

Vicarious Liability Theory on Vicarious Liability on Artificial Intelligence (AI) in the context of Cryptocurrency

Ayu Pramachanti Rumiarta¹
Timotius Nico Yogatama²

Abstract

This study aims to discuss and analyze how substitute accountability in Artificial Intelligence (AI) in the context of Cryptocurrency, analyzed with Vicarious Liability theory. The use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency. Technological developments have given birth to various kinds of alternative tools or instruments as a substitute for money, which could be possible for violations of the law in the use of Artificial Intelligence (AI) in cryptocurrency transactions. The research method used in this study is a type of normative legal research method. In normative legal research, a study that leads to the process of finding legal rules, legal principles, and legal doctrines that function to answer legal issues faced. The choice of the type of normative legal research in this study is related to the analysis of Vicarious Liability Theory in the context of substitute liability in Artificial Intelligence (AI). The results of the study show the importance of understanding the theory of Vicarious Liability as a theory that determines substitute liability in Artificial Intelligence (AI), this is because the use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency, so it does not rule out the possibility that the AI does not carry out actions in accordance with AI commands which will certainly harm all parties, including business consumers of digital financial transactions in the event of a digital transaction error, then the person responsible is not the AI subject but the subject who from the beginning provides the use of Artificial Intelligence (AI) in cryptocurrency transactions.

Keywords: Vicarious Liability, Artificial Intelligence, Cryptocurrency

Copyright (c) 2024 Author (s).



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

¹Bachelor of Law, Bali Dwipa University, Indonesia, email : ayupramachanti@gmail.com

²Researcher, Plekhanov Russian State University, Russia, email : timotiusnicoyg@gmail.com

1. Introduction

That the use of Artificial Intelligence or AI is very beneficial in the aspect of business diversification in the international scope, one example in the banking world business. Many countries have gradually started using Artificial Intelligence or AI in the banking world. A number of banks have implemented bank activities online and without coming to the bank (Nur Kholis, 2018), that in addition to that, governments in countries in the world have also begun to order all banks to be able to utilize this AI technology in their respective banking systems. Considering that banking services are very important and have a major influence on the economic development of a country to achieve a significant business and income.

Furthermore, the use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency. Technological developments have given birth to various kinds of alternative tools or instruments as a substitute for money. An example is the use of digital money that prioritizes speed, convenience and efficiency in conducting a transaction (Untung Rahardja, 2018), this development aims to reduce the level of cash use among the public.

That there are two categories of payments in e-money, namely digital money as used in video game applications and money embedded with crypto password technology or can be called cryptocurrency (Ferry Mulyanto, 2015). Cryptocurrency is a name given to digital currencies that have a cryptographic system or literary cipher base that allows both parties to conduct financial transactions in a non-central distribution way as in traditional currencies (Eli Dourado and Jerry Brito, 2014). The difference between cryptocurrency and existing currencies is that this cryptocurrency is not issued by a central authority, there is no interference or manipulation by the government (Haruli Dwicaksana Pujiyono, 2020).

Artificial Intelligence (AI) is one of the technologies that are of concern to many countries. Broadly speaking, we can interpret that what is meant by Artificial Intelligence (AI) is a "machine" that has the ability and intelligence like ordinary humans, but these abilities are first regulated by humans themselves. This AI was created to help tasks like tasks done by humans, exactly or even more like done by humans (Putri, Anggia Dasa, Dapit Pratama, 2017), So we can conclude that

this AI was created for the same purpose as what humans do in general, namely doing something that can even exceed and as a substitute for humans to do an action

A technological development will have an impact on the positive side and it is possible that there is a negative side that develops as well, it also happens to businesses or transaction processes that require Artificial Intelligence (AI), that every development of AI technology in addition to having a positive impact, will not be separated from the influence of the negative impact caused by AI . One of these negative impacts is the possibility of digital errors, unilateral takeover of one's digital money using AI, cryptocurrency transactions, as well as misuse of personal data or leaking of personal data from the consumers concerned due to Artificial Intelligence (AI) errors. It does not rule out the possibility that the AI does not carry out actions in accordance with orders that will certainly harm all parties, including bank consumers or business consumers of digital financial transactions. Although the AI has initially been set and entered several formulas and data that can later match the intelligence of ordinary humans, it will not make the AI can be said to be a subject of law. . Moreover, if the leakage of personal data is caused by the use of AI errors through electronic features such as e-banking, cryptocurrency transactions and several other features that are certainly inseparable from the personal data of the consumers concerned and cryptocurrency digital financial transactions. So the importance of law enforcement in accountability in the context of substitute accountability for Artificial Intelligence (AI) in cryptocurrency transactions.

Law enforcement is the process of making efforts to uphold or function legal norms in a real way as a guide for behavior or legal relations in public and state life. Viewed from the point of view of the subject, law enforcement can be carried out by a broad subject and can also be interpreted as an effort to enforce the law involving all legal subjects in every legal relationship. . Anyone who carries out normative rules or does something or does not do something based on the norms of the applicable rule of law, means that he is exercising or enforcing the rule of law. In a narrow sense, in terms of its subject, law enforcement is only interpreted as an effort by certain law enforcement officials to guarantee and ensure the enforcement of the law, if necessary, law enforcement officials are allowed to use force (Rais Ahmad, 2007). The use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency, so it does not rule out the possibility that AI experiences digital transaction errors

so that it does not carry out actions in accordance with orders which will certainly harm all parties, including consumers of digital financial transaction businesses. Although the AI has initially been set and entered several formulas and data that can later match the intelligence of ordinary humans, it will not make the AI can be said to be a subject of law.

2. Problem Research & Methode Research

Based on the background of the problem above, the formulation of the problem in this study is how substitute accountability in Artificial Intelligence (AI) is analyzed with the theory of Vicarious Liability. Legal research can be classified into two types, namely normative research and empirical research (Soerjono Soekanto, 2014). The type of research used in this study is a type of normative legal research. In normative legal research, a research that leads to the process of finding legal rules, legal principles, and legal doctrines that function to answer legal issues faced (Mukti fajar and Achmad Yulianto, 2015). The type of normative legal research in this study was chosen because this study examines the Vicarious Liability Theory on substitute liability in Artificial Intelligence (AI) in the context of Cryptocurrency transactions. In answering legal issues, this research used a study of documents obtained through literature materials and laws and regulations, this was done to obtain the results of research on Vicarious Liability Theory in the context of substitute liability in Artificial Intelligence (AI) in the context of Cryptocurrency transactions.

3. Analysis and Discussion

Law enforcement is the process of making efforts to uphold or function legal norms in a real way as a guide for behavior or legal relations in public and state life. Viewed from the point of view of the subject, law enforcement can be carried out by a broad range of subjects and can also be interpreted as law enforcement efforts that involve all legal subjects in every legal relationship. Anyone who carries out normative rules or does something or does not do something based on the norms of the applicable rule of law, means that he is exercising or enforcing the rule of law. In a narrow sense, in terms of its subject, law enforcement is only interpreted as an effort by certain law enforcement officials to guarantee and ensure the enforcement of the law, if necessary, law enforcement officials are allowed to use force (Rais Ahmad, 2007). That the importance of law enforcement in cases related to the occurrence of digital transaction system errors in the use of

Artificial Intelligence is also often used in the business of digital money transactions, such as cryptocurrency.

The use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency. Technological developments have given birth to various kinds of alternative tools or instruments as a substitute for money. An example is the use of digital money that prioritizes speed, convenience and efficiency in making a transaction (Untung Rahardja, 2018), This development aims to reduce the level of cash use among the public.

That there are two categories of payments in e-money, namely digital money as used in video game applications and money embedded with crypto password technology or can be called cryptocurrency (Ferry Mulyanto, 2015). Cryptocurrency is a name given to digital currencies that have a cryptographic system or literary cipher base that allows both parties to conduct financial transactions in a non-central distribution way as in traditional currencies (Eli Dourado and Jerry Brito, 2014). The difference between cryptocurrency and existing currencies is that this cryptocurrency is not issued by a central authority, there is no interference or manipulation by the government (Haruli Dwicaksana Pujiyono, 2020).

The use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency, so it does not rule out the possibility that AI experiences digital transaction errors so that it does not carry out actions in accordance with orders which will certainly harm all parties, including consumers of digital financial transaction businesses. Although the AI has initially been set and entered several formulas and data that can later match the intelligence of ordinary humans, it will not make the AI can be said to be a subject of law. Furthermore, who will be held accountable for the actions of AI that experiences errors, in this case, the possibility of digital errors, unilateral takeover of one's digital money using AI, cryptocurrency transactions, as well as misuse of personal data or leaks of personal data from consumers concerned due to Artificial Intelligence (AI) errors; It does not rule out the possibility that the AI does not carry out actions in accordance with orders that will certainly harm all parties, including bank consumers or business consumers of digital financial transactions.

To answer these problems, based on the theory of Vicarious Liability on substitute liability in Artificial Intelligence (AI) in the context of Cryptocurrency transactions, in this case Hans

Kelsen once explained that what is meant by legal liability is a legal obligation where a person or legal subject in this case the person must accept sanctions for the actions he commits contrary to the law, then a legal liability is born from the actions of a subject of law that is contrary to the existing law or a violation of the law.

So with the theory of vicarious liability, the theory basically explains that other people, in this case, human legal subjects can be responsible for a behavior or wrong committed by another person or human being. This theory can be applied to the actions of Artificial Intelligence (AI) whose actions can cause losses and other legal consequences, especially in this case related to AI experiencing errors in this case the possibility of digital errors unilaterally taking over someone's digital money using AI cryptocurrency transactions, as well as misuse of personal data or leakage of personal data from concerned consumers due to Artificial Intelligence (AI) errors.

Law as the protection of human interests is different from other norms. Because the law contains orders and or prohibitions, and divides rights and obligations. Sudikno Mertokusumo stated not only about the purpose of law, but also about the function of law and legal protection. He argued that: "in its function as the protection of human interests the law has a purpose. Law has a goal to be achieved while the main purpose of law is to create order and balance. With the achievement of order in society, it is hoped that human interests will be protected. In achieving its goals, the law is tasked with dividing rights and obligations between individuals in society, dividing authority and regulating how to solve legal problems and maintain legal certainty.

Roscoe Pound was quoted by Sudikno Mertokusumo as stating that law is the most important institution in carrying out social control and/or social engineering. Pound also recognized that another function of law is as a means to perform social engineering. He said that the legal system achieves the goal of legal order by recognizing these interests, by setting limits on the recognition of those interests and the rule of law developed and applied by the judicial process has a positive impact and is implemented through authoritative procedures, also trying to respect various interests in accordance with the recognized and established boundaries (Lili Rasjidi & Ira Thania Rasjidi, 2002). Regarding law enforcement, it will relate to accountability by perpetrators, one example is that electronic system operators are obliged to protect their users and/or user subjects from losses incurred by electronic systems that they create or maintain.

That the theory of vicarious liability essentially explains that another person, in this case,

the subject of human law, can be responsible for a behavior or wrong committed by another person or human being. This theory can be applied to the actions of Artificial Intelligence (AI) whose actions can cause losses and other legal consequences, especially in this case related to AI experiencing errors, in this case the possibility of digital errors unilaterally taking over someone's digital money using AI cryptocurrency transactions, misuse of personal data or leakage of personal data from consumers concerned due to Artificial Intelligence (AI) errors. Furthermore, the legal principle offered by the researcher is that the operator of the electronic system must protect its users and / or user subjects from losses incurred by the electronic system that he makes or is organized by the organizer.

4. Conclusion

Analysis of Vicarious Liability Theory in the context of substitute liability in Artificial Intelligence (AI), shows the importance of understanding Vicarious Liability theory as a theory that determines substitute liability in Artificial Intelligence (AI), this is because the use of Artificial Intelligence is also often used in the business of digital money transactions, for example such as cryptocurrency, so it does not rule out the possibility that the AI does not carry out actions in accordance with AI commands which will certainly harm all parties, including digital financial transaction business consumers if there is a digital transaction error, then the person responsible is not the AI subject but the subject who from the beginning provides the use of Artificial Intelligence (AI) in cryptocurrency transactions. That what is meant by legal liability is a legal obligation in which a person or legal subject in this case the person must accept sanctions for the actions he commits contrary to the law, then a legal liability is born from the actions of a legal subject who is contrary to the existing law or violation of the law.

So with the theory of vicarious liability, the theory basically explains that other people, in this case, human legal subjects can be responsible for a behavior or wrong committed by another person or human being. This theory can be applied to the actions of Artificial Intelligence (AI) whose actions can cause losses and other legal consequences, especially in this case related to AI experiencing errors in this case the possibility of digital errors unilaterally taking over someone's digital money by using AI cryptocurrency transactions, and misuse of personal data or leakage of personal data from consumers concerned due to Artificial Intelligence (AI) errors. Furthermore,

the legal principle offered by the researcher is that the principle of the operator of the electronic system must protect its users and / or user subjects from losses incurred by the electronic system that he makes or organized by the organizer

Reference

- Eli Dourado and Jerry Brito, (2014), *Bitcoin - Solving Double Spending*, The New Palgrave Dictionary of Economics, London, hlm. 4.
- Ferry Mulyanto, (2015), *Utilization of Cryptocurrency as the Application of Rupiah Currency into Digital Form Using Bitcoin Technology*, *IJNS – Indonesian Journal on Networking and Security – Volume. 4 No. 4*, p. 7.
- Haruli Dwicaksana Pujiyono. (2020). "Legal Effects Arising from Cryptocurrency as a Payment Instrument in Indonesia", *Journal of Private Law Civil Affairs Section, Faculty of Law, Sebelas Maret University, Surakarta*.
<https://jurnal.uns.ac.id/privatlaw/article/view/48407/29941>, accessed March 5, 2024.
- Lili Rasjidi & Ira Thania Rasjidi, (2002). *Introduction to Legal Philosophy*, Mandar Maju, Bandung, p. 74.
- Mukti fajar and Achmad Yulianto, (2015). *Dualism of Normative & Empirical Legal Research*, Student Library, Yogyakarta, p. 280
- Nur Kholis, (2018). "Banking in the New Digital Era", *Journal of Economicus* 12, No. 1 (80-88)
- Putri, Anggia Dasa and Dapit Pratama. (2017). "Expert System Detects Cybercrime Using Web-Based Forward Chaining Method in Batam City", *Journal of Edik Informatika* 3, No. 2 (197-210), p. 199
- Prabu Buana Rumiarta, I. N. (2022). *Correlation Theory A.V. Dicey Perspective of the Rule of Law in Indonesia: Correlation Theory A.V. Dicey Perspective of the Rule of Law in Indonesia*. *Focus Journal Law Review*, 2(1).
<https://ojs.balidwipa.ac.id/index.php/fjl/article/view/19>
- Riswandi, S. &. (2021). *Juridical Analysis of the Guidance and Formation of Inmates in Class Correctional Institutions* *I, 1*, 101–108.
- Rumiarta, I. N. P. B., Astariyani, N. L. G., & Indradewi, A.A.S. (2022). *Human Rights of Indigenous People in Indonesia: A Constitutional Approach*. *Journal of East Asia and International Law*, 15(2), 395-402. http://journal.yiil.org/home/archives_v15n2_10

Rumiarta, I. N. P. B., Astariyani, N. L. G., & Amaral, A. M. (2022). The Comparative Law on the Distribution of Power in the 1945 Constitution of the Republic of Indonesia and the Constitution of the Republic Timor Leste. *Jurnal IUS Kajian Hukum Dan Keadilan*, 10(3), 541–554. <https://doi.org/10.29303/ius.v10i3.1134>

Rumiarta, I.P., Indradewi, A.S., & Gomes, A. (2023). Comparative Law on the Authority of the House of Representatives (Indonesia) with the National Parliament (Timor Leste). *SASI*, 29(1), 18-28. DOI: <https://doi.org/10.47268/sasi.v29i1.1075>.

Rais Ahmad, (2007). *The Role of Humans in Law Enforcement*, Pustaka Antara, Jakarta, p. 19

Soerjono Soekanto, (2014). *Introduction to Legal Research*, University of Indonesia Press, Jakarta, p.2.

Sudikno Mertokusumo, (1999). *Knowing the law An Introduction*, Liberty, Yogyakarta, p. 71.

Untung Rahardja. (2018). Application of Blockchain Technology as a Media for Securing the E-Commerce Transaction Process. *Journal of Computer Engineering Systems and Science*. Vol. 5 No.1, available on <https://jurnal.unimed.ac.id/2012/index.php/cess/article/view/14893>, accessed March 5, 2024.