DOI: 10.23977/law.2025.040114
ISSN 2616-2296 Vol. 4 Num. 1

Research on Challenges and Legal Measures for Personal Data Protection in Generative AI

Wang Jiayi

Beijing University of Chemical Technology, Chaoyang, Beijing, China

Keywords: Generative Artificial Intelligence, Protection of personal data, Legal issues, Response strategies

Abstract: GenAI jeopardizes personal data through misinformation proliferation, invasive profiling, and algorithmic opacity. Current legal frameworks lack AI-specific adaptability, failing to address synthetic data governance and risk escalation. Urgent reforms demand adaptive legislation harmonizing GDPR/PIPL standards, strengthened enforcement mandates, and ISO 31700-certified privacy engineering. Key priorities are defining algorithmic accountability, creating systems for certifying synthetic content, and integrating Privacy-by-Design principles in AI development for a balance between innovation and data protection.

1. Challenges to personal information protection in generative AI

1.1 Overview of Generative AI Skills

GenAI uses Transformer architecture and self-review for contextual understanding, assisting industrial applications via iterative data training. Data processing risks arise from opaque algorithms, forced consent, and outputs that breach privacy and knowledgeable consent.[1]While Personal Information Protection Law mandates ethical vetting, current frameworks inadequately address synthetic content legality and accountability gaps. Mitigation requires embedding Privacy-by-Design protocols, establishing explainable AI certification systems, and aligning algorithmic transparency requirements with relative standards to reconcile innovation with GDPR/PIPL compliance.

1.2 Major challenges to personal information protection

GenAI's massive data ingestion risks sensitive privacy breaches, with current regulations like China's 2023 Interim Measures lacking enforcement teeth against synthetic data exploits. Regulatory arbitrage thrives in cross-border data governance gaps and ambiguous algorithmic accountability frameworks. Reforms need synthetic content watermarking per ISO/IEC 23053, energetic consent revocation like GDPR Article 17, and mandatory algorithmic impact assessments following NIST AI RMF guidelines. Essential safeguards include embedding differential privacy in transformer architectures, establishing real-time model monitoring under ISO 42001 certification, and creating multi-jurisdictional sandboxes for ethical AI validation.

These measures must balance innovation with strict liability regimes for privacy-invasive outputs, particularly addressing deep learning models' emergent data inference capabilities.

2. Legal analysis of personal information protection challenges in generative AI

The Personal Information Protection Act establishes the basic principles for the processing of information to prevent the misuse of personal information. These principles face challenges in their application in the face of generative artificial intelligence.[2]Therefore, it is necessary to examine the legality of data processing, risk assessment and information security from a legal perspective in order to improve the regulatory framework.

2.1 Analysis of the legality of data collection and processing

Generative AI's unclear data handling violates the data rights outlined in GDPR/PIPL, often breaching principles of necessity and knowledgeable consent.While China's Cybersecurity Law mandates explicit user authorization, AI corpus construction frequently bypasses transparency obligations regarding data retention periods and processing purposes. Essential safeguards involve real-time data tracking, energetic consent dashboards aligned with GDPR Article 15, and enforceable algorithmic transparency standards per NIST AI RMF. Cross-jurisdictional conflicts emerge in balancing China's data localization mandates with EU's right-to-erasure provisions, necessitating interoperable anonymization frameworks certified under ISO 31700. Mitigating risks demands strict adherence to accuracy/legality principles through watermarking synthetic outputs and establishing third-party audit mechanisms for training datasets.

2.2 Risk assessment and analysis of legal issues related to information security

China's AI governance framework integrates the Cybersecurity Law, Personal Information Protection Law (PIPL), and 2023 Generative AI Interim Measures, yet struggles with multimodal data provenance verification and algorithmic opacity. Critical gaps persist in defining "excessive data collection" under PIPL Article 6's necessity principle and establishing service provider liability thresholds under Civil Code Article 1195. The Cambridge Analytica case reveals widespread risks in synthetic data environments, emphasizing that existing regulations do not tackle the specific infringement issues posed by generative AI, such as multi-agent interactions, probabilistic decisions, and emerging privacy concerns. Judicial challenges intensify due to the latency of AI-induced damages and causal attribution complexities in neural network operations. Proposed solutions involve using ICO-like algorithmic impact assessments, adopting NIST AI RMF risk-tiering for training datasets, and creating flexible compliance frameworks that align PIPL's data localization requirements with GDPR-style rights. Courts must develop technical assessor systems to evaluate neural network decision traces under Civil Code Article 1165's tort provisions, while reinforcing real-time data flow monitoring through ISO 42001-certified audit mechanisms.

2.3 Adaptability analysis of legal norms and regulatory frameworks

Creating a shared model to define personal data usage limits in generative AI is difficult due to varied objectives and data usage levels.Generative AI is widely used in various fields, involving data of different types and sensitivities. While existing regulations govern data processing, new technologies may exceed the scope of existing regulations, resulting in insufficient supervision and legal loopholes.[3] The failure to promptly improve relevant regulations has resulted in delays in the appropriate regulation and supervision of generative AI, posing challenges to personal data protection. In addition, ambiguities in the terminology and definitions of existing legislation, such as “personal data generated” and “automated decision-making”, have led to difficulties and uncertainties in practical applications. It's essential to refine the terminology to ensure regulations accurately address the practical use of generative AI technology.In order to adapt to technological developments and address emerging risks and challenges, the repair and improvement of existing regulations is of great significance to better protect personal information and ensure the proper application of generative AI technology. [4]To effectively protect personal information in generative AI, it's important to discuss timely regulatory updates, clearer definitions in regulations, and standardized data flow norms.

In the field of personal information protection, the division of responsibilities among regulatory agencies may lead to competition in the face of possible infringement issues caused by generative AI. In China, the supervision of AI is shared by multiple departments, involving the State Administration for Market Regulation, the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the Ministry of Science and Technology, and other agencies. This cross-departmental supervision model aims to address the diverse legal risks posed by AI, but it may also lead to new challenges.Specifically, the fragmentation of regulatory responsibilities may lead to competition between different regulatory bodies, which may affect the efficiency of law enforcement due to conflicts of interest. In addition, due to the complexity and diversity of situations, regulatory bodies may evade their responsibilities. This lag means that regulators are unable to respond immediately to technological innovation, which may allow some companies to exploit legal loopholes and unclear definitions to circumvent legal requirements, thereby undermining the core of data protection. [5]

3. Legal measures for personal data protection in generative AI

Generative artificial intelligence applications pose different risks at various stages of personal information protection, and therefore compliance measures should be taken from the legislative, judicial, law enforcement and supervision links to protect them, integrate legal norms into technical processes, and make specific recommendations.

3.1 Improve the legal framework for personal data protection

GenAI governance necessitates GDPR/PIPL-aligned transparency mandates requiring service providers to disclose data processing purposes, retention periods, and third-party sharing through real-time dashboards. Data minimization principles under Cybersecurity Law Art.41 must integrate homomorphic encryption and federated learning architectures to ensure necessity compliance. User control rights, encompassing access/rectification/erasure under Civil Code Art.1034 and right-to-be-forgotten laws necessitate consent frameworks with blockchain audit trails. Regulatory upgrades should implement ISO 31700-certified privacy-by-design architectures, mandating third-party algorithmic audits for neural network opacity. Cross-border data flows demand harmonized protocols under Data Security Law Art.38, coupled with GDPR-calibrated penalty matrices reflecting infringement severity. Industry self-regulation requires establishing accredited review boards to certify differential privacy implementations and conduct synthetic data impact assessments. Prosecutorial guidelines must enforce strict liability for design defects per PIPL Art.69, while institutional mechanisms must enhance cooperation among agencies to avoid regulatory loopholes in multi-jurisdictional cases. [6]

3.2 Give full play to the remedial role of judicial channels in the protection of personal information

In judicial practice, the number of punitive compensation cases for personal information infringement is on the rise, especially violations by Internet companies in handling personal data rights and interests.[7] Under the current legal framework, the punitive damages for such infringements are generally low, reducing the financial risks faced by companies for the illegal use of personal data of the public, which may indirectly provide hidden incentives for Internet companies and weaken the deterrent effect of the law on personal data protection. The legal profession and regulators must assess the current punitive damages system to ensure compensation accurately reflects personal information's value and is an adequate deterrent. [8] This may involve a reassessment of the compensation amount and a comprehensive consideration of the consequences of the infringement, including the actual damage caused to the victim, the illegal gains of the enterprise, and the impact on the social trust system. The punitive compensation claim in the public interest litigation is intended to correct the imbalance of interests between the infringing company and the victimized user by increasing the compensation amount. However, punitive compensation precedents are not common in cases involving personal privacy information and data breaches. [9] In the case of consumer personal data rights infringement by Li Moumou, which was prosecuted by the Supreme People's Procuratorate, the Supreme People's Procuratorate demanded three times the compensation, which went beyond the traditional approach of making up for losses through punitive damages, and demonstrated that class actions are feasible in practice. In addition, in cases of personal data breaches, prosecutors may demand multiple damages, and judicial authorities may also initiate multiple typical data protection lawsuits to protect personal data rights and interests through legal means.

Article 98 of the “Rules for Handling Public Interest Litigation by the People's Procuratorate” clearly defines the general conditions for the application of public interest litigation, but does not provide specific guidance on public interest litigation involving public privacy. In lawsuits between large Internet technology companies and individuals, since the company has strong technical and economic resources, individuals face difficulties in obtaining evidence and a huge gap in economic strength, resulting in a low probability of individuals winning the lawsuit. Even in the rare cases where they are successful, the penalties are usually limited to minor punishments such as compensation, apologies, and deletion of data, which fail to meet the comprehensive protection standards set out in the Civil Code. Therefore, it is recommended that the resolution mechanism for public interest litigation to protect personal information be improved. The procuratorial authorities must promptly intervene in cases of personal information leaks and publicize typical cases to promote the protection of personal information. On the other hand, it is recommended that the judicial authorities formulate relevant legal interpretations to clarify the scope and standards of application of the Personal Information Protection Law, provide a specific legal basis for courts to hear personal information protection cases, and improve the efficiency and quality of the proceedings.

In cases of personal information infringement, attention needs to be paid to the allocation of liability and judicial remedies. Generative AI is not a legal entity, and commercial products are the actual form of application. It is difficult to disclose the design and operating status of complex algorithms, and it is difficult to determine who is responsible for the leakage. Therefore, the strict liability presumption in such cases should be broad and its application should be cautious. The infringement of citizens' personal data by generative AI products is closely related to their algorithm design, and it is necessary to determine whether the cause of the violation is related to the product design. Designers should be responsible for design defects within the scope of foreseeable risks; if the damage is caused by improper use by the user or owner, the responsibility should be borne by the user or owner. If generative AI technology automatically transfers user data to unauthorized third parties, the information processor and the third party may use algorithms and trade secrets as an excuse to avoid scrutiny, leading to technological hegemony and algorithmic black boxes, and even the illegal abuse or sale of personal data. AI developers, users, and relevant third parties should be accountable for personal data breaches without joint liability.The data subject may hold all offending entities liable, and then allocate responsibility within the offending entities based on fault.

In legal practice, it's essential to protect personal information and balance various rights. According to the current standard of proof in China, when a party claims damages, they must provide evidence to prove that they have suffered damage and the amount of damage, otherwise they will bear the consequences of failing to provide evidence. However, the rules of generative AI technology are complex, and it is difficult for parties to prove the specific damage caused by the technology. [9]Therefore, preventing future harm is the key. If harm does exist, the rights holder may require the infringer to take reasonable measures to avoid the technological risks. Article 11 of the Personal Information Protection Law emphasizes the construction of a sound personal information protection system to prevent and punish acts that infringe on personal data rights. Article 22 of the Data Security Law requires the establishment of a centralized, efficient, and authoritative system for data security risk assessment, information dissemination, resource sharing, and monitoring and early warning.[10] Introducing risk prevention in the field of generative AI will not affect the stability of the legal system. Although the Personal Information Protection Law and the Data Security Law clearly define the concept of risk prevention, specific risk prevention regulations have not yet been formulated. Establishing risk prevention rules at the level of data subjects and data controllers will help implement risk prevention.[11]

3.3 Clear responsibilities for law enforcement agencies and standardization of law enforcement procedures

GenAI's technical complexity demands specialized administrative enforcement units with cross-sectoral coordination capacities under PIPL Articles 60-62 mandates.Law enforcement should incorporate algorithmic governance to enhance swift data breach response, including audits, international evidence gathering, and GDPR-compliant cross-border enforcement. Essential reforms require standardized verification of data origins via compliance with Data Security Law Article 32, implementation of federated learning for source validation, and adjustable penalty matrices based on infringement severity and corporate revenue. Institutional safeguards require establishing independent technical review boards to audit neural network architectures, coupled with ISO 27001-certified data sanitization protocols mitigating synthetic misinformation risks. Prosecutorial guidelines must delineate strict liability thresholds for design defects under Civil Code Article 1165, while implementing presumption-of-fault reversals in public interest litigation contexts to address algorithmic opacity challenges. [12]

3.4 Improvement of the supervisory governance framework for generative AI

China's generative AI governance needs quick updates to close enforcement gaps in PIPL Article 60 and tackle algorithmic accountability issues. This reform focuses on creating cross-departmental oversight teams that include CAC cybersecurity experts, forensic analysts, and ISO 27090-certified auditors, equipped with blockchain-based data tracking systems that meet ISO 27555 standards.Critical infrastructure upgrades must include neural network monitoring protocols implementing NIST AI RMF risk classifications, particularly for biometric data streams requiring differential privacy safeguards. Platforms must implement CEN-CENELEC JTC 21-compliant watermarking for synthetic content and GDPR Article 17-compliant consent revocation. Cross-border activities require federated learning structures that follow UNCTAD's AI governance principles.

Algorithmic governance mechanisms require SHAP value-driven explainability thresholds in decision layers and ISO 42001-certified incident response systems with mandatory 72-hour breach notifications. Independent ethics boards must conduct quarterly model audits using adversarial neural networks for bias detection, complemented by cryptographic hashing verification of multimodal training data sources. Judicial adaptations under Supreme People's Court guidelines should create technical assessor panels specializing in transformer-based inference pattern analysis, particularly for evaluating emergent privacy harms under Civil Code Article 1165's tort liability provisions. This multilayered approach balances innovation with strict compliance through real-time model card disclosures, automated compliance dashboards, and sandboxed testing environments for high-risk AI applications.

4. Conclusion

GenAI governance demands legal-technical interoperability: Update regulatory frameworks balancing innovation with GDPR/PIPL-compliant safeguards through algorithmic transparency mandates and synthetic data audits. Future research must integrate socio-ethical impact assessments with federated learning architectures to address emergent cross-border data challenges.

References

[1] Mao Taota, Tang Gan, Ma Jiawei, Liu Jie. A study on the identification of factors influencing the willingness of artificial intelligence generated content (AIGC) users to adopt: A case study of ChatGPT [J]. Journal of Intelligence, Science and Technology, 2023, 40(8): 1-15.

[2] Dong Hao. The communication ethics risks of human-machine dialogue in the era of generative artificial intelligence and its response [J]. Yuejiang Academic Journal, 2024, 19(1): 1-11.

[3] Bai Long. Reflection and reconstruction: the ‘China solution’ to artificial intelligence in the process of Chinese-style modernisation – a summary of the special forum ‘Empowerment and innovation: artificial intelligence and Chinese-style modernisation’ [J]. Yuejiang Academic Journal, 2023, 18(6): 1-9.

[4] Guo Chenzhen. Coherent legal governance of generative Al: taking generative pre-trained models (GPT) as an example, Modern Law, 2023(3): 88-107.

[5] Ruan Shenyu: The tort law protection of personal information from the perspective of the Civil Code: focusing on factual uncertainty and its resolution. Jurist, 2020(4):29-39, 192.

[6] Wang Xiaolin, Xie Niyun. Future industry: connotative characteristics, organisational change and ecological construction [J]. Social Sciences Journal, 2023(6): 173-182.

[7] Chen Yuheng. Construction of a full-process compliance system for personal information protection in generative artificial intelligence [J]. Journal of East China University of Political Science and Law, 2024, 27 (02): 37-51.

[8] Wang Xiaoli and Yan Chi. Risk Issues and Regulatory Approaches of Large Generative AI Models: Taking GPT-4 as an Example [J]. Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition), 2023, 36(4): 1-11.

[9] Tong Xiaodong: Risk and Control: On the Protection of Personal Information in the Application of Generative Artificial Intelligence [J]. Political Science Forum, 2023, (04): 59-68.

[10] Gao Desheng, Ji Yan. Research on personal information security governance strategies in the era of artificial intelligence [J]. Journal of Intelligence Science, 2021, 39(8): 53-59.

[11] Ong L C J ,Seng J J B ,Law F Z J , et al. Artificial intelligence, ChatGPT, and other large language models for social determinants of health: Current state and future directions. [J]. Cell reports. Medicine, 2024, 5 (1): 101356-101356.

[12] Wilson E S ,Nishimoto M .Assessing Learning of Computer Programing Skills in the Age of Generative Artificial Intelligence. [J]. Journal of biomechanical engineering, 2024, 146 (5):