Advances in Social Behavior Research Vol.16 Issue 5 EWA Publishing
Available Online: 25 June 2025 DOI: 10.54254/2753-7102/2025.24455

The typification of infringement issues of humanoid robots: with special reference to the governance of infringement caused by learning algorithms

Xiaojun An

Department of Law, Shanxi University of Finance and Economics, Taiyuan, China

19722762891@163.com

Abstract. Humanoid robots possess technical features such as external human-like appearance, intelligence, and human-machine hybrid control. These may lead to the anthropomorphic trap, expanding the risk of infringement and complicating the attribution of liability. Different causes of infringement result in different types of infringement, which have different focuses in legal practice. Therefore, on the basis of clear classification standards, a typified discussion can be conducted. After dividing them into two major types: passive infringement and active infringement, further subdivisions can be made to clarify the nature and resolution of each type of infringement. Among the various types of infringement, the type caused by learning algorithms is the most distinctive due to its autonomous occurrence and difficulty in explanation. The method of law and economics can be utilized to allocate responsibilities among the relevant parties involved in the humanoid robot industry chain: humanoid robot manufacturers should follow the dynamic national regulations based on their development stage and different application scenarios under the guidance of the Hand Formula; users should be responsible for their negligent behavior due to failure to fulfill reasonable care obligations; and providers of general artificial intelligence models may be held jointly liable with humanoid robot product providers if they fail to fulfill the responsibility of transparency.

Keywords: humanoid robots, typified discussion, infringement caused by learning algorithms, responsibility allocation

1. Introduction

At present, China's humanoid robot industry has entered a stage of explosive growth. In 2023, the number of patent disclosures reached 2,903, and the market size of humanoid robots in China is expected to be approximately 2.76 billion yuan in 2024, exerting a significant impact on the economy and society. As pointed out in the "Guiding Opinions on the Innovative Development of Humanoid Robots" issued by the Ministry of Industry and Information Technology of China, humanoid robots are expected to become another disruptive product that profoundly changes human production and lifestyle, following computers, smartphones, and new energy vehicles, and will reshape the global industrial development pattern.

While humanoid robots are developing rapidly, the issue of their liability for infringement has also sparked extensive discussions in the academic community. As the AI Good Governance Academic Working Group has pointed out, humanoid robots, along with smart justice, autonomous driving, and the metaverse, have become core issues in the era of artificial intelligence. Among them, the civil legal liability of embodied intelligence is of paramount importance [1]. Currently, there are several urgent issues in this field that need to be addressed: first, the "debate on whether to establish a specialized governance system for humanoid robot infringement liability"; second, the lack of typified discussion and dissection of the complex issue of humanoid robot infringement, resulting in confusion regarding the legal application for different causes of infringement; third, the difficulty in allocating responsibilities among the relevant parties in the special issue of "infringement caused by the algorithm black box due to learning algorithm failure". This article will explore these issues to address the risks of the emerging data intelligence industry and provide clear guidance for its trustworthy development.

2. Technical characteristics of humanoid robots

To answer the "debate on whether to establish a specialized governance system for humanoid robot infringement liability", it is crucial to clarify the particularity of the infringement risks of humanoid robots, which necessitates sacrificing the universality

Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

and stability of the law to adapt and modify the "old law" to deal with the risks of new things. The particularity of the infringement risks of humanoid robots is derived from their technical characteristics. This article holds that humanoid robots possess typical technical features such as external human-like appearance, intelligence, and human-machine hybrid control. Humanoid robots with these technical features may trigger the anthropomorphic trap, expand the risk of infringement, and bring about difficulties in attributing liability among the relevant subjects after the occurrence of infringement. These issues should be important considerations in the legal liability system.

Firstly, humanoid robots have an external human-like appearance. Humanoid robots not only have human-like parts such as heads, limbs, and trunks but can also imitate human upright walking and physical functions such as grasping and picking up objects. This makes the movement of humanoid robots more flexible, expands their activity scenarios, and enables them to perform more complex human-like activities such as washing and dancing, thus broadening the application space of humanoid robots. With the further development of technology, humanoid robots are transforming into strong humanoid robots. Researchers are striving to add perception systems such as touch, hearing, and vision to robots, as well as features like variable body temperature and soft skin. The human-like features of humanoid robots increase the sense of closeness when humans interact with them, facilitating human-robot interaction and enhancing the sociality of robots, which is a unique functional advantage of humanoid robots [2].

Secondly, humanoid robots have intelligence. The realization of intelligence depends on the algorithms behind them, such as large language model machine learning technology, data collection and analysis, signal data transmission, and other complex artificial intelligence technologies [3]. The algorithms of humanoid robots can be divided into ordinary algorithms and learning algorithms. Ordinary algorithms are manually set by programmers and solve specific problems according to predetermined clear rules and logical steps. Although they have determinacy and explainability, they lack the ability to adapt and adjust to changing environments and lack decision-making autonomy. Learning algorithms, on the other hand, are algorithms that can automatically learn patterns and rules from data and use them for prediction, classification, or decision-making. Because they better meet the expectations of the public for the intelligence of humanoid robots, learning algorithms are now more widely applied in the programs of humanoid robots. However, while learning algorithms bring innovative outputs, they also bring "accidents", with the characteristics of being unpredictable and unexplainable [4].

Finally, human-machine mixed control. The intelligent program of humanoid robots and the user interact to achieve mixed control of the humanoid robot. Although humanoid robots have a certain degree of intelligence due to the embedded machine algorithms, this intelligence is not absolute, and humans still have control over them. Humans use humanoid robots through three steps: starting the robot, giving instructions to the robot, and the robot making decisions (acting or not acting) based on the instructions. Among them, the start of the robot is still controlled by humans, and in robots powered mainly by charging, humans also have the ultimate control means of "power off ". The intelligence of humanoid robots is mainly reflected in the second and third steps. Unlike the early human-robot interaction that often relied on simple methods such as buttons and indicator lights, humanoid robots can capture human body movements and even micro-expressions to receive commands and make decisions, and their interaction methods are gradually developing towards naturalization and intelligence.

The technical features of humanoid robots have brought about a series of new risks. First, it brings the trap of anthropomorphism. The external human-like features greatly increase the sense of closeness when humans interact with robots, making them easier to be accepted and trusted by humans; intelligence gives humanoid robots strong communication abilities, imitating the mental connection between humans in human-robot interaction, leading users to easily regard humanoid robots as entities with human thinking and emotions. In short, users will treat humanoid robots overly emotionally like real people, ignoring their non-human nature and limitations, making the boundary between humans and robots increasingly blurred. Second, it expands the scope of infringement risks. As mentioned above, humanoid robots with external human-like features participate in social life at a depth and breadth nearly equivalent to that of a social person. For example, unlike traditional robots that move by wheels or tracks, humanoid robots can walk upright, enabling them to go up and down stairs and enter and exit rooms; humanoid robots have joints and arms similar to those of real people, allowing them to grasp objects and open doors and cabinets; the application scenarios of humanoid robots may be expanded to various fields such as medical care, housekeeping services, errand running, and robot teachers. This not only expands the scope of infringement risks but also easily leads to the leakage of human privacy. Third, it causes difficulties in attribution of liability. The occurrence of the infringement by human-machine mixed control may be the result of both the user and the algorithm black box [5]. Moreover, humanoid robots are a combination of artificial intelligence systems, the Internet of Things, robot technology, and physical hardware. Some robot intelligent systems are even trained based on upstream general artificial intelligence models. This involves the distinction of responsibilities among hardware, software (including learning algorithms and general algorithms), service providers, and general artificial intelligence model providers.

3. Typification of infringement issues of humanoid robots

After clarifying the technical characteristics of humanoid robots and the new infringement risks they may bring, it is necessary to further discuss the various situations of liability for infringement caused by humanoid robots. This is because some infringements caused by humanoid robots have not escaped the scope of the traditional liability system for infringement. Different types of infringement behaviors have different focuses of legal disputes, and existing research lacks systematic sorting and clear classification standards on this issue. The author believes that the liability for infringement caused by humanoid robots can first be classified into two major categories from a macro perspective: passive infringement and active infringement. Subsequent classification can be made based on this.

3.1. Situations where humanoid robots passively infringe upon others' rights

First, the user's fault causes the humanoid robot to infringe upon others' rights. This situation can be further divided into intentional or negligent. For intentional acts by natural persons, for example, the user uses the humanoid robot to commit theft, murder, or damage property. In this case, the humanoid robot is similar to a tool in the user's hand, only a more advanced means. It does not have independent will and is merely a passive object under the user's control. The liability for infringement clearly belongs to the user and does not escape the traditional liability system for infringement. For negligent acts by natural persons, the tort law often adopts the standard of an ordinary person for judgment, and the setting of this standard is closely related to the degree of intelligence of the humanoid robot. However, China currently lacks classification standards for the degree of intelligence of humanoid robots. In the field of unmanned driving in China, the "Automotive Driving Automation Classification" (hereinafter referred to as the "Standard") has been issued, which classifies unmanned driving into six levels from L0 to L5 based on the degree of intelligence and automation of driving and stipulates the attention obligations of drivers at different levels. For example, in levels 1 to 2, the intelligent driving system is only an assistant, and the driving subject is still a human who needs to bear the main driving obligations for the road, route, and operation; in level 3, the driver only needs to take over the driving system when necessary; in levels 4 to 5, the driver does not need to intervene in the driving system, but the operating conditions of autonomous driving are different. Therefore, the field of humanoid robots can learn from the experience of the intelligent driving field in China and improve the classification standards for the intelligence level of humanoid robots.

Second, natural persons indirectly operate humanoid robots and infringe upon others' rights. This situation mainly includes cases where a third party (such as a hacker) tampers with the program or attacks the algorithm system, causing the humanoid robot to commit infringement. Whether the third party has the intention to use the humanoid robot to commit infringement or not does not affect the third party's liability for infringement. Because the infringement occurs ultimately due to the tampering of the originally normal program by the third party, which causes the humanoid robot to lose control and deviate from its original decision-making and actions. In short, the act of tampering with the program or attacking the algorithm system has a causal relationship with the subsequent infringement by the humanoid robot and meets the general elements of liability for infringement. However, in practice, it is often difficult to trace the attacker when an external attack occurs. At this time, the provider of the humanoid robot can be required to bear joint liability for failing to fulfill the obligation of ensuring network security, etc. [6].

Therefore, in the types of passive infringement by humanoid robots, the infringement is not caused by the intelligence of the humanoid robot's algorithm system but by the direct influence of the operator. The liability for infringement should be borne by the operator.

3.2. Situations where humanoid robots independently infringe upon others' rights

The situations where humanoid robots independently infringe upon others' rights can be classified into the following three categories:

The first category is the hardware defects of humanoid robots. Apart from the algorithm system, the humanoid robot itself is composed of extremely complex parts, including but not limited to mechanical arms, sensors, screws, scanners and other hardware facilities. If the infringement occurs directly due to the dropping or wearing of the equipment, product liability can be directly applied for handling.

The second category is the "algorithm failure" phenomenon of humanoid robots, but the cause of the failure is the ordinary algorithm defect of the artificial intelligence system behind the humanoid robot. Ordinary algorithm defects also exist in traditional intelligent systems (such as the lagging or unresponsiveness of smart phone systems), including but not limited to failure to respond to warnings, unresponsiveness of electronic control systems, user privacy leakage, and network security issues. The author believes that the ordinary algorithm flaws of humanoid robots can be treated in the same way as the hardware flaws of humanoid robots and subject to product liability. There are three reasons for this: First, the intelligent system software plays a core role in the movement, work, and decision-making of humanoid robots and may directly lead to accidents, so it is not

inappropriate to treat it as strict liability for product use; second, many of the software used by humanoid robots are sold on a large scale in the market, so they should be regarded as commercial software and treated as products. Because for commercial software, it has the characteristics of mass production and large-scale sales, and its producers are in a better position to control risks and have a stronger ability to share product accident costs [7]. This view is also adopted by the Uniform Commercial Code of the United States. Third, the essence of the intelligence of humanoid robots lies in the existence of artificial intelligence software, which is embedded in humanoid robots and shapes the core features and performance of this product. Therefore, the defects of the software in humanoid robots should be regarded as the product defects of the humanoid robots themselves.

In judicial practice, as a complex system, it is difficult for victims to prove the existence of product defects in humanoid robots. The Product Liability Directive (PLD) of the European Union points out that the probability of consumers of complex products losing lawsuits due to insufficient evidence is as high as 53% [8]. To solve this problem, the information disclosure rule can be introduced. Article 1222 of the Civil Code of the People's Republic of China stipulates that if medical institutions conceal or refuse to provide medical records related to disputes or lose, forge, tamper with, or illegally destroy medical records, it can be presumed that they are at fault. In the field of humanoid robots, a defect presumption based on information disclosure can also be set. For example, Article 9.1 of the PLD stipulates that when the plaintiff presents facts and evidence sufficient to support the reasonableness of their compensation claim, the defendant should disclose the relevant information they possess; otherwise, it can be presumed that the product has defects (Article 10.2). The Artificial Intelligence Act of the European Union also stipulates the mandatory information recording obligation of product safety components. Therefore, when humanoid robots cause infringement due to ordinary algorithm defects, if their manufacturers fail to fulfill their mandatory obligations or have information disclosure defects, it can be presumed that the product has defects and the manufacturers should bear product liability.

The third category involves infringement caused by the malfunction of learning algorithms in artificial intelligence systems, which leads to "algorithm failure" and results in "unforeseeable autonomous infringement by robots" that is most special and will be further discussed below. To meet human expectations for the high intelligence of AI products, developers continuously optimize machine learning algorithms to enhance the autonomy of humanoid robots. However, the higher the autonomy of humanoid robots, the more the unexplainability of the algorithm black box makes it impossible for people to predict, and even the developers themselves are powerless. At this point, the so-called "autonomous safety paradox" emerges: if too much emphasis is placed on the safety considerations of intelligent learning systems at the development and design stage and their no-fault liability is increased, it will inevitably lead to a conservative use of technology and hinder innovation; but if the responsibility is overly concentrated on the users, who are weak in professional knowledge, it will be difficult for them to complete the burden of proof, and developers may take the opportunity to refuse disclosure on the grounds of business secrets or unfavorable evidence, or even explain ordinary algorithm defects as unexplainable learning algorithms, making it impossible for users to seek redress. Article 3 of the "Interim Measures for the Administration of Generative Artificial Intelligence Services" in China states that "the relationship between safety and development must be balanced, and innovation and law-based governance must be combined" as the development principle.To address the "autonomous safety paradox" in the development of cutting-edge and complex technology industries and achieve a fair balance of responsibilities among all parties, it cannot rely solely on traditional abstract legal principles but must be supplemented by theories such as economic efficiency and cost-benefit analysis to find a balance point for all parties to assume responsibility and build systems based on this. In the humanoid robot industrial chain, the main parties involved are humanoid robot manufacturers, general artificial intelligence model providers, and humanoid robot users.

4. Responsibility allocation among relevant parties in infringement caused by learning algorithms of humanoid robots

4.1. Responsibility determination of humanoid robot product providers

We must recognize that no humanoid robot can completely eliminate all risks of infringement. Therefore, the goal of establishing an infringement liability system should shift from completely avoiding infringement to reducing the occurrence of infringement, which is a more practical goal [9]. This concept can be traced back to Ralph Nader's book "Unsafe at Any Speed", which discussed the obligations of vehicle manufacturers in the field of traffic accidents [10]. This book had a significant impact on the U.S. traffic accident liability system, and the mainstream U.S. case law requires vehicle manufacturers to fulfill a "reasonable duty of care" to avoid "unreasonable risks of personal injury", without the need to design perfect vehicles [11]. Therefore, when humanoid robot developers fulfill their reasonable obligations and reach the standard of a generally rational person, they do not need to bear responsibility.

The Hand formula proposed by U.S. Judge Learned Hand states that a potential tortfeasor is liable for negligence only if the cost of preventing the future accident (B) is less than the product of the probability of the accident (P) and the loss from the accident (L). In addressing the algorithm black box problem of autonomous infringement by artificial intelligence, the prevention

cost (B) includes the cost of developing explainable technologies, the cost of regular review and monitoring of algorithms, and the cost of training personnel to understand and manage algorithms, etc.; the probability of the accident (P) can be assessed by analyzing the historical data of the artificial intelligence system, calculating the frequency of infringement behavior, and considering factors such as the complexity and stability of the algorithm; the loss from the accident (L) can be quantified based on the possible economic losses, personal injuries, and reputational damages caused by autonomous infringement by artificial intelligence. Then, the prevention cost (B) is compared with the product of the probability of the accident (P) and the loss from the accident (L): if B is less than PL, then preventive measures should be taken and the developer needs to bear responsibility; If B is greater than PL, from the perspective of economic efficiency, it may not be necessary for developers to take excessive preventive measures. The calculation and assessment of specific costs, probabilities, and losses can be considered by relevant regulatory authorities from two aspects: the stage of technological growth and the field of technological application. From a vertical perspective, during the growth stage of humanoid robot technology, due to its immaturity, the probability of causing serious accidents is high, which will inevitably lead to a large product of P and L and high prevention costs. At this time, a lenient policy on the allocation of manufacturers' responsibilities should be adopted to support technological development. When it reaches the mature or decline stage, humanoid robots have rich application experience, making the product of P and L relatively low. At this point, the prevention cost B is often small, and legal regulations on technology can be strengthened to prompt manufacturers to produce safe products. From a horizontal perspective, different application fields of humanoid robots have different probabilities and hazards of causing infringement damages. Therefore, relevant authorities can adopt or expand or restrict the tort liability of humanoid robot manufacturers based on the different stages of humanoid robot technology development and different application scenarios (high-risk fields, ordinary-risk fields, and low-risk fields) to convey social policies, increase social net safety benefits, and guide intelligent technology to develop in a direction that conforms to human fundamental interests [12].

4.2. The responsibility of general artificial intelligence model providers

General artificial intelligence model providers are not necessarily humanoid robot manufacturers, and their tort liabilities should also be different. The author believes that the regulation of general artificial intelligence large models should adopt an inclusive and prudent attitude. There are three reasons for this: First, building a large model is no easy task, requiring the collection of a large amount of high-threshold data and the construction of an extremely complex model,which makes it very difficult to control the accuracy of the output results. If general artificial intelligence model providers are required to comply with completely safe and controllable technical standards, it is obviously too demanding. Second, the most significant feature of general artificial intelligence models is their universality, which is a key link in industrial development. If they are directly regarded as high-risk artificial intelligence, it may lead to the situation of discarding the baby with the bathwater. Third, humanoid robot manufacturers, as the downstream industry, are the true decision-makers regarding whether and how to use general large models. They integrate general artificial intelligence models into specific humanoid robot intelligent systems and directly bear the responsibility for risk control. Humanoid robot manufacturers can enhance their ability to control safety risks by restricting the usage scope of general artificial intelligence models, supplementing training data, modifying the source code and parameters of general large models in the open-source mode, etc. [13]. In fact, the Ministry of Industry and Information Technology of China proposed in 2023 the development direction of "taking the breakthrough of artificial intelligence technologies such as large models as the lead", demonstrating the country's positive attitude towards general artificial intelligence large models leading the development of the intelligent industry. As some scholars have pointed out, inclusive and prudent regulation promotes the combination of an effective market and a proactive government, providing new industries with necessary trial-and-error space while reserving the government's power to intervene appropriately based on the size of public risks [14]. This enables humanoid robots to develop in a regulated manner and be regulated in the process of development, achieving a dynamic balance between development and safety [15].

Therefore, this article holds that if general artificial intelligence model providers only provide libraries or Application Programming Interface (API) access for humanoid robot intelligent systems, at this time, the obligation to ensure product safety and controllability should be fulfilled by the humanoid robot providers. However, general artificial intelligence model providers need to fulfill certain transparency obligations, such as providing detailed information about the general artificial intelligence model to humanoid robot manufacturers, explaining the application scenarios and potential safety risks of the model, etc., allowing humanoid robot manufacturers to choose whether to use or to what extent to use this model. When the provider of general artificial intelligence models fails to fulfill the responsibility of transparency, or when the manufacturer of humanoid robots has designed the product based on the safety scope defined by the general artificial intelligence model but still causes damage beyond the risk notification, it can be reasonably inferred at the legal level that the provider of the general artificial intelligence model has not fulfilled the responsibility of transparency. In such a situation, the provider of the general artificial intelligence model and the provider of the humanoid robot should be jointly held liable, to ensure the rationality and fairness of liability determination, protect the legitimate rights and interests of relevant parties, and promote the standardized development of the technology application and product manufacturing fields.

4.3. The responsibility of users of humanoid robots

Under the technical architecture of human-machine mixed control, due to the interaction between the system's autonomous learning mechanism and human behavior, the occurrence of infringement risks often involves both the technical factor of the algorithm black box and the human factor of the user's fault. For example, humanoid robots may have incorrect learning under the user's control and thus cause infringement. As highly intelligent products, humanoid robots are often equipped with adaptive artificial intelligence systems that continuously record data and learn during operation, and adjust the algorithm rules in a timely manner. If the intelligent system of a humanoid robot is fixed at the time of sale, not only will its ability to adapt to various environments be reduced, but it will also fail to meet the public's expectations for its intelligence. In fact, adaptive artificial intelligence has long been applied in the field of autonomous driving: for example, Tesla's shadow mode continuously simulates decisions and compares them with the driver's actual operations. Abnormal data that does not match will be determined by the system as "extreme conditions" to facilitate the vehicle system's correction. In other words, the user of the robot plays the role of a teacher, and the data source of the intelligent system includes both the innate data from the trainers at the time of product manufacture and the acquired data from the user during use.

At this point, when allocating the responsibility between the provider of the humanoid robot and the user, it should be confirmed: first, whether the user has engaged in "malicious teaching". As stipulated in Article 56 of the EU's "Proposal for a Regulation on Civil Law Aspects of Robotics", the responsibility of each party should be proportional to their relative levels of control over the robot's instructions and the robot's actual degree of autonomy. For humanoid robots with strong learning ability and autonomy, if the user conducts long-term and high-density bad training on the humanoid robot, the user becomes the party with more control over the infringement and should bear strict liability [16]; second, the inducing cause of the infringement. The party that triggers the infringement is responsible for the damage. However, it is not easy to determine the cause of the infringement in judicial practice. Therefore, it is very necessary to design a device similar to the "black box" in aircraft in humanoid robots to record detailed information such as the robot's movement trajectory, speed, time, executed program, human control and learning algorithm control status, and accident conditions. While the humanoid robot manufacturer retains the relevant data information, a third-party regulatory agency can also conduct algorithm testing and auditing [17] to clarify the legal facts related to the infringement. If both the provider of the humanoid robot and the user have caused the system to record incorrect data and it is impossible to determine which error led to the infringement, the principle of causal presumption can be referred to. For example, Article 4.1 of the AILD (Artificial Intelligence Liability Directive) proposal stipulates that if the plaintiff can prove that the original intelligent system caused the damage, there is no need to prove the causal relationship between the defendant's fault and the damage.

5. Conclusion

After clarifying the technical features of humanoid robots as a new thing and the potential infringement risks they may bring, the author believes that the infringement issues of humanoid robots can be divided into two major types: passive infringement of others' rights and autonomous infringement of others' rights. In the former type, the infringement behavior is caused by the direct influence of the operator, so the responsibility should be borne by the operator; in the latter type, if the cause of the infringement is due to hardware defects or ordinary learning algorithm defects, product liability can be applied; the learning algorithm infringement type is more complex, and the responsibility allocation can be carried out by combining the methods of legal economics:

First, humanoid robot manufacturers, under the guidance of the Hand formula, should follow the dynamic national institutional norms according to their development stage and different application scenarios. Second, users and victims should be responsible for their negligent behavior of not fulfilling reasonable care obligations. Third, if the provider of the general artificial intelligence model fails to fulfill the transparency responsibility, or if the humanoid robot manufacturer has designed the product based on the safety scope defined by the general artificial intelligence model but still causes damage consequences beyond the risk notification, they constitute joint infringement with the provider of the humanoid robot product. In conclusion, the infringement of humanoid robots is a complex issue, and the further realization of its substantive justice still requires continuous exploration in theory and practice.

References

[1] AI Good Governance Academic Working Group. (2025). Continuation and new chapter: Observations on China's AI rule of law research in 2024. *Legal Application*, *3*, 146-166.
[2] Yu, H. Z., & Feng, X. M. (2010). The development and current situation of humanoid robot technology. *Mechanical Engineer*, *7*, 3-6.
[3] Ji, W. D. (2019). The concepts, laws and policies of artificial intelligence development. *Oriental Legal Science*, *5*, 5-6.
[4] Shen, W. W. (2019). The myth of algorithmic transparency: A critique of algorithmic regulation theory. *Global Law Review*, *6*, 20-39.
[5] Shen, W. W. (2024). The dilemma and response of the accident liability system for humanoid robots. *Oriental Legal Science*, *3*, 88-100.

[6] Xie, L. (2024). Liability determination for autonomous infringement by humanoid robots. *Oriental Legal Science*, *3*, 77-81.
[7] Ding, L. M. (2010). Legal thoughts on including commercial software in the scope of product liability objects. *Journal of Dalian Minzu University*, *4*, 361-363, 366.
[8] European Commission. (2018). *Commission staff working document evaluation of product liability directive* (SWD(2018)157). https: //eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD: 2018: 157: FIN
[9] Choi, B. H. (2019). Crashworthy code. *Washington Law Review*, *94*(1), 39-91.
[10] Nader, R. (1965). *Unsafe at any speed*. Grossman.
[11] Larsen v. General Motors Corp., 391 F.2d 495 (8th Cir. 1968).
[12] Zhang, J. S. (2021). The concept of a community with a shared future for mankind from the perspective of a risk society. *Journal of Shanghai Jiao Tong University (Philosophy and Social Sciences Edition)*, *6*, 93-101.
[13] Liu, J. R. (2024). New risk and regulatory framework for generative artificial intelligence large models. *Administrative Law Review*, *2*, 28-32.
[14] Liu, Q. (2022). The legal logic of inclusive and prudent regulation from the perspective of digital economy. *Chinese Journal of Law*, *4*, 37-51.
[15] Liu, Q. (2024). An exploration of the rule of law that emphasizes both the development and security of artificial intelligence: A case study of humanoid robots. *Oriental Legal Science*, *5*, 32-42.
[16] Bertolini, A., & Episcopo, F. (2021). The expert group's report on liability for artificial intelligence and other emerging digital technologies: A critical assessment. *European Journal of Risk Regulation*, *12*(3), 644-659.
[17] Ding, X. D. (2020). On the legal regulation of algorithms. *Social Sciences in China*, *12*, 152-159.