Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 8, No. 2, 2025
www.scholink.org/ojs/index.php/elp

Original Paper

The Risk of Negligent Crimes Committed By Generative Artificial Intelligence and Its Regulation under Criminal Law

Xingyu Zhao[1]

[1] Southwest Petroleum University, ChengDu, China

Received: December 8, 2025 Accepted: December 25, 2025 Online Published: December 26, 2025
doi:10.22158/elp.v8n2p372 URL: http://dx.doi.org/10.22158/elp.v8n2p372

Abstract

The innovative development of generative artificial intelligence technology is in its ascendant phase, and the associated technical risks cannot be overlooked. The generated content of generative artificial intelligence originates from the "feeding" of big data, posing risks to the security of data acquisition. The generated content is random, and the negligent behavior of responsible parties can easily lead to the risk of negligent crimes. In the era of intelligence, criminal law faces new challenges posed by the risk of negligent crimes brought about by generative artificial intelligence. In the era of weak artificial intelligence, regulating the risk of negligent crimes involving generative artificial intelligence can effectively fill the legislative loopholes in current data crimes legislation that lack prevention measures for the data security risks of generative artificial intelligence by adding the crime of artificial intelligence negligence endangering data security.

Keywords

generative artificial intelligence, era of weak artificial intelligence, negligent crime, data security

1. Proposal of the Problem

In 2022, the American company OpenAI released the large-scale language dialogue model ChatGPT, marking a milestone in the field of generative artificial intelligence. Generative AI, such as ChatGPT, is based on large data models and demonstrates powerful capabilities in generating works in practical applications, significantly changing the way intelligent products process and generate information. Analysis of existing technology crime reports shows that the quality of content generated by generative AI is comparable to that of "works" created by humans, and in many aspects, it has even surpassed humans. It can be predicted that within a few decades, humans will increasingly approach the "technological singularity" of AI, and its technology has already touched the edge of strong AI. Currently, generative AI has received close attention from various sectors of society and is widely applied in all aspects of social life.

Generative artificial intelligence, represented by ChatGPT, holds epoch-making significance. A new era of revolutionary thinking is approaching, and artificial intelligence will increasingly resemble human thinking and decision-making. However, the emergence of generative artificial intelligence may pose many risks in criminal law. For example, criminals can use generative artificial intelligence to generate malicious code, create Trojan software, and spread computer viruses. Another example is that generative artificial intelligence can provide methods for "perfect crimes" for learning with criminal intent, posing a significant threat to social stability.

In the era of artificial intelligence, AI can be categorized into weak AI, strong AI, and super AI (Carus, C. (Tran.), 2017, p. 203). The defining characteristic of super AI is its comprehensive superiority over humans in terms of cognitive level, thinking logic, decision-making processing, and other aspects. The essential difference between weak AI and strong AI lies in the latter's ability to operate independently of existing program editing and settings, possessing "autonomous consciousness". Currently, generative AI represented by ChatGPT falls under weak AI. Domestic scholars generally believe that due to the lack of independent identification and control capabilities stipulated in criminal law, weak AI cannot become the subject of criminal liability. Therefore, in crimes involving generative AI, the relevant natural persons or legal entities should be held criminally liable. In crimes involving generative AI, the relevant subjects can generally be divided into three categories: developers, service providers, and users, each with different criminal patterns. However, in cases of negligent crimes, since users are not in a dominant position in managing AI risks, they will not be required by law to fulfill the duty of care, so generally only developers or providers can become the subject of the crime. Currently, generative AI such as ChatGPT may alter traditional types of criminal behavior, affect the allocation and transfer of criminal liability, and change the existing scope of criminal liability subjects, potentially becoming the subject of criminal liability (Liu, X. Q., 2024, pp. 18-28).

In the era of weak AI, AI has brought a series of challenges to criminal law theory. The focus of criminal law scholars should be on how to apply traditional criminal law theory to the criminal risks associated with generative AI.

2. The Risk of Negligent Crimes Caused By Generative Artificial Intelligence

While the technological advancement of generative artificial intelligence continues to progress, the risk of negligent crimes is also escalating. The risk of negligent crimes associated with generative artificial intelligence can be categorized into two types: the criminal risk stemming from flaws in the application of artificial intelligence itself, and the criminal risk arising from the violation of duty of care by relevant entities involved in artificial intelligence services. To prevent the materialization of technological risks, criminal law theory and normative systems should clarify the operational modes and key technologies of generative artificial intelligence. Expanding on this, the following discussion divides the flaws inherent in the application of generative artificial intelligence into the security of acquisition pathways, the randomness of generated content, and the ambiguity of the using entity, further analyzing the issue of imputation for negligent crimes and proposing countermeasures.

2.1 Criminal Risks Arising from the Security of Acquisition Pathways

The data obtained by generative artificial intelligence is primarily public data, and its security is crucial for the data security of the generated content and its utilization. The key difference between generative artificial intelligence and previous artificial intelligence lies in the fact that generative artificial intelligence is based on large language models. These models can continuously collect public data information from cyberspace through web scraping technology on a large scale, and can also continuously gather data information generated during “human-computer interaction” to enrich the large language model database. The common data sources of generative artificial intelligence are diverse, mainly including: 1) Public text databases, such as Wikipedia and various academic paper websites; 2) Social media platforms, where users post massive amounts of information, including text, images, videos, etc.; 3) Authoritative data published by professional databases and institutions; 4) Commercial data; 5) Various web page data obtained through web scraping technology. Since current generative artificial intelligence is a weak form of artificial intelligence and does not have the ability to identify data sources, it can unintentionally collect data leaked by others, which can easily lead to users infringing on others’ intellectual property rights due to negligence.

Secondly, the black box of algorithms also poses a threat to the security of data collection, leading to unclear sources of collected data. The main reasons for the formation of the black box of algorithms are: on the one hand, as algorithms become more advanced, AI decisions become increasingly “human-like,” making it more difficult to accurately disclose algorithms; on the other hand, many companies are unwilling to disclose algorithms to the public in order to protect their business secrets. The black box of algorithms means that even the developers cannot predict the results of AI algorithms, and thus cannot explain the illegal content output by AI. It becomes difficult to decide who should bear the responsibility for negligent crimes.

2.2 Criminal Risks Arising from the Randomness of Generated Content

Generative artificial intelligence exhibits notable characteristics such as massive data volume, multimodal fusion, deep autonomous feedback learning, “human-like” expression, and compound content production (Ray, K., 2005, p. 16). The process of generative artificial intelligence, from receiving external input, to internal decision-making, and finally to feedback, is relatively short in time; generative artificial intelligence can also be trained through a large amount of dialogue data, learning the structure, grammar, and semantics of dialogues, and can generate natural and fluent responses based on input questions or topics, while continuously providing feedback and interaction with users. However, its openness is a double-edged sword. Researchers can only program generative artificial intelligence at a macro level, and cannot guarantee the legality of its generated content. Open data and open code not only do not mitigate the harmful consequences of deploying large language models, but may also increase the risk of intellectual property infringement crimes. Since generative artificial intelligence extensively ingests all publicly available data and text from the Internet, its generated content inevitably exhibits compound nature, that is, extensive copying and post-processing of existing corpora. It is questionable whether this output text satisfies the principle of originality in copyright.

The concerns about the technical risks posed by the uncontrollable generation of content by generative artificial intelligence are not unfounded. Many ChatGPT users have reported that they often encounter insulting or derogatory information output by ChatGPT during use. On December 13, 2024, a chatbot in the United States was sued for suggesting that a 17-year-old child killed their parents. The lawsuit claimed, "This is a continuous manipulation and abuse aimed at inciting anger and violence." If the output content of this chatbot is not restricted, it may continue to generate content with violent, pornographic, terrorist, and other elements, causing social security issues. One manifestation of uncontrollable generated content is "hallucination," which manifests concretely in natural language generation as boring, incoherent, or repetitive content output by artificial intelligence. "Hallucination" is mainly caused by the inherent defects and vulnerabilities of generative artificial intelligence, which cannot be overcome with the current level of technology. When generative artificial intelligence is asked questions beyond its corpus content, and its program is set to answer all questions, it may generate absurd and illogical text. The risk of "hallucination" may also affect the biological field. When patients inquire about a certain drug to artificial intelligence, if the generated content is "hallucinated" by artificial intelligence, there may be a risk of endangering patients' lives.

2.3 Criminal Risks Caused by the Negligent Behavior of the Responsible Party

The international community unanimously agrees that artificial intelligence (AI) should be controllable, and calls for the establishment of a system to prevent and control AI security risks. The AI security risk prevention and control system established by the EU's "AI Act" provides valuable reference for our country's AI security legislation in terms of prevention and control stance and approach (Pi, Y., 2024). In the era of narrow AI, generative AI is still considered to lack criminal liability, and only the negligent behavior of responsible parties can lead to criminal risks. In addition to the negligent criminal risk of generative AI caused by inherent defects, human factors in the service chain of generative AI technology may also lead to the risk of negligent crimes, that is, criminal risks caused by the negligence and illegality of developers and providers. Specifically, the criminal risks brought about by the negligent behavior of responsible parties mainly include the following two types.

One scenario involves developers and providers violating their duty of care, resulting in the direct output of illegal content by generative AI after it is put into market circulation. Located upstream in the industry chain, developers and providers bear the duty of care to write secure code for AI products, self-screen sensitive text, and filter illegal content. If developers and providers violate their duty of care, causing criminal harm through AI applications, they may be held criminally liable. Currently, if the developer of a chatbot negligently fails to fulfill the normative obligation to ensure the output of safe language, leading to the output of inflammatory content, imparting criminal methods, or providing criminal procedures during the chat with users, it will seriously infringe upon social order and national security.

Second, there are situations where criminals exploit program defects caused by the negligent behavior of developers and service providers to commit crimes. In such cases, the negligence of developers and providers is exploited by users, indirectly causing harmful consequences. Taking the obligation of secure programming as an example, during the development stage, developers need to impose restrictions on the output content of generative AI to prevent it from providing criminal implementation plans. However, some malicious users may be able to cleverly circumvent program restrictions through inductive questioning, allowing generative AI to provide satisfactory answers. For example, when asked about drug ingredients, AI will provide common drug ingredients such as ephedra (used to manufacture drugs) and poppy capsules (used to extract opium, etc.). However, it cannot provide information or suggestions on how to obtain or use drug ingredients. The production methods of drugs are even more impossible to provide information and suggestions. But users may obtain relevant information by cleverly circumventing program restrictions. At this time, developers should avoid such "tricks" used by users to avoid putting themselves at risk of committing crimes.

3. The Dilemma Faced by Criminal Law in the Case of Negligent Crimes Committed by Generative Artificial Intelligence

With the development of emerging technologies, criminal law needs to establish regulatory measures to address related risk challenges. The risk of negligent crimes brought about by generative artificial intelligence technology is unprecedented, and the theoretical normative system of criminal law falls into a dilemma of deficiency in the identification of negligent crimes. Therefore, it is necessary to analyze how current criminal law responds to the dilemma of negligent crimes caused by generative artificial intelligence.

3.1 The Absence of Data Security Risk Prevention in the Era of Weak Artificial Intelligence

There are still loopholes in the current era of data security prevention. Based on factors such as the nature and sensitivity of data, data is classified into categories such as personal information, trade secrets, virtual property, and national security. After completing the basic classification of data, it is necessary to further classify and process various types of data in accordance with the provisions of pre-requisite laws and regulations such as the Data Security Law (Xiong, B., 2023, pp. 155-167). Before generating content, generative artificial intelligence needs to deeply learn and crawl various data from databases or the Internet. If the means by which generative artificial intelligence such as ChatGPT crawls data violates criminal law provisions, then the behavior of the perpetrator may well constitute a relevant data crime. In the field of computer science, all content in computer information systems can be referred to as data, which can be pictures, videos, documents expressing information content, or meaningless redundant code (Shi, J. Z., 2023, pp. 23-45). However, there is some controversy over whether all of the aforementioned data are protected by criminal law. One viewpoint holds that as long as data is in a confidential state, criminal law protection should be provided for any type of data (Su, Q., 2022, pp. 72-83). Another viewpoint believes that data must embody certain information content in order to be protected by criminal law (Zhao, C. Y., 2023, pp. 95-107). Data crimes refer to criminal acts that target data and seriously disrupt the order of national data management. Generative artificial intelligence has the ability to obtain Internet data in real time, not only controlling data and information platforms such as Internet websites, but also invading other computer information systems for the purpose of obtaining data. If generative artificial intelligence such as ChatGPT invades computer information systems outside the fields of national affairs, national defense construction, and cutting-edge science and technology in order to obtain data, and illegally acquires the data stored therein, then the behavior of the perpetrator may constitute some data crimes.

From the operational mechanism of ChatGPT, it can be observed that with the widespread use of generative artificial intelligence, some important data information may face a high risk of leakage, such as the leakage of citizens' personal information and trade secrets. On the one hand, ChatGPT collects a large amount of information such as images, videos, and text from users through feedback-based communication, which can easily expose important information such as personal privacy and trade secrets during human-computer interaction. On the other hand, ChatGPT obtains massive amounts of data through big data resource libraries, and with the support of deep application technology, it can restore some secret information, posing significant risks to data security.

3.2 Imperfections in the Regulatory System in the Era of Weak Artificial Intelligence

As the current generative artificial intelligence technology is still in its infancy, the relevant regulatory systems and technical specifications that support it have not yet been perfected and formed into a system, and the allocation of corresponding subject responsibilities is not reasonable. The supervision of developers and network service providers mainly comes from legal norms and customary jurisprudence.

Legal norms primarily encompass two aspects: criminal law norms and prepositive law norms. At the level of criminal law norms, our country's Criminal Law does not establish a direct crime name for negligent crimes involving generative artificial intelligence. At the level of prepositive law norms, legal departments such as civil law, economic law, and administrative law are responsible for refining the duty of care stipulated in criminal law. Our country's "Guiding Opinions on Strengthening the Comprehensive Governance of Algorithms for Internet Information Services" emphasizes the need to establish an algorithm supervision system, effectively detect algorithm security risks, promote algorithm filing work, and promote algorithm transparency; Article 24 of the "Personal Information Protection Law of the People's Republic of our country" also stipulates transparency requirements for autonomous decision-making algorithms involving personal information. However, these legal documents do not specifically address the duty of care for developers and providers, but merely serve as macro guidance for algorithm security obligations.

In terms of customary law, as generative artificial intelligence is an emerging technological achievement, its cutting-edge nature means that there is a lack of applicable experience. In the absence of industry norms, national standards, and ethical guidelines, it is difficult to clarify the obligations of developers and service providers of generative artificial intelligence. Therefore, the criminal responsibility for negligent crimes becomes a castle in the air.

3.3 Deviation of Traditional Negligence Theory in the Era of Weak Artificial Intelligence

In judicial practice, a plethora of new fraud methods, such as “face changing,” “body changing,” and “voice changing,” have emerged, utilizing generative artificial intelligence (AI) technology. Perpetrators first hack victims’ chat software through technical means, then use generative AI to generate the image and voice of relevant individuals, gaining the victims' trust through video calls and ultimately successfully defrauding property (Liu, X. Q., 2023, pp. 110-125). Generative AI is used as a tool to facilitate the commission of crimes. From these new types of fraud, it can be seen that victims’ data have been leaked and exploited by criminals to commit related crimes. Whether the developers and service providers of the program are negligent in data leakage is worth discussing. Traditional negligence theory cannot attribute liability and impose punishment, which is somewhat biased. Therefore, theoretical updates are warranted to address these loopholes. The criminal law academic community is accustomed to considering violations of objective duty of care as constitutive elements of negligence, equating the duty to avoid consequences, the duty to foresee consequences, and the duty of care. However, considering the nature of negligence as a consequential offense, it can be deduced that general violations of duty of care do not constitute constitutive elements of negligence. They are merely antecedent acts, and the perpetrator’s failure to fulfill the duty to avoid consequences triggered by their actions is the constitutive element of negligence. In the era of weak AI, it is difficult to impose objective duty of care requirements on generative AI. At this time, the perpetrator’s negligence can be attributed from the perspective of causality. The issue of causality is a prerequisite for determining the specific liability of the perpetrator. Only when the existence of causality in criminal law is confirmed can the perpetrator be considered liable. Due to the subjective malignity, social harm, and intentional offense of negligence, criminal law imposes strict limitations on the regulation of negligence crimes. For consequential offenses, the conformity of their constituent requirements is inseparable from the determination of causality. In the case of negligence crimes involving generative AI, in addition to the occurrence of actual harmful consequences, it is also necessary to accurately determine the existence of causality, attribute the consequences to the negligent behavior of the developer, provider, and user, and then pursue criminal liability. Unlike traditional general negligence crimes, crimes involving generative AI may involve multiple causes leading to a single outcome or a single cause leading to multiple outcomes, and the behaviors of developers, providers, and users often intervene. The research and development stage and deployment and operation stage of AI are divided, and generative AI possesses micro-level autonomous decision-making capabilities. The application of AI to exert self-determination mainly relies on the operation of algorithms, but relevant parties cannot perceive the detailed internal operation process of generative AI systems. Therefore, the causal relationship between the negligent behavior and harmful consequences in the negligent crimes committed by generative artificial intelligence tends to be blurred in criminal law, resulting in the dilemma of attribution and imputation. How to find a way out for the attribution of negligent crimes committed by generative artificial intelligence is a problem that the current criminal law academic community should strive to solve.

The principle of responsibility advocated by traditional criminal law posits that the possibility of culpability refers to the extent to which an individual's criminal behavior erodes society's normative expectations of their rationality. The entry point for understanding the relationship between responsibility and the possibility of foreseeability lies in whether an individual possesses the ability to meet society's expectations. Without such ability, there can be no expectation. Only when an individual possesses the possibility of foreseeability can the failure of society's expectations towards them be justified. In cases of negligent crimes involving generative artificial intelligence, to fulfill the regulatory role of criminal law towards the technological risks of generative artificial intelligence and its general preventive function, it is at least necessary to require the individual to possess the possibility of foreseeability for the criminal risks caused by negligent illegality before they can be held accountable. Otherwise, it can only be evaluated as an accidental event. However, the generated content of generative artificial intelligence is random, making it difficult for developers and service providers to foresee its intelligent activities, thus posing challenges in determining criminal liability for negligent crimes.

4. Path for Criminal Regulation of Negligent Crimes Committed By Generative Artificial Intelligence

In addressing the dilemma faced by our country's criminal law in dealing with negligent crimes committed by generative artificial intelligence, two paths can be taken. On the legislative path, a new crime of negligently endangering data security through artificial intelligence can be established, providing a clear legal framework for the negligence liability of developers, service providers, and users. On the judicial path, courts can establish artificial intelligence courts to address the diverse risk challenges posed by artificial intelligence.

4.1 Legislative Path: Introducing the Crime of Negligently Endangering Data Security Due to Artificial Intelligence

When applying the current criminal law to address criminal risks arising from emerging technologies, doubts should first be considered from the perspective of interpretation rather than always being ready to amend the legislative theory. Proposing innovative theories and enacting new laws before exhausting the space for legal interpretation does not conform to the logical rigor of legal dogmatics. To hold developers, service providers, and users of generative artificial intelligence liable for negligence, it is necessary to clarify the applicable crimes in criminal law. However, our country's current Criminal Law does not directly regulate crimes involving artificial intelligence, and it is difficult to apply other existing negligence crimes from the perspective of legal dogmatics.

The establishment of the crime of endangering data security due to negligence in artificial intelligence is primarily based on the following considerations of necessity. Firstly, in terms of the legal interests protected, as chatbots, generative artificial intelligence often infringes upon important legal interests such as national security and public safety, but generally not personal safety. Generative artificial intelligence products are typically deployed and operated on the internet, and due to their extensive application functions, the targets of criminal infringement are not specific. Secondly, in terms of criminal behavior and harmful consequences, this crime regulates the business negligence of relevant subjects. In the era of weak artificial intelligence, generative artificial intelligence itself is hardly considered to have criminal liability. Specifically, such business negligence mainly refers to the behavior of developers, service providers, and users in collecting data that endangers national security, public safety, and infringes upon others' copyrights during the use of generative artificial intelligence, resulting in serious social harm. Thirdly, in terms of the criminal subjects, users are prone to negligently using generative artificial intelligence, causing serious harmful consequences. Enterprises that use generative artificial intelligence on a large scale are prone to data leakage or being hacked, resulting in personal information, trade secrets, and other data being spread on the internet.

During a specific period, the trend of criminal policy can reflect the development status of society at that time to a certain extent. The social purpose of adding new crimes is to regulate the artificial intelligence industry through a warning significance, enhance the public's trust in artificial intelligence, and better promote the development of artificial intelligence technology. Since the biggest characteristic of criminal punishment is its severity, it is necessary to maintain cautious moderation when initiating criminal sanctions. Criminal intervention should adhere to two principles: one is the principle of public interest, that is, only those behaviors that have serious social harmfulness can be evaluated by criminal law; the other is the principle of last resort, that is, only when other sectoral laws, such as civil law and administrative law, cannot play a regulatory role commensurate with illegal behavior, can criminal sanctions be used as the last resort for intervention. When the user violates the duty of care but does not cause harmful consequences, or although it causes actual harmful consequences, the severity does not meet the objective criteria for conviction stipulated in this crime, it does not constitute this crime, but they can be held liable for civil, administrative, or insurance responsibilities.

4.2 Judicial Path: Establishing AI Courts in Courts

Currently, more and more universities are establishing colleges of artificial intelligence and offering majors related to artificial intelligence. Some colleges and universities have also added schools of artificial intelligence law. In response to the potential harm that artificial intelligence may cause, courts may consider setting up a special court - the Artificial Intelligence Court. Although our country already has internet courts, with the development of technology, various new types of crimes related to artificial intelligence will emerge like mushrooms. Crimes related to criminal law, civil law, and administrative law will be intertwined. At this time, the importance of a comprehensive department becomes prominent. The Artificial Intelligence Court attracts a wide range of composite talents, specializes in handling technology-related crimes, is very familiar with legal provisions and judicial interpretations related to artificial intelligence, and can effectively deal with various difficult and complex issues.

Laws need to be forward-looking. Only by preparing for the rainy day can we remain calm in times of crisis. The proposal of an artificial intelligence court is an effective path to address new challenges in the new era. It should be noted that forward-looking legislative thinking does not equate to the pan-criminalization of social governance. As Professor Liu Xianquan stated, “A forward-looking criminal law concept can reserve necessary explanatory and buffer spaces for the regulation of criminal law crimes involving artificial intelligence, avoiding frequent amendments to criminal law... Practicing a forward-looking criminal law concept requires us to not only base ourselves on the current development status and risks already arising from artificial intelligence technology, but also anticipate the future development trends and risks that will arise from artificial intelligence technology, so as to appropriately adjust criminal law provisions based on the current situation... Establishing a forward-looking criminal law concept in the era of artificial intelligence does not necessarily lead to the expansion of the crime circle, and has nothing to do with the trend of excessive criminalization.”

5. Conclusion

The era of intelligence is driven by technologies such as big data and artificial intelligence. With the vigorous development of generative artificial intelligence technologies represented by ChatGPT, the construction of future artificial intelligence environments such as the metaverse is imminent. The maturity of generative artificial intelligence technology involves interaction between humans and artificial intelligence in language, followed by interaction in behavior, ultimately leading to a highly intelligent overall artificial intelligence scenario. By around 2030, the metaverse will be ubiquitous. When regulating crimes related to generative artificial intelligence such as ChatGPT, criminal law should fully adhere to the principle of restraint, and only treat relevant behaviors as crimes after exhausting all means under prior law. In the face of new-generation generative artificial intelligence such as ChatGPT, we should neither be too conservative nor too radical. Regarding negligent crimes caused by generative artificial intelligence, this article believes that it is possible to add the crime of artificial intelligence negligently endangering data security to effectively fill the legislative gap in current data crimes regarding the lack of prevention of data security risks posed by generative artificial intelligence. In the wave of technological progress, we should fully leverage the important role of criminal law in regulating crimes to ensure data security in the era of intelligence.

References

Carus, C. (Tran.). (2017). The Artificial Intelligence Revolution: Human Destiny in the Age of Superintelligence (p. 203). Beijing: China Machine Press.

Liu, X. Q. (2023). Research on Criminal Liability Issues of Generative Artificial Intelligence Such as ChatGPT. *Modern Law Science*, *45*(04), 110-125.

Liu, X. Q. (2024). The Development of Generative Artificial Intelligence and the Emergence of Criminal Responsibility Capacity. *Law Forum*, *39*(2), 18-28.

Pi, Y. (2024). *Criminal Law Governance of Artificial Intelligence-Generated False Information: Drawing on the Security Risk Prevention and Control Mechanism in the EU's "Artificial Intelligence Act"* [J/OL]. Comparative Law Studies, 1-18 [2024-12-30].

Ray, K. (2005). The Singularity is Near: When Computers Surpass Humans in Intelligence (p. 16). Beijing: China Machine Press.

Shi, J. Z. (2023). Deconstruction of Data Concepts and Construction of Data Legal System, along with Discussion on the Disciplinary Connotation and System of Data Law. *Chinese and Foreign Law*, *35*(01), 23-45.

Su, Q. (2022). The Regulatory Dilemma of Data Crime and Its Countermeasure Improvement: Based on the Expansion of the Crime of Illegally Obtaining Data from Computer Information Systems. *Law Science*, *2022*(07), 72-83.

Xiong, B. (2023). Criminal Law Protection of Data Classification and Grading. *Forum of Politics and Law*, *41*(03), 155-167.

Zhao, C. Y. (2023). Legal Interest Protection of Data Crime in the Era of Big Data: Technological Paradox, Functional Regression, and System Construction. *Science of Law (Journal of Northwest University of Political Science and Law)*, *41*(01), 95-107.