Vol. 3 No. 2 Sep (2025)

J.O.U.R.N.A.L SCIENTIA IUSTITIAE

The Void of Artificial Intelligence Criminal Accountability Norms in Indonesian Criminal Law Reform

Desy Ervitasari[1], Riri Tri Mayasari[2]

[1] [2]College of Universitas Muhammadiyah Bengkulu, Indonesia

email: desy.ervitasari@umb.ac.id

ARTICLE INFO

ABSTRACT

Keywords:

Artificial Intelligence, Legal Subjects, Criminal Responsibility, National Criminal Code, Strict Liability.

DOI. 10.36085/jsi.v2i2.10109

The criminal law reform through Law No. 1 of 2023 (National Criminal Code) has not fully addressed technological disruption, in particular*Artificial Intelligence*(AI) that is autonomous. This study aims to analyze the position of AI in the Indonesian criminal law subject system and the implications of the lack of accountability norms for legal certainty. The research method used is normative juridical with a statutory and conceptual approach. The results of the study indicate that the National Criminal Code still adheres to a rigid anthropocentric paradigm, where Article 45 limits legal subjects to humans and corporations. The legal deadlock occurs in Article 36 concerning the psychological requirement for responsibility, as well as Articles 47 and 50 which provide loopholes for impunity for corporations through the excuse of "preventive measures." The implication is that there are*accountability gap*which is detrimental to the victim. Researchers formulated a legal reconstruction by shifting the paradigm*fault-based liability* going to *strict liability*(absolute accountability) through optimizing Article 37 of the National Criminal Code to guarantee legal protection in the digital era.

INTRODUCTION

The development of global technology has now entered the era of the Industrial Revolution 4.0 which is marked by integration*Artificial Intelligence*(AI) in almost every aspect of human life. AI is no longer merely a mechanical instrument, but has transformed into an autonomous entity capable of massive data processing and decision-making through algorithms.*deep learning*Globally, this autonomous capability is triggering a shift in the legal paradigm, where technology is beginning to transcend the boundaries of traditional regulations that have historically focused solely on human legal subjects. This phenomenon requires law to be more than static, but rather adaptive and progressive in responding to technological dynamics to continue to protect the legal interests of the public.[1]

The dynamics that occur show that AI has reached a level of artificial cognition that is capable of carrying out independent discretion without human intervention.*real-time*This situation disrupts classical legal theory, which views objects as objects completely subject to the control of their owners. Ontologically, the presence of AI capable of "learning" and "adapting" from its environment blurs the boundaries between tools (*instrument*) and actor (*agent*). If the law remains steadfast in the 19th century regulatory patterns, then the law will lose its functional relevance (*functional relevance*) in the face of increasingly exponential algorithmic complexity.

At the national level, Indonesia is undertaking fundamental criminal law reform through the enactment of Law Number 1 of 2023 concerning the Criminal Code (National Criminal Code). This new Criminal Code seeks to modernize Indonesia's penal system by adopting a corrective and rehabilitative justice paradigm. However, although the National Criminal Code is a modern legal product, its provisions regarding legal subjects remain conventional. Based on Articles 45 and 46 of the National Criminal Code, criminal law subjects are still limited to individuals (*natural person*) and corporations (*legal entity*). This limitation indicates that the reform of Indonesian criminal law has not fully addressed the reality of the existence of intelligent digital entities that have the potential to carry out harmful actions independently.[2]

The inconsistency between the spirit of modernizing the National Criminal Code and the limitations of legal subjects reflects the legislative unpreparedness to project future technological risks. Although corporations have been recognized as legal subjects through legal fiction (*legal fiction theory*), the extension of a similar doctrine to AI entities appears to still be a heated debate among Indonesian legal sociology academics. This is crucial, given that in cyber justice practice, cases often occur where losses arise purely from algorithmic decisions that cannot be directly attributed to corporate directors or specific human employees, resulting in deadlocks in criminal prosecutions.

The disparity between the progress of AI technology and existing regulations creates a serious legal problem, namely a normative vacuum (*legal vacuum*) related to criminal responsibility. In Indonesian criminal law doctrine, responsibility is very dependent on the existence of fault (*debt*) which includes intent (*deceit*) or forgetfulness (*blame*). Construction*mens rea*This becomes problematic when applied to AI, because the algorithm does not have a human inner dimension, but its decisions can cause losses that fulfill the

[1] Satjipto Rahardjo, *Ilmu Hukum*, Bandung: Citra Aditya Bakti, 2000, hlm. 124..

[2] Rizky P.P. Karo Karo, "Tantangan Hukum Pidana dalam Menghadapi Perkembangan Artificial Intelligence di Indonesia", *Jurnal Legislasi Indonesia*, Vol. 17, No. 3, 2020, hlm. 297.

elements of a criminal act (*guilty act*).[3]Challenges arise when AI causes harm beyond the control of the programmer (*programmer*) or user (*user*), which has the potential to create accountability gaps (*accountability gap*) where no subject can be punished for the losses incurred.[4]

Inner problems (*mens rea*) in AI is at the heart of the current dogmatic crisis of criminal law. How can the law hold a binary code that lacks moral consciousness accountable? If the law imposes accountability on*programmer*on unpredictable AI autonomous actions (*unforeseeability*), this would actually violate the principle of justice and hinder technological innovation. On the other hand, allowing losses without any responsible subject would undermine the dignity of criminal law as an instrument for victim protection. This dilemma demands a reorientation from a theory of psychological fault-based responsibility to a theory of risk-based responsibility (*risk-based liability*).

More specifically, the absence of regulations regarding the legal status of AI as a subject of electronic law creates legal uncertainty in the enforcement of cybercrime law in Indonesia.[5]If this situation is allowed to continue, the legal objectives of achieving justice and benefit will be difficult to achieve in this era of disruption. Therefore, this research is urgently needed to address this normative gap and find an appropriate formulation of criminal liability for AI.

Based on this background, the problem formulation in this research is: First,*B*What is the position?*Artificial Intelligence*in the current Indonesian criminal law subject system? Second, What are the implications of the lack of norms on AI criminal liability for legal certainty and victim protection in Indonesia? The objectives of this study are: to analyze the limitations of current criminal regulations in reaching legal subjects based on artificial intelligence and to formulate a reconstruction of thinking regarding AI criminal liability as an effort to fill the gap in norms in Indonesian criminal law in the future.

METHOD

This research is normative legal research, namely a process to find legal rules, legal principles, and legal doctrines in order to answer the legal issues faced.[6]The main focus of this research is to examine the gap in norms (*legal vacuum*) related to criminal responsibility*Artificial Intelligence*in the positive legal system in Indonesia. The approach used in this research includes a legislative approach (*statute approach*) and conceptual approach (*conceptual approach*The legislative approach is carried out by examining Law Number 1 of 2023 concerning the Criminal Code (National Criminal Code) and regulations related to electronic information and transactions. Meanwhile, a conceptual approach is used to understand the doctrines of criminal liability and develop the concept of new legal subjects in the digital realm.[7] The legal materials used consist of primary and secondary legal materials. Primary legal materials include laws and regulations related to criminal law and information technology. Secondary legal materials consist of legal textbooks, scientific journals, and

[3] Mahrus Ali dan Arif Rahman, "Kecerdasan Buatan, Subjek Hukum, dan Pertanggungjawaban Pidana", *Jurnal Hukum Ius Quia Iustum*, Vol. 28, No. 1, 2021, hlm. 10.

[4] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2008, hlm. 165.

[5] Ahmad M. Ramli, *Cyber Law dan Digital Forensic dalam Sistem Hukum Indonesia*, Jakarta: Refika Aditama, 2004, hlm. 25.

[6] Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana Prenada Media Group, 2017, hlm. 35.

[7] Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, Malang: Bayumedia Publishing, 2006, hlm. 300.

previous research relevant to the research object.[8]All legal materials that have been collected are then analyzed using a qualitative descriptive analysis method with a deductive thinking pattern, namely drawing conclusions from general statements to specific statements, in order to produce comprehensive legal arguments for the problems being studied.[9]

RESULT AND DISCUSSION

Position*Artificial Intelligence*In the Current Indonesian Criminal Law Subject System: An Exegetical Analysis of Articles 45 to 50 of the National Criminal Code

Subjects of criminal law are traditionally understood as holders of rights and obligations who have the capacity to perform legal acts and be held accountable. In criminal law doctrine, two main types of legal subjects are recognized, namely natural persons (*natural person*) and legal entities or corporations (*legal entity*). The concept of a corporation as a legal subject itself is the result of legal evolution which recognizes that non-human entities can have legal rights and obligations through legal fiction (*legal fiction theory*). This theory states that law creates personification for non-biological entities so that they can carry out legal actions.[10]

However, challenges arise when AI begins to demonstrate autonomous capabilities that transcend corporate organizational structures. As technology advances, discourse has emerged regarding "electronic legal subjects," referring to autonomous, algorithm-based entities. This idea underpins the need to expand the definition of legal subjects beyond biological or organizational dimensions. This expansion of legal subjects is crucial because in modern criminal law, the primary focus is no longer simply on the physical existence of the perpetrator, but rather on the entity's ability to create legal impacts that are detrimental to protected legal interests.[11]

Criminal liability rests on the principle*no punishment without guilt* or *no punishment without guilt*, which means there is no crime without guilt. Guilt in the psychological sense includes the existence of an inner connection between the perpetrator and his actions, whether in the form of intent (*deceit*) or negligence (*blame*).[12]Moeljatno emphasized that for there to be criminal responsibility, the conditions must be met that the act is against the law and the perpetrator has the ability to take responsibility (*accountability*).[13]

The capacity for responsibility requires normal rational functioning to distinguish between socially appropriate and inappropriate actions. However, when the legal subject is an autonomous entity such as AI, conventional fault doctrine runs into a dead end because machines lack moral and psychological aspects. This has led to the emergence of the concept of absolute liability (*strict liability*) in economic and environmental criminal law, where the focus shifts from inner intentions (*mens rea*) toward the real risks or consequences caused by the entity's activities. In the context of AI, this reorientation is crucial so that victims do not

[8] Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Jakarta: Rajawali Pers, 2001, hlm. 13

[9] Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum*, Jakarta: Rajawali Pers, 2012, hlm. 118.

[10] Muladi dan Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Jakarta: Kencana, 2010, hlm. 24.

[11] Mahrus Ali dan Arif Rahman, "Kecerdasan Buatan, Subjek Hukum, dan Pertanggungjawaban Pidana", *Jurnal Hukum Ius Quia Iustum*, Vol. 28, No. 1, 2021, hlm. 12.

[12] Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana*, Yogyakarta: Cahaya Atma Pustaka, 2014, hlm. 158.

[13] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2008, hlm. 154.

lose their right to justice simply because of the absence of a human subject whose intentions can be identified.[14]

In the realm of cyber law,*Artificial Intelligence*categorized as an electronic system that has the ability of autonomy, interactivity, and learning ability (*machine learning*). Theoretically, AI can be classified based on its capabilities, starting from*Weak AI*which only performs specific tasks, up to*Strong AI*which has human-like reasoning abilities. Legal issues arise at the autonomous AI level, where the system is capable of performing actions that were not previously predicted by its creator (*unforeseeability*).[15]

Characteristics of AI that are*black box*This often results in the algorithmic decision-making process being opaque. This poses a challenge for law enforcement in proving the causal chain between the code written by programmers and the crimes committed by machines. Therefore, Indonesian cyber law requires certainty regarding the legal status of AI, whether it remains a tool (*instrument*) or start to be recognized as a legal agent (*legal agent*) which has independent responsibility to ensure legal certainty in cyberspace.[16]The idea of AI as a legal subject is based on the argument that if AI can make decisions that are detrimental to legal interests independently, then there must be a clear legal attribution mechanism to ensure legal certainty and protection of victims from anonymous and automated cybercrime.

Criminal policy (*criminal policy*) is a rational effort by society to combat crime. In the context of technological criminal law, this policy is not only oriented towards the penal aspect (criminal law), but also non-penal aspects such as systemic and technical policies.[17]Normative criminal policy in Indonesia is currently being tested by the presence of*Artificial Intelligence*which has the potential to cause far more damage than conventional crimes. A policy shift from a reactive to an anticipatory approach is essential to ensure the law remains thriving in keeping pace with technological advancements. This underpins the idea that the functionalization of criminal law in the digital realm must include regulations on algorithmic risk management as part of the legal obligations of the relevant legal entities.[18]

In an effort to reach the accountability of non-human entities, criminal law recognizes the doctrine of*vicarious liability*(vicarious liability), where a person is responsible for the actions of another person within his/her scope of supervision. In addition, there is*identification theory*which states that the actions and intentions of the "brain" of an entity can be attributed as the actions of the entity itself.[19] In the context of AI, this doctrine was developed to determine whether AI's faults can be attributed to its creators (*developer*) or its users (*user*). A review of this doctrine becomes crucial to fill the legal gap when*mens rea*biologically not found, but real detrimental impacts have occurred due to the failure or misuse of artificial intelligence systems.[20] The results of the study show that the position*Artificial Intelligence*(AI) in the

[14] Sudarto, *Hukum dan Hukum Pidana*, Bandung: Alumni, 1981, hlm. 95.

[15] Ahmad M. Ramli, *Cyber Law dan Digital Forensic dalam Sistem Hukum Indonesia*, Jakarta: Refika Aditama, 2004, hlm. 38.

[16] Rizky P.P. Karo Karo, "Tantangan Hukum Pidana dalam Menghadapi Perkembangan Artificial Intelligence di Indonesia", *Jurnal Legislasi Indonesia*, Vol. 17, No. 3, 2020, hlm. 301.

[17] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*, Jakarta: Kencana, 2008, hlm. 28.

[18] Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana*, Yogyakarta: Cahaya Atma Pustaka, 2014, hlm. 95.

[19] Sudarto, *Hukum dan Hukum Pidana*, Bandung: Alumni, 1981, hlm. 102.

[20] Mahrus Ali dan Arif Rahman, "Kecerdasan Buatan, Subjek Hukum, dan Pertanggungjawaban Pidana", *Jurnal Hukum Ius Quia Iustum*, Vol. 28, No. 1, 2021, hlm. 15.

Indonesian criminal law system is still in the zone"Legal Paralysis". Although Law No. 1 of 2023 is a manifestation of legal decolonization, its regulations regarding legal subjects are stillanthropocentric.

1. Limitation of Legal Subjects in Article 45 Provision Article 45explicitly states: *"Corporations are subjects of criminal acts."*[21]

Researchers argue that the restrictive use of the term "Corporation" in this article closes the gap for recognizing digital entities as independent subjects. Ontologically, Indonesian law still views legal subjects in only two spectrums: biological (human) and organizational (corporation). Autonomous AI falls outside of both spectrums. Based on*Theory of Legal Personhood*, an entity is considered a legal subject if it has rights and obligations. Modern AI, which has autonomy in economic transactions and technical decision-making, should be viewed as "Digital Personhood." However, Article 45 reduces AI to the status of an inanimate object (*case*) or mere tools. This creates a legal imbalance where an entity has the capacity to act (*capacity to act*) but does not have legal capacity (*legal capacity*) to be held accountable.[22]

Furthermore, Article 46It details that corporations include legal entities (PT, Foundation, Cooperative, BUMN/D) as well as associations, both legal entities and non-legal entities. Normatively, AI does not have a place in the human category (*natural person*) and corporations (*legal entity*). Researchers argue that this limitation reflects the law's unpreparedness to capture the reality of digital autonomy. Based onLegal Fiction Theory (*Legal Fiction Theory*), if the law is able to create "artificial figures" in the form of corporations, then there is no strong theoretical reason to reject AI as a subject of electronic law (*electronic personhood*), considering that AI has the ability to make independent decisions (*autonomous agency*).[^2]

2. Attribution Deadlock in Article 47The most crucial obstacle was found inArticle 47which reads: *"Criminal Acts by Corporations are Criminal Acts committed by managers who have a functional position in the Corporation's organizational structure or people who, based on work relationships or other relationships, act for and on behalf of the Corporation."*[23]

At the theoretical level, Article 47 adopts*Identification Theory*, where the actions of managers are identified as corporate actions. However, this theory suffers from "functional death" when dealing with autonomous AI. AI does not operate based on instructions.*step-by-step*from the administrator, but through*Dynamic Learning*. Researchers found that there is a phenomenon of "Algorithmic Blindness" among corporate managers; they provide the infrastructure, but do not control it.*output*End. Because AI is not a biological "manager" or "person with an employment relationship," any losses arising from AI's independent decisions cannot be attributed to the corporation through Article 47. This is a fatal attributional deadlock in our corporate criminal liability system.[24]

In an AI system that uses*deep learning*, a phenomenon occurs"Breaking the Chain of Command" (*Decoupling*)AI operates outside the daily instructions of managers. When AI engages in market manipulation or algorithmic discrimination, these actions are not a manifestation of human managers' commands, but rather the result of the algorithm's own evolution. Under Article 47,

[21] Indonesia, *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*, Ps. 45.

[22] Mahrus Ali dan Arif Rahman, "Kecerdasan Buatan, Subjek Hukum, dan Pertanggungjawaban Pidana", *Jurnal Hukum Ius Quia Iustum*, Vol. 28, No. 1, 2021, hlm. 35.

[23] Indonesia, *Op.Cit.*, Ps. 47.

[24] Rizky P.P. Karo Karo, "Tantangan Hukum Pidana dalam Menghadapi Perkembangan Artificial Intelligence di Indonesia", *Jurnal Legislasi Indonesia*, Vol. 17, No. 3, 2020, hlm. 312.

AI cannot be classified as a manager or worker, so legally, its autonomous actions are considered without a responsible subject.[25]

Implications of the Lack of AI Criminal Responsibility Norms for Legal Certainty and Victim Protection

The absence of AI accountability norms has implications for the collapse of the pillars of criminal justice regulated in Chapter II of the National Criminal Code. The Crisis of the Principle of Fault in Article 36 Article 36 paragraph (1) confirms the main pillars of Indonesian criminal law: *"Any person can only be held responsible for the criminal acts they commit if that person has the capacity to be responsible at the time of committing the criminal act."*[26]

The researcher's analysis shows that Article 36 is a "great wall" protecting AI from criminal charges. The phrase "responsibility" is always dogmatically associated with the functions of reason and will (*intellect* And *will*). AI has artificial intelligence (*artificial intellect*), but does not have free will (*free will*). If we refer to the doctrine*The act does not make a person guilty unless the mind is guilty.*, then the absence of a psychological dimension in AI means that digital crimes can never be turned into perfect crimes. The implication is that developers (*programmer*) will always use Article 36 as a defense that they did not have "evil intent" (*malice*) when their algorithms make mistakes autonomously. This creates an "accountability vacuum" that endangers public order.[27]

This norm requires the existence of an inner psychological dimension (*mens rea*). The implications for AI are fatal; AI does not have the mind to form intention (*deceit*) or negligence (*blame*). If an accident occurs in an AI-based medical system, the law will be at a dead end. Developers (*programmer*) is difficult to be charged with negligence if it has followed the code standards, while AI cannot be charged because it does not have "mental capacity" according to Article 36. This creates"Impunity Loophole", where real losses occur (*guilty act*), but there is no subject who can be blamed morally-juridically.

Impact on Victim Protection: Misuse of Articles 48 and 50 The most detrimental implication for victims is the potential misuse of Article 48 which stipulates the conditions for criminalizing corporations, particularly point (c):*"accepted as Corporate policy"*. How to prove that AI's "self-learning" actions are a policy?

Researchers conducted a micro-analysis of Article 50, which reads:*"A corporation cannot be punished if the corporation has taken preventive measures..."*[28]The phrase "preventive measures" in the context of AI is highly biased and technically immeasurable. Corporations can simply prove they have conducted a formal system audit to absolve themselves of criminal liability. However, AI has inherently*unpredictability*As a result, victims (e.g., individuals harmed by discriminatory AI credit scoring systems or robotics malpractice) find themselves in a very vulnerable position. Corporations enjoy the economic benefits of AI efficiency, but when risks arise, they use Article 50 as a "fire escape" to shift losses to victims. This is a form of distributive injustice in our digital criminal law.[29]

Under Article 50, technology companies can easily escape criminal liability by claiming they have implemented security protocols, but the AI autonomously bypasses those protocols. This

[25] *Ibid*

[26] Indonesia, *Op.Cit.*, Ps. 36 verse (1).

[27] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2008, hlm. 165.

[28]Indonesia,*Op.Cit.*, Ps. 50

[29] Ahmad M. Ramli, *Cyber Law dalam Sistem Hukum Indonesia*, Jakarta: Refika Aditama, 2004, hlm. 120.

allows corporations to profit from AI while shifting the risk of harm to the victims.

Reconstruction of Thought: Urgency*Strict Liability*in Article 37

In response to the research objective regarding the reconstruction of thought, the researcher proposes the use of Article 37 letter a as a transitional solution:

"Any person can be punished solely because the elements of a crime have been fulfilled without regard to any fault."[30]

The reconstruction offered by researchers is by shifting the paradigm from*Fault-based Liability* the *Risk-based Liability*. Considering that AI is an entity that contains high inherent risks (*inherently dangerous*), then the use of Article 37 letter a must be the standard in technology-based crimes. With the doctrine*Strict Liability*, prosecutors no longer need to get bogged down in proving the developer's inner workings or complicated board policies. Simply prove that the corporation's AI has caused harm (*guilty act*), then corporations must bear criminal responsibility. This step is crucial to filling the regulatory gap while providing legal certainty and maximum protection for victims in the AI era.[31]

Researchers argue that specifically for AI-based crimes, Indonesia must shift from an error-based paradigm (*fault-based*) to Absolute Responsibility (*Strict Liability*). In this way, legal responsibility is placed on the technology risk owner, in order to ensure the protection of the legal interests of society (*social defence*) remains maintained in the era of digital disruption.

To prove the inability of Articles 36 to 50 of the National Criminal Code to address technological dynamics, the researcher presents two case analyses that are directly confronted with Indonesian positive legal norms:

1. Autonomous Vehicle Case (2018 Uber Case in Arizona) vs Article 36 and Article 47

In a fatal 2018 incident, an Uber self-driving car struck a pedestrian, killing him. An investigation revealed that the car's AI failed to correctly classify human objects.Confrontation with Article 36:If this case happened in Indonesia, the public prosecutor would hit a limit.Article 36 of the National Criminal Code. The AI does not possess a "mental state" or "responsibility capacity" to recognize the unlawful nature of its actions. Because the AI is not a human being, it cannot be considered a "person" under Article 36. Confrontation with Article 47:To convict the Uber corporation, prosecutors must prove that the act was committed by a "manager holding a functional position." However, the accident arose from*error*autonomous algorithm, not direct instructions from the board of directors. Happened*decoupling*(disconnection) between the intentions of the management and the actions of the machine, so that the attribution of corporate crime becomes impossible without expanding the meaning of the legal subject.[32]

2. Case*Flash Crash*Banking and Trading Algorithms vs Article 48 and Article 50

In the world of banking and investment, the use of AI for*High-Frequency Trading*(HFT) often triggers extreme volatility that causes massive public harm in a matter of seconds.

[30] Indonesia, *Op.Cit.*, Ps. 37 huruf a.

[31]Rizky P.P. Karo Karo,*Op.Cit.*, p. 335.

[32] Rizky P.P. Karo Karo, "Criminal Law Challenges",*Indonesian Journal of Legislation*, Vol. 17, No. 3, 2020, hlm. 335.

Confrontation with Article 48:This article requires that a corporate crime must "unlawfully benefit the corporation" or "be accepted as corporate policy." In the case of a trading algorithm that has experienced*glitch*or acts wildly beyond parameters, a corporation can argue that the AI's actions are not company "policy," but rather a technical anomaly. Confrontation with Article 50:This is where the "emergency door" for corporations opens wide.Article 50 of the National Criminal Codestates that corporations cannot be prosecuted if they have taken "preventive measures." Banks can easily prove that they have installed industry-standard security protocols. However, the nature of AI is*self-learning*This allows it to bypass the protocol. As a result, public harm still occurs, but the corporation is exempt from criminal liability due to the protection of Article 50. This creates an injustice where the risks of technology are borne entirely by the public, not by the owners of the technology. Based on the article-by-article analysis and the confrontation of the cases above, the researcher found that the current Indonesian doctrine of criminal responsibility is experiencing..."Legal Involution". Our criminal law seems to have returned to the past by maintaining human psychological requirements (Article 36) for technological phenomena that are mechanical-digital in nature.

The implication is the emergence of"Irresponsible Actor" (*responsibility-free actors*). If this continues, the legal objective of realizing benefits and distributive justice for victims of technological crimes will never be achieved. Researchers emphasize the need for a shift from the paradigm*fault-based liability*(error-based) towards*risk-based liability*(risk-based), where Articles 45 to 50 of the National Criminal Code must be amended to include the categoryElectronic Agentas a legal subject who can be held absolutely accountable (*strict liability*).

Conclusion

This study confirms thatThe lack of norms in Law No. 1 of 2023 arises from the persistence of the anthropocentric paradigm that locks the conditions for accountability to the psychological dimension of humans (Article 36) and the functional attribution of administrators (Article 47), thus creating a gap of digital impunity when dealing with autonomy.*Artificial Intelligence*.The implications of the rigidity of these articles, particularly the use of Article 50 as a corporate "emergency exit," have shifted the risk of technological loss entirely to the victims without any certainty of criminal restitution. Therefore, legal reconstruction through the adoption of the doctrine of*strict liability*which is based on Article 37 letter a becomes a legal imperative to fill this gap, to ensure that national criminal law is not only an artifact of the past, but is able to act as an instrument for community protection that is responsive to the dynamics of digital autonomy in the future.

BLIBLIOGRAPHY

Amiruddin dan Zainal Asikin. (2012). *Pengantar Metode Penelitian Hukum*. Jakarta: Rajawali Pers.

Arief, Barda Nawawi. (2008). *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana.

Hiariej, Eddy O.S. (2014). *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka.

Ibrahim, Johnny. (2006). *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia

Publishing.

Marzuki, Peter Mahmud. (2017). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.

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

Muladi dan Dwidja Priyatno. (2010). *Pertanggungjawaban Pidana Korporasi*. Jakarta: Kencana.

Rahardjo, Satjipto. (2000). *Ilmu Hukum*. Bandung: Citra Aditya Bakti.

Ramli, Ahmad M. (2004). *Cyber Law dan Digital Forensic dalam Sistem Hukum Indonesia*. Jakarta: Refika Aditama.

Soekanto, Soerjono dan Sri Mamudji. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers.

Sudarto. (1981). *Hukum dan Hukum Pidana*. Bandung: Alumni.

Ali, Mahrus dan Arif Rahman. "Kecerdasan Buatan, Subjek Hukum, dan Pertanggungjawaban Pidana". *Jurnal Hukum Ius Quia Iustum*, Vol. 28, No. 1, 2021.

Karo Karo, Rizky P.P. "Tantangan Hukum Pidana dalam Menghadapi Perkembangan Artificial Intelligence di Indonesia". *Jurnal Legislasi Indonesia*, Vol. 17, No. 3, 2020.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.