Exploring Personal Information Protection Issues in the Context of Generative Artificial Intelligence

Yuehan Ming

School of Environmental Design, Tiangong University, Tianjin 300387, China

18810231286@163.com

Abstract. The full-chain mechanism of generative artificial intelligence—comprising the stages of "preparation–computation–generation"—has fundamentally transformed conventional modes of data processing. This transformation directly and substantively challenges traditional personal information protection frameworks. At the same time, it introduces a range of embedded risks, including data misuse and the opacity of the algorithmic black box As a result, existing regulatory mechanisms such as informed consent are increasingly ineffective in large-scale and highly automated application scenarios. In response, this paper proposes a regulatory framework oriented toward personal information risk prevention and control. Specifically, the framework emphasizes strengthening regulation to constrain key actors, employing privacy-preserving computation technologies to define AI-adapted legal rights and compliance standards, and enhancing users' ability to exercise their rights effectively. Through these measures, a governance structure can be established in which technology, institutions, and responsible actors operate in coordination, thereby achieving a genuine balance between technological innovation and personal information protection.

Keywords: Generative artificial intelligence; Personal information protection; Algorithmic black box; Right to erasure; Three-dimensional governance pathway.

1. Introduction

Artificial intelligence is a strategic technology ushering in the new scientific and technological revolution and industrial transformation, which has a deep impact on the production and living ways of humans.Most importantly, generative AI has increased efficiency in many industries, including autonomous driving and content creation, and emphasised the fundamental role of data as a new factor of production. The so-called massive amount of personal information in the training datasets is however subject to risks of misuse or leakage during the preparation, computation and generation stages. Mistakes made in this area have been harrowing, like AI face swapping and information fabricating. So the challenge of balancing technological innovation and data protection has become a pressing issue.Some actors have not gathered and used data in standardized and legal ways in the creation of generative AI in particular. These are the wrong ways to do things, and they've created a basic conflict between these technologies and the current personal information protection system. The majority of the relevant legal principles in China date back to before the advent of generative AI. Article 4 of the Interim Measures for the Administration of Generative Artificial Intelligence Services provides for the protection of rights and interests to personal information, but there are no specific and operational legal rules. This means that it is challenging to deal with a number of structural tensions such as those between large-scale data learning and the right to erasure, between opacity of algorithms and transparency obligations, and between automated processing and purpose limitation.This regulatory delay has directly resulted in a dilemma of two-fold. In the field of civil law, the old "notice-and-consent" doctrine is no longer operational, and the rights to informed consent, deletion and rectification are very hard to apply in automated processing contexts. The problems in the field of criminal law are even more accentuated. The new modalities of crime brought about by generative AI are precision fraud and false information dissemination. These new approaches go beyond the current framework and challenge direct the current system of criminal responsibility. How to make the decisions about who is responsible when more than one person is involved, whether its service providers, technical models, or users? Is the liability of highly

autonomous AI systems possible? There is no theoretical guidance and comprehensive legislation, which leaves judges in a passive position without existing guidelines for their work when dealing with individual cases. Hence, it is necessary to adapt China's criminal law theory and institutional structure in a proactive and prudent manner in order to address these emerging challenges.

2. Operational Mechanism of Generative Artificial Intelligence

Generative artificial intelligence demonstrates a distinct and rigorous full-process data dependency characterized by the stages of "preparation–computation–generation." Consequently, issues such as the accuracy and fairness of training data, as well as the uncontrollable risks associated with massive volumes of personal information, run throughout the entire lifecycle of the technology. For this reason, compliance with personal information protection has become a new focal point that distinguishes generative AI from traditional algorithmic systems.

2.1. Preparation Stage

The preparation stage constitutes the foundation for the operation of generative artificial intelligence. Its primary objective is to establish the data infrastructure that supports the model. This stage typically involves three key processes: large-scale data collection, preliminary data processing, and human-assisted calibration. Each of these processes carries potential risks of violating legal boundaries related to personal information protection.Therefore, it is necessary to clarify that this stage should rely primarily on publicly available data and data collected through targeted and lawful means as training materials. If personal information is obtained without the explicit consent of the data subject, or if sensitive personal information is collected in violation of applicable regulations, such conduct violates the principles of "prior notification and voluntary consent" established in personal information protection law [1] and directly infringes upon individuals' rights and interests in their personal information.More specifically, during the stage of preliminary data processing, insufficient data anonymization and inadequate security protection measures may easily lead to information leakage. During the human-assisted calibration process, personnel may have direct access to raw personal information. Without strict confidentiality mechanisms, this access may result in the illegal dissemination or misuse of personal information. Moreover, the subjective preferences of human annotators may introduce biases into the training process, which can subsequently influence how the model processes personal information. Such biases may further increase the risk of future legal disputes.

2.2. Computation Stage

Non-compliant use of personal information and possible data security issues are the main legal challenges during the calculation phase. Models are often optimized using real-time user data in real-world systems. With no proper and noticeable disclosure to the user about the purpose, scope and duration of the data being used, and no consent for using the data to train models, such uses are in direct violation of compliance requirements. In fact, this situation is fairly prevalent in the industry.Similar to this, there are risks at the data-cleaning process. Leakage of personal information is easily possible if discarded data with personal information is improperly disposed of, or if it is not anonymized or desensitized. As a result, the security management of data cannot be overlooked when they are marked as "pending deletion".More significantly, and in more subtle way, personal information can embed itself during the process of model optimization. When the record of the data processing trajectory is not complete and reliable, it is hard to establish who is responsible when there is misuse or a leak of personal information and the burden of evidence becomes considerably higher. Thus making a computation process traceable and auditable can be considered one of the most powerful tools to keep pace with technological progress while adhering to regulations.

2.3. Generation Stage

The generation stage is when the model is finally utilized to generate its output. Thus, the most salient and usual legal concerns in this phase are indirect disclosure of personal information and the challenge of proving tort liability. A generative AI product made by a technology company revealed the plaintiff's privacy in its outputs, in a case before a Beijing court [2]. The information in the training set was not adequately de-identified, and contained the plaintiff's name, contact details, and other personal information. Based on this, the court concluded that the company did not meet its obligation to anonymize the data. There was a direct and clear causal connection between its conduct and the harmful result and it was an actual invasion of the plaintiff's right to privacy and personal information rights and interests. The court finally determined the company to be completely liable for the plaintiff's damages.This case also gives a clear indication of another important point; in most cases, the risks that occur during the generation phase are the result of non-compliant data processing during previous phases. These are then seen at the output stage as legal liability. In other instances, the nature of risk is even more hidden. Content created using non-compliant data may inadvertently lead to a breach of personal privacy in a manner that is very hard to identify, causing harm that is very hard to track and trace. Another issue is that the technological path is long and participants are various. After the infringement, the duties of the development, operation and use phases are easily mixed up and the liability is often not easily determinable. This lack of accountability and responsibility significantly complicates the task of rights protection, in essence.So, the generation stage risk governance should not only be an ex post content review. Rather, it should be proactive in establishing a comprehensive linkage with upstream data compliance practices and adding a comprehensive accountability mechanism. This is the only way that a systematic, rigorous and practical risk prevention and control system can be built.Technology innovation and rights protection should not be seen as being mutually exclusive, because they are directly and substantially linked to the protection of personal information throughout the entire process of technology functioning. Rather, they should be coordinated and unified. The foregoing case analysis reveals that the personal information protection process must be sufficiently penetrated by technology and compliance, compliance obligations for each personal information related party must be clarified, and the entire compliance process must be fully linked with the prevention, control and emergency response mechanism. This can then serve as the foundation for developing a systematic, clear and enforceable regulatory framework.

3. The Concrete Manifestation of Dual Risks:The Governance Dilemma of Data Abuse and Algorithmic Black Box

The issues of data misuse and algorithmic opacity triggered by generative AI have placed the personal information protection rules centered on the Civil Code in a situation of practical difficulty. Current legislation lacks sufficient operability, making it difficult to regulate these issues effectively. At the same time, the intrinsic characteristics of generative artificial intelligence—particularly its reliance on massive datasets and complex algorithms—mean that the mechanisms driving technological innovation themselves involve various risks. Among these, data security and algorithmic transparency are the most prominent.

3.1. Legal Dimension: Structural Conflicts in Personal Information Protection

Generative AI's success relies on the access to large quantities of high-quality data. But there are several challenges to data collection, such as unclear legal boundaries, inconsistent data quality and high-security risks. As with any case, the fundamental conflict between the automated, large-scale data collection models and the current personal information protection model is evident, with the model being trained on about 45 TB of data and 175 billion parameters.

Generative AI often involves the integration of data from various sources and the collection of implicit data, which poses new challenges for the protection of personal information. Data processors do not always manage to present to users the information clearly with regard to the sources and

specific purposes of its collection. Furthermore, with behavioral data, it is possible to gather data without the user knowing that they are being taken. In most cases, the users are not aware that such data is being collected. This gives considerable room for doubt regarding the base of users' right to be informed. More seriously, some service providers use general, vague authorization clauses, which in effect prohibit the ability to give true and informed consent by the users.

Moreover, when personal information is used for model training, it is very hard to disassociate or remove the information from the trained model. Thereby, the rights of the user to be deleted under Article 1037 of the Civil Code are hard to put into practice. In this aspect the provision is not in accordance with the principle of voluntary which should be followed in civil activities.

Such phenomena highlight an inherent legal challenge arising at the data collection phase: the fundamental principle of "notice and consent" can easily turn into a formality in the era of generative AI. The Civil Code considers personal information to be a major concern. In Article 111, personal information is expressly defined as civil right and civil interest and in Article 1034-1039 there is a systematic and hierarchical regulation based on the notions of "notice and consent" and "purpose limitation." The provisions make clear the obligations that apply to the processing of personal information in the traditional world, and offer strong and viable legal grounds for the safeguarding of the rights and interests of individuals. It should be noted that the use of the old rules inevitably brings structural problems with the advent of the new data-processing logic that generative artificial intelligence provides.

The concept of purpose limitation presents unique challenges when it comes to AI that generates content.The concept of purpose limitation faces specific challenges in the realm of generative AI content creation. The primary goal of generative AI is to improve the model's overall learning ability. This inbuilt generalisation function is in direct and substantive conflict with the need of the Civil Code for the personal information to serve specific purposes. In reality, personal data inputted by individuals may be utilized for multiple domains and beyond the initial context in generative AI systems. Fine tuning can also be done to base models to suit different scenarios. Consequently, a trend towards "single collection, multiple reuse, and multiple applications" has developed. This model goes beyond users' expectations, raises the risk of over processing information/leaks of data, and further confuses legal lines. Similarly, the massive amounts of data that power generative AI are compiled from various information sources. These data inevitably contain inequalities in the real world, such as inequities in the distribution of resources, as well as biases, such as gender and racial stereotypes.

3.2. Algorithmic Dimension: The Crisis of Rights Protection Triggered by the Black-Box Nature of Algorithms

Algorithmic "black box" created by generative artificial intelligence is very opaque. It's algorithms are not explainable and traceable. This results in both a challenge to the current information compliance framework, as well as to the information protection premises laid down in the Civil Code. More seriously, such systems can trick users into doing things and an over zealous collection of information. This undermines the subjectivity of people and eventually jeopardizes the autonomy in using personal information.

The autonomous decision-making mechanisms developed by Generative artificial intelligence are built using deep neural networks [4]. This architecture is the typical "algorithmic black box" with "input－output" black box processes. This obfuscation itself undermines the set of assumptions of the Civil Code that underlie the idea of regulating conduct and imputing blame. There are 3 approaches to this problem.First, the fact that algorithmic decisionmaking is hidden, undermines the basis of legal remedies. Algorithmic bias can result in discriminatory information processing, which may be hard to identify, due to the lack of explainability and traceability of algorithmic decisions. If, on the one hand, there is a large amount of data, and on the other hand, complex algorithms are applied, the principle of fault liability provided for in Article 1165 of the Civil Code will place a

burden of proof on the victim of the action, which will require strict proof of the fault of the actor and the direct causative link between the fault and the harmful result. But the technical aspects of generative Artificial Intelligence could hinder or disrupt this causal chain. In this case, the provisions of the relevant laws can be implemented in a way that fails to effectively address the situation.Second, algorithms evolve independently, which presents a challenge for static regulations. This can be achieved by the sheer size of the parameters combined with the computing power of these large models, which gives rise to "emergent capabilities". The capabilities can engender new functions that the developer cannot foresee and cannot manage, significantly adding to the uncertainty of possible hazards. Under these conditions, it can be very challenging for data processors to adequately implement the security protection duties under Article 1038 of the Civil Code. More seriously, algorithms change their dynamics over time and this makes fault determination problematic at the time of fault. Processors may claim that negative results were "beyond reasonable expectations" and this deadlocks the issue of liability.Thirdly, algorithmic power erodes human subjectivity. Algorithms can subtly change how users act through personalized interaction, leading to users giving too much personal information. As a result, in practice, the right to informational self-determination guaranteed by Article 1035 of the Civil Code may not function properly. Users can slowly become "cognitive comfortable" with algorithmic systems, and willingly cede control over their information. In the end, this is not consistent with the basic principles of civil law that are aimed at promoting human dignity and respecting the autonomy of the individual.

4. Practical Dilemmas and Breakthrough Paths: A Three-Dimensional Perspective Based on Technology, Law, and Users

Considering both the technical characteristics of generative artificial intelligence and the practical needs of personal information protection, it can be reasonably concluded that regulatory strategies should adopt a three-dimensional perspective involving algorithms, law, and individuals. Through systematic and layered improvements in regulatory measures across these dimensions [5], and by ensuring coordination and mutual complementarity among them, it becomes possible to balance industrial innovation with the protection of personal information.

4.1. Algorithmic Dimension: Optimizing Technical Regulation to Address Governance Challenges

Algorithms constitute the core component of generative artificial intelligence. The opacity and uncontrollability of algorithmic operations are key factors that trigger risks to personal information protection. Therefore, regulation at the algorithmic level is a crucial element in the personal information protection framework for generative AI. The primary objective of such regulation is to improve the governance model of algorithms, address existing governance challenges, and promote greater transparency and controllability in algorithmic operations.the lack of algorithmic transparency can be appropriately addressed through mechanisms of algorithmic explainability review. This approach requires first clarifying the scope of review and determining the appropriate depth of examination. On this basis, it becomes possible to balance the need for personal information protection with the legitimate commercial interests of data processors. Specifically, for fundamental aspects of algorithms that do not involve trade secrets, processors should be required to proactively disclose the basic principles of the algorithm, its operational logic, and its methods of data processing. By contrast, for technical details involving core commercial secrets, alternative disclosure mechanisms—such as simplified disclosure and third-party professional auditing—may be adopted. This approach ensures that users' right to be informed is adequately protected while also safeguarding the legitimate commercial interests of information processors. With regard to deviations in algorithmic operations, the high degree of autonomy inherent in generative AI systems means that reliance on initial parameter settings alone is insufficient. Accordingly, mechanisms for dynamic algorithmic adjustment and real-time monitoring should be established in order to systematically and

promptly identify and correct deviations.Finally, because legal requirements must be strictly implemented throughout the entire process, technical governance practices may incorporate a multi-factor privacy disclosure impact model. Such a model can systematically evaluate the actual impact of personal information processing activities on users' privacy rights and interests. This approach allows risks to be identified and addressed at an early stage. On this basis, a comprehensive lifecycle risk management mechanism can be established, covering the stages of data collection, storage, use, and destruction. By strengthening risk control capabilities at each stage through technical means, potential risks of data leakage and misuse can be effectively prevented at their source.

4.2. Legal Dimension: Improving the Regulatory Framework and Strengthening Liability Constraints

Legal regulation provides the fundamental institutional guarantee for personal information protection in the context of generative artificial intelligence. Accordingly, the core task at this level is to improve the existing system of legal rules, clarify and strengthen the binding force of responsibility allocation, and ensure that all regulatory measures have a clear legal basis. At the same time, the rules governing personal information protection should be aligned with the pace of technological development in generative AI, so that legal regulation can govern the entire process of data application and address the many compliance challenges arising in the data field.

First, the application of personal information protection rules should be optimized. The provisions of Chapter II of the Personal Information Protection Law of the People's Republic of China on rules for personal information processing, as well as the provisions of Chapter IV on the rights of information subjects, both show clear limitations when applied in the context of generative artificial intelligence. The notice-and-consent rule provides an appropriate starting point for this analysis. Because generative AI involves large-scale data processing and highly opaque algorithmic operations, basic principles such as purpose limitation and data minimization face substantial difficulties in practical application, and the principle of openness and transparency is also difficult to implement in any meaningful sense. More importantly, these principles are directly and closely connected to the notice-and-consent rule in terms of legal logic.

Accordingly, from the perspective of risk mitigation in legal provisions, the risk-allocation function of the notice-and-consent rule should be used in a systematic and prudent manner, so that legal rules can be effectively implemented in practice. In more detail, the concept of data minimisation can be applied more flexibly. The law should strike a balance between enabling the gathering of data needed to innovate and full disclosure of the purpose, method, scope and risk-control measures of processing by the processors. In this way, the right to be informed and the right to autonomous choice, can be actually safeguarded. The reasoning of the judicious use of the law would thus be reconceived as risk allocation instead of compliance with the static norm. The user's consent to the processing of the information, which is explicitly consented to by the user, can be considered as the voluntary acceptance of the corresponding processing risks if the information processor has fulfilled the duty of disclosure. This design will help to strike a balance between safeguarding the right to personal information and leveraging generative artificial intelligence for practical applications.

Second, the legal obligations and liability attribution system needs to be further enhanced. It is essential that this be understood first: simply using a risk-oriented approach to interpreting the legal provisions is not enough to ensure a sensible distribution of the risks. So the legal duties of information processors should be reinforced and law enforcement should be truly effective. In this regard, the basic idea of risk-based regulatory classification can be adopted. Personal information processing risks can be divided into three types: unacceptable risks, high risks and limited risks. It is based on this principle that differentiated rules of regulations, with clear hierarchical distinctions, should be created. The following activities must be banned outright because they are considered unacceptable risk; those with high risk must be evaluated at every stage of the process and regulated by internal control processes; and limited-risk activities must be subject to improved disclosure and supervisory control. Concurrently, the requirements of "ex ante assessment" and "ex post

remediation" should be progressively clarified and strengthened so as to ensure clear responsibilities can be held.

Consequently, a system of graduated administrative liability should be put in place. Malicious violations, in view of the degree of harm, the extent of the subjective fault and the effectiveness of the corrective measures, should be subject to more severe sanctions; negligent violations that are followed by timely and adequate remedial action, should be met with less severe sanctions. This would make proportionate sentencing: e.g., between wrongdoing and punishment. In addition, supporting mechanisms should be established including regulatory interviews and regular inspections, to tighten the control of platform operators and to ensure effective rectification. As regards civil liability, the concept of presumed fault can be adopted, which means that the burden of proof lies with the information processor to prove that there is no fault. Last but not least, it should be given to the user the right to prohibit any generated output that results from his or her personal information, explicitly. These measures will allow the legislative goal of balancing rights and responsibilities and providing adequate protection to be met.

4.3. Individual Dimension: Strengthening Awareness and Improving Rights Protection

Individuals, as the owners of personal information and the direct beneficiaries of the rights associated with it, play a crucial role in the protection of personal information in the context of generative artificial intelligence. Active participation and cooperation at the individual level constitute an important social foundation for effective protection. The core objective of regulation at this level is therefore to enhance users' awareness of privacy protection and to improve mechanisms for safeguarding users' personal information rights. By encouraging users to actively participate in the collaborative protection of personal information, it becomes possible to establish a governance framework characterized by regulatory guidance, corporate self-discipline, and individual participation. In this way, the ultimate goals of technological optimization and legal regulation can be fully realized through the systematic protection of users' legitimate rights and interests.

On the one hand, efforts should be made to strengthen users' awareness of privacy protection. The interactive nature of generative artificial intelligence objectively increases the risk of information leakage. Users must therefore correct habits such as unintentionally entering sensitive information—including identification numbers and bank card details—during interactions with AI systems. Such practices may lead to excessive collection and misuse of personal information due to insufficient risk awareness. Accordingly, public education initiatives, science communication programs, and coordinated online and offline outreach should be used to disseminate knowledge about personal information protection in the context of generative AI. These activities should clarify common types of information leakage risks and provide practical prevention strategies, thereby improving users' ability to identify and prevent risks and encouraging them to protect their personal information proactively. In parallel, information processors should optimize product interfaces and embed clear and prominent risk warning functions. When users attempt to input sensitive information, real-time alerts—such as pop-up notifications—should be provided to guide users toward cautious behavior and to prevent information leakage at its source.

At the same time, a more comprehensive system for safeguarding users' personal information rights should be established. This requires creating more convenient and efficient channels through which users can exercise their rights. On the basis of the existing provisions of the Personal Information Protection Law of the People's Republic of China, users should be granted clearer and more effective rights concerning the deletion and management of their personal information. Specifically, the right to deletion allows users to request that processors delete personal information collected or stored about them, including personal information contained in training datasets and generated content. Processors should delete such information within the limits of technical feasibility and clearly inform users of the processing outcome. In addition, users should have the right to request the separation of their personal information from other datasets, requiring processors to store and process such information independently. This approach can effectively reduce the risks associated

with data integration and cross-analysis, which may otherwise lead to the failure of anonymization or the re-identification of individuals.

The effective implementation of these rights can strengthen users' practical control over their personal information and significantly reduce the risks of information leakage and misuse. It can also encourage users to move from passive defense toward active participation in personal information protection. Ultimately, this approach promotes a collaborative governance model in which users, platforms, and third parties jointly contribute to risk prevention and control, thereby safeguarding users' subject status and protecting their information rights in a substantive manner.

5. Conclusion

Generative AI is advancing at an unprecedented rate, but not at the cost of personal information rights and interests. The study has thus investigated the entire generative AI life cycle, from preparation to computation to generation and highlighted the current shortcomings of traditional legal regulation in the face of the new challenges of dynamic data processing and algorithmic black boxes. In fact, the existing systems of informed consent have become more and more bureaucratic, and the exercise of individual rights has become much more limited in practice.The paper suggests to establish a three-dimensional governance paradigm of algorithm, law, and users based on this. Technically, the principles of privacy by design should be integrated into algorithmic systems. From the legal perspective, the legal standards of the right to erasure should be enhanced, so as to strike a balance between the standards set and technological progress. User-level constraints on the exercise of personal information rights need to be lowered so that people can become active rather than passive participants in governance. In the future, the cooperation of the regulators, enterprises and users will be crucial to develop an agile and prudent governance system based on the rule of law. This type of system can help to balance technological progress with data protection, ensuring responsible and sustainable development of generative AI.

References

[1] Yang Q W, Tang Q. Conflicts and coordination between generative artificial intelligence and legal norms for personal information protection [J]. Henan Social Sciences, 2024, 32(12): 81–93.

[2] Luo v. Technology Co., Ltd., dispute over the right to privacy and personal information protection, Beijing Fourth Intermediate People's Court (also known as the Beijing Railway Transport Intermediate Court), (2022) Jing 04 Civil Final No. 494.

[3] Zhang X B. Research on personal information protection in training data for generative artificial intelligence [J]. Chinese Journal of Law, 2024, (06): 86–107.

[4] Lin Z, Ng Y L. Unraveling gratifications, concerns, and acceptance of generative artificial intelligence [J]. International Journal of Human-Computer Interaction, 2025, 41(17): 10725–10742.

[5] Ye X B. Personal information protection in the context of generative artificial intelligence: Paradigm transformation and improvement of regulatory rules [J]. Jurists, 2025, (04): 61–73, 192.