests are in the form of public trust in the banking system protected by banking law. Because both legal interests are equally harmed, a law enforcement approach that uses only one of the legal regimes will have the potential to reduce the effectiveness of legal protection. Therefore, the cumulative application of the provisions in the Banking Law and the Information and Electronic Transactions Law is relevant to provide legal certainty while creating a deterrent effect on perpetrators.[33]

The development of regulations through Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector further emphasizes the importance of protecting the digital financial system. The law no longer views technology as a mere instrument to support business activities, but as an integral part of financial sector risk governance. Thus, any misuse of technology that results in the disruption of the reliability of the financial system can be seen as a threat to the stability of the national financial sector. This perspective shows that AI-based *credit scoring* manipulation is not solely a violation of electronic systems, but also an attack on the foundations of trust that underpin the operations of the modern banking industry.[34]

Some countries have developed specific arrangements regarding the use of AI in the financial sector. The European Union through *the Artificial Intelligence Act* classifies AI systems used in creditworthiness assessments as high-risk AI systems so that they must

[32] Article 35 of Law Number 11 of 2008 concerning Information and Electronic Transactions as last amended by Law Number 1 of 2024.
[33] Romli Atmasasmita, *Integrative Legal Theory: Reconstruction of Development Law Theory and Progressive Legal Theory* (Jakarta: Kencana, 2012), p. 94.
[34] Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector.

meet the requirements of transparency, data quality, risk management, and human supervision. Meanwhile, Singapore through the *AI Governance Framework Model* emphasizes the principles of accountability, clarity of algorithmic decision-making, and data governance. Compared to the two countries, the regulation in Indonesia is still spread across various regulations so that it has not specifically regulated legal liability for the misuse of AI in *the credit scoring* system.

2. Criminal Liability and Ratio Decidendi Analysis Decision Number 438/Pid.Sus/2020/PN Jkt.Utr on the Misuse of Artificial Intelligence-Based Credit Scoring Feature

Criminal liability is a juridical consequence imposed on a person who is proven to have committed a criminal act accompanied by an element of guilt (*schuld*). In modern criminal law, the principle *of geen straf zonder schuld* or no crime without fault applies. Therefore, even if an action is carried out by utilizing artificial intelligence technology, criminal liability must still be traced to legal subjects who have the ability to be responsible and have an inner relationship with the act committed.[35] In its deliberations, the panel of judges considered that the defendant consciously changed the data used in the credit granting process so as to produce information that was not in accordance with the actual circumstances. These considerations show that the judge placed the element of intentionality as the main basis for imposing criminal liability. Thus, the focus of the judge's consideration does not lie in the existence of the electronic system used, but in the will of the perpetrator in utilizing the system as a means of committing a criminal act.

These findings are different from a number of previous studies that focused more on the security aspects of electronic systems. This study actually shows that the existence of *trail audits*, system activity logs, and electronic information have an important function to prove the relationship between data manipulation and the element of perpetrator error. Thus, electronic evidence not only serves as supporting evidence, but also becomes the main instrument in proving AI-based crimes.

In the North Jakarta District Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr, the panel of judges placed humans as the main legal subjects responsible for the manipulation of data used in the process of providing credit facilities. The judge argued that electronic systems and software only function as means or tools used to realize the will of the perpetrator. Thus, the existence of technology cannot be used as an excuse to

[35] Andi Hamzah, *Indonesian Criminal Law* (Jakarta: Sinar Grafika, 2019), p. 128.

remove criminal liability because artificial intelligence systems do not have the legal ability to form wills or have malicious intentions (*mens rea*).[36]

Based on the legal facts revealed at the trial, the panel of judges found that there was a conscious and planned action to change or enter data that was not in accordance with the actual circumstances. This act results in the system conducting an incorrect assessment of the debtor's risk profile so that credit can be disbursed to parties who actually do not meet the requirements. The existence of active actions taken by the perpetrator shows that the element of intentionality (*dolus*) has been met. In the doctrine of criminal law, intentionality can be categorized as *opzet als oogmerk*, which is intentionality that is indeed aimed at achieving a certain goal in the form of unlawful disbursement of credit.[37]

The judge's legal considerations in the decision also show that the proof does not only rely on banking administrative documents, but also uses electronic evidence in the form of transaction data, system track records (*audit trail*), and expert testimony in the field of information technology. The use of electronic evidence is in line with the provisions of Article 5 of the Electronic Information and Transaction Law which recognizes electronic information and electronic documents as valid legal evidence. Thus, digital traces that show data changes are an important instrument in proving the involvement of the perpetrator.[38]

From the perspective of criminal liability theory, the verdict reflects the application of *the culprit theory* which requires a relationship between the perpetrator's actions and inner attitudes. The judge does not solely assess the consequences caused, but also assesses the motives, goals, and patterns of action of the perpetrator before the disbursement of credit. Such an approach shows that the Indonesian criminal justice system still places the element of guilt as the main foundation in determining whether or not a person can be convicted.[39]

Interestingly, the panel of judges did not apply the concept of corporate criminal liability even though the crime was committed in the financial services industry. This shows that the judge considers that the main source of error lies with the individual who directly manipulates the data, not with the corporation as an institution. However, in the context of the development of modern financial technology, this approach still leaves

[36] Sutan Remy Sjahdeini, *Corporate Criminal Liability* (Jakarta: Kencana, 2017), p. 145.
[37] Moeljatno, *Principles of Criminal Law* (Jakarta: Rineka Cipta, 2008), p. 171.
[38] Article 5 of Law Number 11 of 2008 concerning Information and Electronic Transactions as last amended by Law Number 1 of 2024.
[39] Muladi and Dwidja Priyatno, *Corporate Criminal Liability* (Jakarta: Kencana, 2010), p. 89.

room for debate because the failure of internal supervision of companies can also contribute to the occurrence of criminal acts. Therefore, in the future, the application of *the corporate criminal liability doctrine* has the potential to be an important instrument in ensnaring corporations that neglect to build an adequate internal control system and information technology security.[40]

From the perspective of corporate criminal liability, *digital lending* service providers can in principle be held accountable if they are proven to be negligent in implementing technology governance, internal supervision, and risk control systems as required in the financial services sector regulations. This negligence can create conditions that allow data manipulation to be carried out by employees or other parties so as to cause losses to financial institutions and the community.

A number of countries have developed corporate accountability mechanisms for AI governance failures. The European Union places high-risk AI system providers as the obligatory parties to ensure compliance with security, transparency, and human oversight standards. This approach shows that legal accountability is not only imposed on individual perpetrators, but can also be extended to corporations if failure of internal supervision contributes to the occurrence of criminal acts. Such an approach can be a reference in the development of Indonesia's criminal law, especially in dealing with the abuse of AI in the financial services sector.

The ratio decidendi built by the panel of judges ultimately emphasized that the manipulation of data used in *the credit scoring* system is a form of criminal act that attacks the integrity of the banking system and the reliability of the electronic system at the same time. This ruling shows that technological developments do not change the basic principle of criminal law, namely that accountability remains inherent in humans as the holder of control over the technology. Therefore, the existence of artificial intelligence must be seen as a tool that can expand the modus operandi of crime, but it cannot replace the position of human beings as legal subjects responsible for the legal consequences they cause.[41]

CONCLUSION

Based on the results of the research and discussion, it can be concluded that the abuse of *Artificial Intelligence* (AI) *-based* credit scoring features in *digital lending* schemes is a form of hybrid criminal act that is at the intersection of banking law and cyber law

[40] Sutan Remy Sjahdeini, *Corporate Criminal Liability*, p. 152.
[41] North Jakarta District Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr.

regimes. Juridically, the act fulfills the elements of a criminal act as stipulated in Article 49 paragraph (1) letter a of Law Number 10 of 1998 concerning Banking because it causes incorrect recording or bookkeeping as a result of manipulation of data used in the credit granting process. In addition, the act also fulfills the elements of Article 35 of Law Number 11 of 2008 concerning Information and Electronic Transactions as last amended by Law Number 1 of 2024 because it is carried out through the manipulation of information or electronic documents so that incorrect data is treated as if it were authentic data. Therefore, the misuse of AI-based *credit scoring* not only threatens the integrity of electronic systems, but also has the potential to undermine public trust in the banking industry and the stability of the national financial system.

Furthermore, criminal liability in the North Jakarta District Court Decision Number 438/Pid.Sus/2020/PN Jkt.Utr is charged to human legal subjects (*natuurlijke persoon*) who deliberately manipulate data to obtain profits illegally. Through the ratio *decidendi analysis*, the panel of judges emphasized that the artificial intelligence system cannot be positioned as a responsible legal subject because it does not have the ability to form will or malicious intent (*mens rea*). AI in such cases only functions as a tool (*instrumentum delicti*) that is used to realize the will of the perpetrator. The judge's legal considerations based on electronic evidence, *audit trails*, and expert testimony show that Indonesian criminal law has been able to accommodate the development of digital technology in the evidentiary process. With the enactment of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, it is necessary to strengthen technology governance, algorithm audits, and supervision of *AI-based credit scoring* systems to ensure data integrity, prevent misuse of financial technology, and realize legal certainty in the digital financial ecosystem. This research provides a scientific contribution to the development of Indonesian criminal law by offering a construction of the qualification of credit *scoring* abuse based *on Artificial Intelligence* as a hybrid criminal act at the intersection between the banking law regime and cyber law. In addition, this study clarifies the concept of criminal liability attribution by emphasizing that AI cannot be positioned as a legal subject, but rather as an instrument used by humans in committing criminal acts. The findings are expected to enrich the study of criminal law, especially in the face of technological developments in the digital financial services sector.

This research has limitations because it uses a normative legal research method that focuses on the analysis of laws and regulations, legal doctrines, and one court decision as the object of study. Therefore, this study has not analyzed the implementation of criminal liability for AI abuse in the practice of *implementing digital lending* empirically or compared more broadly regulatory practices in various countries. Further research is

suggested using an empirical approach or a comparative legal approach to examine the implementation of supervision of the use of AI in the financial services sector, the effectiveness of the implementation of corporate criminal liability, and the development of AI regulation in various countries. The study is expected to provide a more comprehensive basis for the formation of national legal policies in anticipation of the development of artificial intelligence technology in the digital financial sector.

REFERENCES

Books

Amiruddin, dan Zainal Asikin. Pengantar Metode Penelitian Hukum. Jakarta: RajaGrafindo Persada, 2014.

Atmasasmita, Romli. Teori Hukum Integratif: Rekonstruksi Terhadap Teori Hukum Pembangunan dan Teori Hukum Progresif. Jakarta: Kencana, 2012.

Hamzah, Andi. Delik-Delik Tertentu (Speciale Delicten) di Dalam KUHP. Jakarta: Sinar Grafika, 2016.

Hamzah, Andi. Hukum Pidana Indonesia. Jakarta: Sinar Grafika, 2019.

Ibrahim, Johnny. Teori dan Metodologi Penelitian Hukum Normatif. Malang: Bayumedia Publishing, 2016.

Makarim, Edmon. Pengantar Hukum Telematika. Jakarta: RajaGrafindo Persada, 2005.

Marzuki, Peter Mahmud. Penelitian Hukum: Edisi Revisi. Jakarta: Kencana, 2021.

Moeljatno. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta, 2008.

Muladi, dan Dwidja Priyatno. Pertanggungjawaban Pidana Korporasi. Jakarta: Kencana, 2010.

Shidarta. Hukum Penalaran dan Penalaran Hukum. Jakarta: Kencana, 2013.

Soekanto, Soerjono, dan Sri Mamudji. Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: RajaGrafindo Persada, 2015.

Sunggono, Bambang. Metodologi Penelitian Hukum. Jakarta: RajaGrafindo Persada, 2018.

Legislation:

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.

Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi.

Putusan Pengadilan Negeri Jakarta Utara Nomor 438/Pid.Sus/2020/PN Jkt.Utr.

Journals

Agustina, Rosa. "Legal Challenges of Artificial Intelligence in Financial Technology Services." Jurnal Hukum Ius Quia Iustum 30, no. 1 (2023): 1–18.

Makarim, Edmon. "Cybersecurity and Electronic Evidence in Indonesian Criminal Law." Jurnal Hukum dan Pembangunan 53, no. 3 (2023): 415–432.

Prasetyo, Teguh. "Corporate Criminal Liability in the Digital Era." Jurnal RechtsVinding 12, no. 2 (2023): 167–184.

Ramli, Ahmad M. "Perlindungan Data dan Integritas Sistem Elektronik dalam Sektor Keuangan Digital." Jurnal Legislasi Indonesia 21, no. 1 (2024): 45–61.

Sari, Dwi Kusuma. "Pertanggungjawaban Pidana atas Penyalahgunaan Teknologi Artificial Intelligence dalam Transaksi Elektronik." Jurnal Yudisial 17, no. 2 (2024): 201–218.

Setiawan, Budi. "Artificial Intelligence Governance dalam Industri Perbankan Digital di Indonesia." Jurnal Legislasi Indonesia 20, no. 4 (2023): 512–529.

Wahyudi, Arief. "Kejahatan Siber dalam Sistem Keuangan Digital dan Tantangan Penegakan Hukumnya." Jurnal RechtsVinding 13, no. 1 (2024): 85–102.

Yuliana, Rina. "Perlindungan Hukum terhadap Konsumen dalam Layanan Digital Lending Berbasis Artificial Intelligence." Jurnal Arena Hukum 17, no. 1 (2024): 55–72.

Turksen, U., Benson, V., & Adamyk, B. (2024). *Legal Implications of Automated Suspicious Transaction Monitoring: Enhancing Integrity of AI*. *Journal of Banking Regulation*.

Haditama, T. K., & Sugianto, F. (2025). *A Comparative Analysis of Corporate Criminal Liability for AI-Based Malware: A Study of Indonesian and European Union Law*. *Indonesia Law Reform Journal*.

Turksen, U., Benson, V., & Adamyk, B. (2024). *Legal Implications of Automated Suspicious Transaction Monitoring: Enhancing Integrity of AI*. *Journal of Banking Regulation*.