Law and Humanities
ISSN Print: 3079-5117
ISSN Online: 3079-5125
https://doi.org/10.63313/LH.9015

Research on the Legal Protection of the Right to be Forgotten in the Context of the Era of Artificial Intelligence

Xianjun Tan
School of Law, Anhui University of Finance and Economics, Bengbu 233000, China
Email: 2371566835@qq.com

How to cite this paper: Tan, X. (2025). Research on the Legal Protection of the Right to be Forgotten in the Context of the Era of Artificial Intelligence. Law and Humanities, 1(2), 55-64. ISSN Print: 3079-5117; ISSN Online: 3079-5125.
https://doi.org/10.63313/LH.9015
Published: 2025-06-24

Abstract

While artificial intelligence technology has changed the production mode of hu-man society, it has also exacerbated the occurrence of personal information in-fringement. Deletion of personal information is an important manifestation of the right to be forgotten and an important way to protect the right to personal information. However, in the context of generative AI, the realization of the right to be forgotten faces both technical and institutional dilemmas, and it is difficult to implement both the current law and the traditional technology of deleting personal information. In order to strengthen the protection of the right to be forgotten, based on the "inclusive and prudent" legal policy, further standardize data collection, expand the interpretation of "deletion", and strengthen the ad-ministrative supervision of the process of generative AI processing personal in-formation. Through the above measures, a balance between the protection of the right to be forgotten and technological development can be achieved.

Keywords

Artificial Intelligence; Generative AI; Right to be Forgotten; Personal Information

1. Introduction

Generative Artificial Intelligence (hereinafter referred to as "generative AI"), as a new paradigm in the development of artificial intelligence technology, is gradually applied to various fields. According to the World Bank's Generative AI Report, the generative AI market is expected to grow to $6.5 billion by 2026, growing at a CAGR of 34.9%, making generative AI a high-speed engine for the growth of the digital economy.[1] Among them, DeepSeek, an artificial intelligence company in China, has attracted attention with breakthrough innovation based on the advantages of low cost, high efficiency and localization. Less than three months after DeepSeek released the AI model R1 on January 20, 2025, hundreds of A-share listed companies and almost all Internet platforms, as well as government systems in Beijing, Guangdong, Jiangsu and other places, have successively

connected to DeepSeek. Although generative AI such as DeepSeek has brought great convenience to our production and life, the ultra-large amount of data processing and complex model training behind it have brought great difficulties to the protection of the right to be forgotten. Therefore, we must consider how personal information protection can be achieved in the context of generative AI.

2. The basic theory of the right to be forgotten and the technical principles of generative artificial intelligence

2.1. The basic theory of the right to be forgotten

The right to be forgotten has been widely discussed by scholars, mainly due to the 2014 judgment of the Court of Justice of the European Union in the Gonzalez case. Prior to this, in order to strengthen the protection of personal information, Article 17 of the General Data Protection Regulation ("GDPR") issued by the European Union in November 2012 officially added the "right to be forgotten and to erasure" (Right to be forgotten and to erasure), and in March 2014, the GDPR was amended again to include the "right to be forgotten and erasure" Reduced to "Right to erasure". Article 17 of the GDPR, which came into force in 2018, defines the right to be forgotten: the right to erasure (right to be forgotten) means that the data subject shall have the right to obtain from the controller without undue delay the erasure of personal data concerning him or her that is incorrect, etc., when "the personal data have become unnecessary in relation to the purposes for which they were collected or otherwise processed", "the data subject withdraws consent", "there is no lawful basis for the priority processing of personal data", "the personal data has been unlawfully processed" The erasure of personal data is necessary in order to comply with a legal obligation of the Union or Member State applicable to the controller" "When the data subject objects to the processing of personal data on marketing grounds", the controller is obliged to erase the personal data without undue delay. [2]With regard to the right to be forgotten, Chinese scholars have a great debate on the nature of its rights and whether it should be transplanted, and those in favor believe that the recognition and protection of the right to be forgotten is conducive to safeguarding human dignity and promoting personality equality.[3] Opposing scholars believe that there is no substantive difference between the right to be forgotten and the right to delete in China, and the essence of the right to be forgotten is the right to delete, and the focus of the right to be forgotten is not to forget, but to delete, and the right to delete is more in line with the essence of the right.[4] The Civil Code provides for the protection of personal information in principle, and the second paragraph of Article 1037 stipulates the "right to be forgotten" for the protection of personal information in China.

2.2. Principles of generative AI technology

Whether it is DeepSeek, or generative AI such as DeepSeek, Doubao, and Kimi, they are all large models based on deep learning, and there may be differences in the specific way of data processing, but there is no difference in the data processing mechanism. In this

paper, we take DeepSeek-R1 as an example to study its mechanism for processing data. The design of DeepSeek-R1 is based on DeepSeek-V3, and the principle of machine learning is the same, using the following technical route: simulating the operation of the human brain to establish an N-latitude space, putting the collected data into the coordinates of the N-dimensional space, and converting each word in the N-dimensional coordinates into a series of numbers that can be understood by the machine, and the number sequence represents the similarity between this token and other tokens in the N-dimensional coordinates (the similarity between the available vectors, such as the cosine of the included angle, whose value falls on [0,1] interval and then calculate the statistical rules of natural language through powerful computing power.[5] Through the obtained natural language statistical rules, the subsequent output content is continuously predicted according to the prompt words entered by the user. The innovation of DeepSeek-R1 is the use of multi-modal large models, which combine the advantages of supervised learning and reinforcement learning through a staged training strategy. According to the official description of DeepSeek, the data processing mechanism of DeepSeek-R1 is shown in Figure 1 below, which includes three links: data input, model training, and data output.[6]

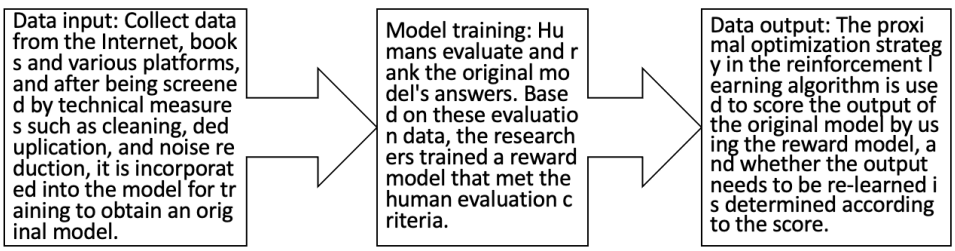

Figure 1 ChatGPT's data processing mechanism

3. The dilemma of the protection of the right to be forgotten in the context of the era of artificial intelligence

3.1. Institutional dilemma: The personal information protection system is not perfect

China already has some legal norms for the protection of personal information, but there is still a lack of governance norms for generative AI. At present, the laws regulating generative AI mainly include: the Interim Measures for the Administration of Generative AI Services (hereinafter referred to as the "Measures"), the Provisions on the Administration of Algorithm Recommendation for Internet Information Services, the Provisions on the Administration of Deep Synthesis of Internet Information Services, etc., and the laws on the protection of personal information mainly include: the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law. However, there is a lag in the law, and the above-mentioned laws only make principled regulations on the legal issues caused by generative AI, and cannot make specific provisions for predictive and recent problems, and the Artificial Intelligence Law is still in the pipeline, so there is a lack of specific legal norms that can be implemented to deal with the deletion of personal information caused by genera-

tive AI. At present, the main laws governing generative AI are the Measures, but the governance rules stipulated in them are too general, and it is difficult to implement them in practice, whether it is a provider or a user of generative AI services. For example, Article 13 of China's Personal Information Protection Law stipulates that the consent of the personal information subject is required when processing personal information. Article 7 of the Measures also stipulates the rules for notification and consent of information processing. However, when the rules of notification and consent are specifically implemented, it is unrealistic to inform the subjects of information one by one. Moreover, a lot of information comes from the public environment of the Internet. In addition, the terminology used in Article 11 and Article 14 of the Measures is different. Different terms are used in the two regulations on the processing of personal information, one is erasure and the other is erasure. It can be seen from the side that it is not easy to completely delete personal information in the context of generative large models, but the inconsistency of the above terms may cause some problems in the specific implementation of the Measures.[7]

3.2. Technical dilemma: Deleting personal information is not feasible

Compared with AI technology, generative AI uses a larger amount of data and more complex technology, which further exacerbates the occurrence of personal information infringement. On the one hand, generative AI collects a huge amount of data, and it is impossible to implement the notification and consent rules required by law to collect personal information. If AI products collect personal information based on policies such as user consent to privacy terms, then generative AI collects personal information without the consent of the information subject. It is understood that the scale of DeepSeek-R1 parameters is 671 billion, and each token activates 37 billion parameters. In addition, the official also provides multiple distillation versions, with parameters ranging from 1.5 billion to 70 billion, to adapt to different hardware scenarios. DeepSeek-R2 has 5.2 petabytes of training data and 1.2 trillion parameter sizes. The data collected comes from a wide range of sources and is so large that it is impossible to fulfill the obligation to inform the information subject one by one as required by the Personal Information Protection Law. On the other hand, generative AI is more autonomous than AI, that is, generative AI can automatically mine and analyze and generate derivative data based on the collected raw data. In addition, AI will accelerate the ability to make reasonable inferences from training data, which may cause deleted data to be re-inferred and restored.[8] This is not the same as the emergence of large models, which refers to the sudden emergence of new behaviors or capabilities when the size or complexity of the model reaches a certain level. There are three main reasons for the reappearance of deleted data: First, DeepSeek's answer is not true or wrong, but based on the prompt words entered by the user, hoping to get the user's satisfaction. Even if the personal information is deleted, it is possible for the large model to generate similar information again

based on the probability of union between that data and other data. Second, DeepSeek will actively collect data about personal information in the process of chatting with users, and incorporate it into the model for training, and the information entered by users will affect the specific content generated subsequently. Even if the original information is deleted, DeepSeek can learn from the user's input patterns and appear similar information in subsequent content generation. The third is that the data stored by DeepSeek may be leaked, causing the deleted information to be re-involved in the model.

4. The path of legal protection of the right to be forgotten in the context of the era of artificial intelligence

4.1. The basic concept of "inclusiveness and prudence".

Under the circumstance that generative AI exacerbates personal information infringement, personal information protection has changed from the traditional "rights-based approach" to the "risk-based" public law approach.[9] "inclusiveness and prudence" is an innovative regulatory approach that adopts an open attitude towards emerging technologies while maintaining prudent oversight, aiming to encourage technological innovation and facilitate sustainable development. The risk balance concept of "inclusiveness and prudence" means that we should not only pay attention to scientific and technological research and development, but also pay attention to the protection of personal information. "Inclusion" is reflected in the support for the technological development, development and exploration of generative AI technology. Generative AI technology is the most cutting-edge technology of today's era, spanning the fields of economy, education, scientific research, art, business, etc., and has become a key technology between national competitions, and it is a technology that requires great attention and support from the state. Generative AI has become a high-speed engine for the development of the digital economy. If too many restrictions are placed on the development of generative AI, China will be at a disadvantage in the face of global scientific and technological development. Therefore, the protection of personal information should be appropriately relaxed. "Prudence" is reflected in paying close attention to the potential security risks of generative AI technology and preventing them in advance. The risk accumulation of generative AI is a gradual and multidimensional process, which involves multiple levels, such as the complexity of technology research and development, the breadth of service areas, and the uncertainty of its use.[10] The development of generative AI technology has also given rise to a series of personal information protection issues, such as the dissemination of false information and information leakage. Public authorities undertaking prudential supervision should not only provide sufficient room for the development of generative AI technology and a fault-tolerant environment, but also maintain a high degree of vigilance against the potential risks of personal information protection, and be able to take effective preventive measures in a

timely manner.

4.2. The specific protection path

According to the risk balance concept of "inclusiveness and prudence", the specific path of personal information protection in generative AI is discussed:

Expand the interpretation of deletion. From the perspective of inclusiveness, China's right to be forgotten is a passive defensive right, which can only be exercised under the circumstances stipulated by laws and administrative regulations, and in the case of not causing adverse consequences or posing danger to others, if too much attention is paid to the protection of the right to be forgotten, it is not conducive to improving the enthusiasm of R&D personnel to pursue high-tech progress. Therefore, an inclusive governance strategy should be given for the development of generative AI, and the standard of deletion obligation for generative AI should be appropriately reduced. Artificial intelligence is divided into weak artificial intelligence, strong artificial intelligence, and superartificial intelligence according to the degree of intelligence. Although DeepSeek is amazing, it is still a weak artificial intelligence, and we are still in the era of weak artificial intelligence. It is precisely because of the technical problems of algorithms and models that it is difficult to delete personal information, but technical problems are unavoidable, and we can only try our best to alleviate the dilemma of personal information deletion, and we need to find other reasonable ways to protect personal information that cannot be solved after technological innovation. From the perspective of legal provisions, one provision in the Measures provides for deletion and the other provision for elimination, indicating that the legislator is also aware that it is technically impossible to completely delete personal information in generative AI. In addition, there is a lag in the law, and in the face of the difficulty in applying the rules, it is possible to expand the interpretation of the provisions to meet the current dilemma of personal information protection and the differences caused by the inconsistency of the provisions. The purpose of expanding the interpretation is to expand the scope of application of the law itself to meet the changing needs of society. Since it is not possible to achieve the absolute legal obligation to erase, it can be interpreted by expanding the interpretation to mean that as long as the personal information output by the generative AI is not visible, the deletion of personal information is in fact deemed to have fulfilled the legal obligation to erase. If there is no infringement of personal information rights when collecting data at the information input end, there will be no infringement of personal information at the information output end, and even if there is a personal information infringement based on a large model at the information output end, then we can also play a role in protecting personal information as long as we keep the personal information unavailable at the information output end. In generative AI products, when the output result contains information that infringes on personality rights, the personal information can not appear in the result of the generative AI

output by prohibiting the generation of the result or prohibiting the user from knowing the result, so as to achieve the effect of actually deleting the information, and the information is still stored in the model's database for model training. For example, Open AI has trained an AI model that filters harmful content (i.e., a filtering model) to identify harmful user input data and model output data (i.e., content that violates its usage policy), so as to control the input and output data of the model.[11] From the perspective of expanded interpretation, the factual methods of deleting personal information from generative AI, such as disconnecting links, disabling user access, and encrypting output results, are broadened to alleviate the deletion dilemma caused by technical shortcomings.

Standardize data collection. From a prudent point of view, the protection of personal information is not only the compensation of property, but more importantly, the protection of individual personality rights. Although generative AI has become a key technology for the development of science and technology, the personality rights of information subjects are incomparable to anything, and it is necessary to be cautious about the processing of data by generative AI and grasp the bottom line of maintaining personal dignity. If the legal regulation of generative AI should start with the legal regulation of algorithms, then the legal regulation of algorithms should start with the legal regulation of data, and the most important thing in the legal regulation of data is to ensure data compliance. In the context of generative AI, the effect of pre-prevention of personal information protection is better than punishment after the fact. Both the PIPL and the Measures stipulate that, except in special circumstances stipulated by law, the collection of information shall be subject to notification and consent from the information subject. Clearly, current rules for information gathering have hindered the development of generative AI and need to be adapted to apply them. There are two ways in which generative AI collects information: active and passive.[12] For the personal information actively collected by generative AI, it is divided into general personal information and personal sensitive information according to the sensitivity of the information. Then, for general personal information that does not normally involve the personality rights of the information subject, we can legally adopt the rule of "implied consent" – as long as the information subject does not explicitly object, generative AI developers can legally process this personal information.[13] The key lies in the collection of sensitive personal information, and China's Personal Information Protection Law stipulates the definition and scope of sensitive information. Compared with general personal information, sensitive information is still a minority, and it still requires the express consent of the information subject before it can be collected. Information is divided into private information and public information based on whether it is disclosed, and disclosure lies in the possibility of making unspecified persons aware of it, but the disclosure of personal information is not always voluntary, and there are also situations where personal information is disclosed by a third-party platform, that is,

disclosure is divided into voluntary disclosure and involuntary disclosure. For personal information that is voluntarily disclosed, refer to the above rules for the handling of general personal information and sensitive personal information. For involuntarily disclosed personal information, the current processing rules of Chinese law require that the principle of necessity be followed. It is very difficult to define the necessary meaning from the positive side, and we can stipulate the bottom line of generative AI's collection of public information from the negative side, as long as the processing does not infringe on the personality rights of the information subject. The information passively collected by generative AI mainly comes from conversations with users, and the collection of conversation content can also refer to the above-mentioned rules for the collection of general personal information and sensitive personal information.

Strengthen administrative regulations on generative AI products. While continuously promoting the development of generative AI technology, we should also pay close attention to and prevent problems that may arise in the development of generative AI in accordance with the concept of "inclusiveness and prudence", and the most suitable subject to undertake this obligation falls on the administrative authorities. At present, there are many institutions exercising administrative functions, and the situation of generative AI infringing on personal information is complex, including network, data, technology, etc., and it is easy to form a chaotic situation without a unified digital regulatory authority to oversee and coordinate the work of various departments. Therefore, generative AI should be administratively regulated by a dedicated digital regulatory authority, and the regulatory authority should assume the responsibility of coordinating the supervision of generative AI and protecting the rights of information subjects. The details are as follows:

First, establish a unified administrative licensing system and policy for generative AI development.[14] Taking into account the requirements for the data and computing power required to develop generative AI, generative AI developers should first apply to the administrative authority for the qualification to develop the product before developing the product, and the administrative agency shall review the developer's self-regulatory plan and compliance plan, and use the review results as the license qualification for the development of generative AI products. Through the administrative licensing system, it is forbidden to privately develop generative AI products, which can not only filter products that infringe on information subjects in advance, but also trace the source of infringing products in the later occurrence of generative AI infringement incidents, so as to facilitate unified and centralized supervision.

Second, in the process of generative AI training, strengthen the supervision of the data processed by the provider and the disclosure of the interpretation of the algorithm. The supervision of data processing includes whether the provider complies with the above rules in collecting personal information, reviewing the quality of

personal information after data cleansing and data desensitization, and using the review results as an important reference for whether it can be included in the model for training. For the algorithm used in training, the provider is required to provide a relatively reasonable explanation. In addition to conducting unscheduled reviews of data processing and algorithmic interpretation, the focus should also be on the prevention and treatment of generative AI infringement of the right to be forgotten, and the timely handling of technological risks. Providers have technical expertise and are more sensitive to potential security breaches, and should take primary responsibility for risk prevention and handling.

Third, conduct a comprehensive evaluation of generative AI products before they are put into use. Generative AI involves a wide range of fields, and the establishment of risk assessment should also be based on the integration of all aspects, including the synthesis of the assessment subject, the assessment aspect, and the assessment results. The comprehensive assessment subject means that the assessment subject should not only be artificial intelligence technicians, but also experts in the fields of law, economics, ethics and other fields; In terms of assessment, it refers to the risk assessment of data set leakage, the assessment of bias of data set, the assessment of data set attack resistance, and the identification and evaluation of sensitive information of data set.[15] The comprehensive assessment results refer to the evaluation of the safety, reliability, controllability, and fairness of generative AI to determine the risk level of the product. Through a comprehensive assessment, a decision will be made on whether to put the generative AI product into use based on the evaluation results, and the risk of infringement of personal information will be controlled before it is put into public use.

4. Conclusion

Problems caused by technology must be solved by technology after all. In practice, we need to clarify the relationship between the protection of personal information and the development and utilization of personal data, and grasp the boundary between the two. In order to cope with these difficulties and reduce the risks brought by the development of generative AI to personal information protection, we have rescued the deletion of personal information in the generative AI scenario based on the risk balance concept of "inclusiveness and prudence". While promoting the continuous development of generative AI, we should pay attention to and prevent the problem of personal information deletion.

Acknowledgements

General Project of the Graduate Research and Innovation Fund Program of Anhui University of Finance and Economics: Research on the Legal Protection of the Right to Be Forgotten in the Context of the era of Artificial Intelligence (Project No: ACYC2023275)

References

[1] World Bank Group Publication（2023）generative artificial intelligence. Washington: WBG,2023.

[2] European Union General Data Protection Regulation（2018） Article 17.

[3] Yang Lixin, Han Xu（2015）Localization and Legal Application of the Right to Be Forgotten in China. Journal of Law Application, 2015, 24-34.

[4] Zheng Zhifeng（2015）Research on the Right to Be Forgotten in Cyber Society. Studies in Law and Business, 2015, 50-60.

[5] Yu Shiwen, Zhu Xuefeng, Geng Libo（2015）Natural Language Processing Technologies and Deep Linguistic Computing. Social Sciences in China, 2015, 127-135.

[6] Github:DeepSeek-ai/DeepSeek-R1.https://github.com/deepseek-ai/DeepSeek-R1?tab=readme-ov-file

[7] Lin Beizheng（2024）No Deletion, Only Oblivion: Interpretation and Reconstruction of the Obligation to Delete Personal Information in AI Large Models. Journal of Xi'an Jiaotong University (Social Sciences), 2024, 152-165.

[8] WACHTER S, MITTELSTADT B. A right to reasonable inferences: re-thinking data protec-tion law in the age of big data and AI. https://papers.ssrn.com/abstract=3248829.

[9] Zhang Tao（2022）Exploring the Dimensions of Risk Control Paths for Personal Infor-mation Protection. Law Science, 2022, 57-71.

[10] Xu Lei（2024）Integrated Regulation of Content Risks in Generative Artificial Intelli-gence. Publishing Research, 2024, 59-66.

[11] Cao Jianfeng（2023）Towards Trustworthy AI: Governance Challenges and Responses to Generative Artificial Intelligence Like DeepSeek. Journal of Shanghai University of Political Science and Law (Legal Forum), 2023, 28-42.

[12] Dou Xiaodong（2023）Risk and Control: On Personal Information Protection in Generative Artificial Intelligence Applications. Tribune of Political Science and Law, 2023, 59-68.

[13] Huang Pei（2024）Challenges and Regulatory Responses to Risks in Personal Information Protection Posed by Generative AI. Modern Law Science, 2024, 101-115.

[14] Deng Jianpeng, Zhu Yicheng（2023）Legal Risks and Countermeasures of the DeepSeek Model. Journal of Xinjiang Normal University (Edition of Philosophy and Social Sciences), 2023, 91-101+2.

[15] Hei Yiming, Chen Wentao, Chen Jie, et al（2024）A Review of Security Risk Assessment and Defense Technologies for Large Models. China Information Security, 2024, 24-27.