ISSN 2706-6827 Vol. 7, Issue 3: 15-20, DOI: 10.25236/IJFS.2025.070303

# Research on Legal Issues of Personal Information Protection in the Context of Artificial Intelligence Development

**Mo Wenyu**

*Shanghai Maritime University, Shanghai, China*

***Abstract:*** *The contemporary technological landscape is witnessing the emergence of generative AI, with international internet and technology companies launching their own generative AI models. Concurrently, concerns regarding personal information security have come to the fore. Users may unintentionally disclose their personal information when using generative AI services, and this unprocessed information may be used for unlawful and criminal activities. The inadequacy of prevailing regulatory frameworks and legal instruments to adequately safeguard user rights and interests is becoming increasingly evident. Consequently, there is an imperative to establish technology laws that are tailored to the unique characteristics of generative AI, utilising a hierarchical approach to safeguarding personal information. This should involve the employment of anonymisation and de-identification techniques during information processing. Moreover, it is essential to foster self-regulation among AI service providers and to enhance the regulatory oversight of personal information processing by authorities. These measures are crucial to ensure the security of personal information across various domains.*

***Keywords:*** *Personal information protection; Artificial intelligence; Institutional improvement*

## 1. Introduction

Once the generative AI Chat-GPT was released in 2023, generative AI products took the world by storm in just a few months. In August 2023, major models such as ERNIE Bot, Inspur Qingyan, Baichuan Intelligence and SenseNova went online, followed by DeepSeek in December 2024. China's big artificial intelligence (AI) models came to the foreground. Generative AI developed with the help of massive data processing and big language models has driven innovative iterations of the digital economy. The accompanying leakage of personal information has a far wider reach than ever before, with serious implications for users' economic security, credit security, and personal privacy security. In pursuing the speed of development of generative AI models, many companies and organisations have neglected to strengthen measures to protect the security of user information and lacked strict regulatory mechanisms.[1]As a result, many illegal behaviours of illegally accessing and reselling personal information are difficult to be effectively curbed, leaving opportunities for lawbreakers to take advantage of them. Just one product, ChatGPT, has been repeatedly in the news for overstepping its authority in collecting personal information and leaking sensitive information.[2]Therefore, in the era of artificial intelligence, adopting measures to protect personal information, increasing the responsibility of service providers or data collectors, and improving relevant laws and regulations are necessary means to protect the security of users' personal information.

## 2. The Dilemma of Personal Information Protection in the Context of Artificial Intelligence Development

Generative AI large model pre-training is the main link for generative AI to gather massive data for analysis. The mainstream generative AI on the market, the number of parameters included in the pre-training model are tens or even hundreds of billions of huge parameters.[3]The massive data almost all come from the public Internet, such as Wikipedia, e-books, journal articles, web crawler datasets, and so on. In the process of assembling massive data, there are many behaviours of service providers that overstep their authority to process personal information. It has become an inevitable issue in the AI era to get the user's consent to collect data legally, as well as to protect the user's rights to data involving personal information, to prevent the leakage of the user's personal information, and to protect

ISSN 2706-6827 Vol. 7, Issue 3: 15-20, DOI: 10.25236/IJFS.2025.070303

the security of the data in the context of facilitating the development of a large model of generative AI.

### *2.1 Difficulties faced in the collection of personal information*

In the process of collecting huge amounts of data, there are numerous behaviours of service providers that exceed their authority to process personal information. While the basic layer of pre-training mainly collects publicly available data on the public Internet, it also contains a lot of personal information, the processing of which is not ipso facto lawful because it is publicly available. On the one hand, such personal information involves sensitive information, and the processing of sensitive information usually requires the individual consent of the user, which the service provider clearly has not obtained. On the other hand, web crawlers involve the illegal act of grabbing personal information when collecting data, and the use of web crawler datasets by generative AI may constitute indirect infringement. When digital platforms engage in big model building or collaborate with generative AI services, the rich data in the digital platforms become the best training data, however, the digital platforms do not fully comply with the notification of consent rule. For example, the data licensing terms for public platforms are included in the terms of the privacy policy, but updating the privacy policy alone is not sufficient to achieve adequate notification, and the generalised consent of the terms of the blanket agreement makes it difficult for users to substantively exercise their right of refusal. Users' use of generative AI is contingent on their consent to the collection of personal data by the service provider, without which they cannot use it properly. This results in users almost ‘voluntarily’ handing over personal data such as communication and login information, and the data generated in the course of use is also collected by the service provider for model retraining, which may be unknowingly or unintentionally ignored by the user.

Storage of personal information and data loss and leakage due to system vulnerabilities, which are used for illegal activities, are also serious problems to be solved. Artificial intelligence systems often rely on complex algorithmic models that may have undetected vulnerabilities.[4] For example, certain deep learning algorithms may have incorrect memory access patterns when processing specific types of data inputs, which is like having gaps in the walls of a ‘warehouse’ where personal information is stored. Hackers can take advantage of these loopholes to bypass normal security detection mechanisms and illegally access databases with personal information stored in them, thereby stealing the information and leaking it. ChatGPT has had a number of leaks of sensitive information, affecting users' rights to their personal information and potentially causing further damage to their rights.

### *2.2 The dilemma of de-identification of personal information*

In the face of the dilemma that generative AI technologies are blurring the distinction between personal and non-personal information, the user's right to information and consent is of great importance. As a consideration for the use of online services, users generally accept the commercial use of their personal information by personal information processors, and the law also allows personal information processors to anonymise personal information in exchange for economic benefits.[5]Chinese legislation provides for the anonymisation of personal information, and the Code of Personal Information Security defines ‘anonymisation’ as the process of processing personal information by technical means in such a way that the subject of the information cannot be identified or associated with it, and the processed information cannot be recovered. The Law on the Protection of Personal Information also provides for ‘de-identification’, which requires that processors of personal information should adopt security technology measures such as encryption and de-identification to ensure that their processing of personal information complies with the law.

There are obvious shortcomings in China's personal information protection legislation with regard to the anonymisation of information, although the anonymisation requirement of 'removal of identifying marks' ensures the security of personal information to some extent. However, as can be seen from the Personal Information Protection Law's stipulation that personal information ‘does not include anonymised information’, the anonymisation requirement protects the interests of the information processor, and legitimises the information processor's commercial interest in the anonymised information. The information processor is frequently the provider of generative artificial intelligence services and the operator of the platform, and has an absolute advantage over users in terms of manpower, capital and technology, and has a better understanding of the flow of information and the impact of its behaviour, so it is essential to require the operator to assume the corresponding obligations.

ISSN 2706-6827 Vol. 7, Issue 3: 15-20, DOI: 10.25236/IJFS.2025.070303

## 3. Hierarchical Protection of Personal Information in the Context of Artificial Intelligence

### *3.1 Classifying personal information according to risk*

Currently, China's legal provisions on the protection of personal information mainly focus on the obligations of information processors and information subjects. The current legal framework for the protection of personal information is predicated on the principle of fault-based liability, a concept that has proven to be inadequate in adapting to the evolving landscape of personal information governance in the era of artificial intelligence.[6]This is due to its inability to address the complexities inherent in the protection of personal information, which is likely to result in the emergence of loopholes and disputes within the legal system. In order to better protect the rights and interests of citizens' personal information, it is necessary to explore a more diversified principle of attribution of responsibility, which should be based on the hierarchical protection of personal information and be compatible with the hierarchy of personal information, so as to cope with the ever-developing technological environment. For risk-based design of legal obligations and liabilities, it is possible to follow the 'risk-based' approach of classifying risk levels and establishing different rules. For the regulation of personal information protection of generative artificial intelligence, the idea of 'risk level - regulatory measures' can be adopted. In the classification of specific risk levels, the probability of occurrence and severity of consequences should be the main considerations, and the difficulty of prevention can also be taken into account if necessary.

The Personal Information Protection Act classifies information risk levels according to the sensitivity of the information, and the relevant legislation reflects the legislative idea of differential protection of personal information, which may change in different scenarios. Therefore, the risk stratification management of the derivative use of personal information data should be assessed and managed differently according to specific information use scenarios, and the risk of derivative use of information can be classified into four levels, low risk, general risk, higher risk and serious risk, and managed hierarchically. As the level of risk increases, the security protection measures taken are progressively more stringent. In the case of serious risks, the data management authorities can order the data processors to stop the derivative use of information.

### *3.2 Establishing detailed rules for the protection of personal data*

In accordance with the provisions outlined in Chapter 5 of the Personal Information Protection Law, which stipulates the obligations of personal information processors to mitigate risk, it is possible to establish detailed regulatory rules by integrating the technical characteristics of generative artificial intelligence with the risk level of associated behaviours. Service providers are required to employ a combination of de-identification technology, automatic algorithmic screening, and manual filtering. This is to ensure that the possibility of sensitive information entering model training at the source is eliminated, and that personal information is anonymised and de-identified in the data involved in model training. Concurrently, the regulatory authority should undertake a review of the outcomes of the service provider's data screening process to ascertain that the personal information contained within the participating databases has attained the requisite anonymisation standard, is suitable for utilisation in training and score generation, and will not compromise the confidentiality of other individuals in subsequent services. Regulators should require service providers to conduct compliance audits in relation to compliance with the provisions of the Personal Information Protection Act. Service providers should also be required to conduct compliance audits of the substantive work and effectiveness of risk prevention in conjunction with the findings of ex-ante impact assessments, and to emphasise that ex-post remediation and notification obligations play an underpinning role in risk prevention.

## 4. Improvement of institutional standards for the protection of personal data in the context of artificial intelligence

### *4.1 Separate notification standard for the risk of collecting personal information involving artificial intelligence*

It is evident that generative AI services themselves do not adequately implement informed consent rules to protect users' rights to personal information. Users lack the right to be fully informed and to make substantive decisions about the use of data generated when using the service for model training.

ISSN 2706-6827 Vol. 7, Issue 3: 15-20, DOI: 10.25236/IJFS.2025.070303

Service providers have mostly chosen to inform of the requirement to collect personal information through their privacy policies, rather than individually prompting for sensitive permissions such as the use of microphones, photo albums, location, etc., as they do. It is reasonable to assume that users are not likely to read the privacy policy in detail at the time of use, and even those who do are unaware of the collection of personal data by big models. It can thus be concluded that generative AI service providers do not adequately provide individuals with easy access to realise their personal data rights and interests.

The EU's General Data Protection Regulation sets out rules for the fair use of personal data, and in addition to 'notification and consent as grounds for lawful processing of personal data', it also sets out grounds for lawful processing of personal data that do not require an individual's consent. These include 'necessary for the performance of a contract', 'necessary for the performance of a legal obligation', 'necessary for the protection of the core interests of others', and 'necessary for the protection of the public interest', which are listed in Article 6. The GDPR's legitimate grounds for processing special personal data include 'lawful processing', 'special consent' and 'non-consent'.[7]The latter two rules are special rules of reasonable use, and under the legal principle that special law is superior to general law, they apply in preference to 'lawful processing', which also governs the special processing of sensitive information. This also establishes a stricter system for the reasonable application of rules that are not based on the data subject's consent in the scenario of special processing of sensitive information, i.e. the processing of information must meet the condition that "the data subject is unable to consent to the processing for his own reasons or for legal reasons, but the processing operation is necessary for the protection of the core interests of the data subject".

### *4.2 Clarification of liability for infringement of personal information by artificial intelligence*

Depending on the level of risk, Level 1 information is personal information that has been anonymised and de-identified, and this type of information cannot be recovered after processing, so no attribution principle needs to be applied. For breach disputes involving second tier, less sensitive information, general fault liability is used as the attribution principle to attribute liability to the information processor. Information processors must be responsible for their own conduct and should be held liable unless there is evidence that they are not at fault. For Level 3 information, which is relatively sensitive and requires more stringent protection measures, information processors cannot easily be exempted from liability and the principle of presumption of fault applies. For level 4 information, which is absolutely sensitive and requires special protection measures, the application of the principle of no fault liability can better protect the rights and interests of the data subject. Regardless of whether the information processor uses artificial intelligence technology, as long as it violates the information subject's right to absolutely sensitive personal information, it should bear the corresponding legal responsibility.

### *4.3 Improving the Compensation System for Personal Information Infringement Involving Artificial Intelligence*

Determining the standard of compensation for personal information infringement involving AI can be based on a number of aspects, such as the assessment of actual losses, the measurement of moral damages, and the profitability of the infringement. It should be based on the actual losses of the victimised users, including direct economic losses, such as the amount of money stolen as a result of the leakage of personal information, indirect economic losses, such as the reasonable costs of restoring damaged credit and dealing with the follow-up of the infringement, as well as compensation for moral damages caused by the infringement of personal information. If the AI service provider is liable, the injured user should be compensated accordingly, based on the size of his or her liability and whether he or she has fulfilled the duty of loyalty and fulfilled his or her own duties, among other considerations.

The right to personal information is intrinsic to both the spirit and property of the individual. In cases where this right is violated, resulting in significant psychological distress, the claim for moral damages serves as a legal remedy. This is not only because the mental trauma must be addressed, but also because the infringement of the right to personal information will inevitably result in the loss of property, which may be masked in a number of ways, including the direct damage to the economic interests of the individual, a lowered credit rating, and so on. Consequently, the individual has the right to claim property damages to compensate for losses suffered as a result of the infringement and to defend the integrity and legitimacy of their legitimate rights and interests.

ISSN 2706-6827 Vol. 7, Issue 3: 15-20, DOI: 10.25236/IJFS.2025.070303

In the context of judicial proceedings, the substantiation of property loss, coupled with the provision of substantial evidence by the aggrieved party, forms the basis for the consideration of a request for property damages. To illustrate this principle, consider instances of credit card theft or fraud resulting from information leakage. In such cases, the property loss is readily quantifiable, with an estimation derived from the profit accrued by the processor of personal information. In the era of generative artificial intelligence, novel forms of infringement, such as excessive information collection and leakage, frequently result in losses that are challenging to detect, intangible and uncertain. This complicates the adaptation of the conventional difference-in-differences method, which is predicated on the actual losses incurred, to this novel infringement model. In instances where the aggrieved individual is challenging to substantiate or where there is a paucity of evidence to substantiate property loss, judicial bodies may encounter challenges in supporting claims pertaining to property damage. In such circumstances, the benefit accruing to the processor of personal information can be regarded as the calculation standard, given that the benefit derived from the processing of personal information is typically verifiable and the benefits that the infringer or the industry might derive from the processing of the same personal information are also foreseeable. Furthermore, the introduction of a punitive damages system within the legal framework for infringing behaviours with obvious malice and serious consequences is imperative. By increasing the cost of violation of the law by the information processor, the infringer is effectively incentivised to safeguard his or her legitimate rights and interests, raise the legal awareness of the personal information processor, and strengthen the protection of the right to personal information.

Similar to the right to assert property rights, the right to prevent infringement, remove obstacles, and reduce risk is a right to assert personality rights in comparison to the right to seek damages. The user has the right to request that the infringement stop, that the obstruction be removed, and that the danger be removed when personal information is consistently violated, such as when a mobile phone automatically activates the positioning function in the background and records the user's behavior without the user's consent. The implementation of a punitive damages system can successfully compensate the victim for losses incurred in cases of infringement with clear purpose and grave repercussions. Through economic sanctions, the punitive damages system can not only make the infringer pay more for his actions and punish him financially, but it can also make it less likely that similar actions would be taken in the future. It can also act as a warning to other possible offenders about the illegality and immorality of their actions, which can stop and reduce the infringement of users' personal information.

## 5. Conclusion

Generative AI has been shown to present a number of issues with personal information protection. These include the overstepping of its authority to collect personal information, the easy leakage of sensitive information, and the failure to inform users individually of how their personal information will be handled. Given the distinctive characteristics of generative AI in data processing, the constraints imposed by the rights-based approach of the Personal Information Protection Law necessitate a transition to a risk-prevention regulatory mindset, and the establishment of a risk-oriented dynamic regulatory scheme within the existing framework of the Personal Information Protection Law, taking into account the unique characteristics of generative AI's data utilisation. On the one hand, it is necessary to provide a risk-based interpretation of the rules on personal information protection, so as to provide sufficient space for generative AI to process huge amounts of data and use deep learning algorithms. In order to ensure the optimal balance between the benefits that personal information processing can offer and the potential risks, it is essential to strengthen the rules on notification and consent. This should be achieved by requiring service providers to provide individuals with comprehensive information regarding the risks associated with the processing of personal information. The decision regarding acceptance of these risks and utilisation of the service should be left to the individual. In addition, it is necessary to incorporate a risk-based design of legal obligations and responsibilities. The obligations and legal liabilities of personal information processors stipulated in the Personal Information Protection Law should be fully detailed under the correspondence of 'risk level - regulatory measures'. A dynamic regulatory scheme with clear hierarchy and reasonable measures should be constructed by data collectors, processors, and regulators, so as to ensure that, while the data empowers generative AI, the processing of personal information should be prevented and controlled as much as possible. The risks associated with the processing of personal information should be prevented and controlled as much as possible, so as to achieve both safety and development.

ISSN 2706-6827 Vol. 7, Issue 3: 15-20, DOI: 10.25236/IJFS.2025.070303

**References**

*[1] YIN Yuhan, LI Jian. Personal information protection issues of generative artificial intelligence and its regulation[J/OL]. Journal of Hainan University (Humanities and Social Sciences Edition), 2023,1-11.(In Chinese)*
*[2] Open AI data breach announcement: https://openai.com/blog/march-20-chatgpt-outage*
*[3] Zhu Rongrong. Legal Protection of Indirectly Identifiable Personal Information in Generative Artificial Intelligence Applications[J]. Technology and Law ,2024,(04):104-114.(In Chinese)*
*[4] Kaltheuner F, Bietti E. Data is power: Towards additional guidance on profiling andautomated decision-making in the GDPR[J]. Joumal of Information Rights Policy andPractice,2018,2(2):17*
*[5] Guo Tianrun. The hierarchical protection and relief of personal information related to artificial intelligence[J]. Journal of Shandong Judges Training Institute,2024,40(04):43-55.(In Chinese)*
*[6] Zheng Huangjie. Risk prevention: a paradigm innovation of personal information protection in the view of AIGC [J/OL]. Credit,2024,(10):23-33.(In Chinese)*
*[7] XU Wei, LI Wenmin. APP personal information collection risk governance: EU experience and inspiration[J/OL]. Journal of Nanjing University of Posts and Telecommunications (Social Science Edition), 2024,1-16.(In Chinese)*