ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

Legal Regulation of Chinese Generative Artificial Intelligence

Gao Xiaowen[1,a], Deng Lingzhao[2,b,*]

[1]*School of Foreign Languages and Business, Shenzhen Polytechnic University, Shenzhen, China*
[2]*School of Undergraduate Education, Shenzhen Polytechnic University, Shenzhen, China*
[a]*gaoxiaowen@szpu.edu.cn,* [b]*denglingzhao@szpu.edu.cn*
[*]*Corresponding author*

Abstract: *While Generative Artificial Intelligence has profoundly transformed socioeconomic production, and business paradigms, it concomitantly encompasses data compliance risks, intellectual property (IP) infringements, and threats to social trust. China's current regulatory framework for Generative AI suffers from several structural deficiencies, including fragmented statutory provisions, ambiguous liability allocation mechanisms, and notable regulatory gaps. Adopting a risk-based governance approach, this study examines these major risks and outlines specific regulatory countermeasures. It argues that effective AI governance necessitates a paradigm shift toward a comprehensive framework that integrates statutory mandates with adaptive regulation, thereby striking a balance between fostering technological innovation and safeguarding digital rights.*

Keywords: *Generative Artificial Intelligence; Data Compliance; Intellectual Property; Social Trust and Ethic*

1. Introduction

Generative Artificial Intelligence (Generative AI) has radically altered the production paradigms, labor structures, and business models. With the continuous advancement of artificial intelligence technologies, establishing a regulatory and legislative regime for Generative AI is urgently needed. Under this background, scholars have conducted extensive research on it, prompting Chinese authorities to issue a series of important policy and regulatory documents, including *the New Generation Artificial Intelligence Development Plan (July 8, 2017), the Governance Principles for the New Generation of Artificial Intelligence—Developing Responsible Artificial Intelligence (June 17, 2019), the Anti-Monopoly Guidelines for the Platform Economy (February 7, 2021), the Provisions on the Administration of Deep Synthesis of Internet Information Services (December 2022), and the Interim Provisions for the Administration of Generative Artificial Intelligence Services (July 10, 2023).*

These regulatory documents aim to promote high-quality development of the artificial intelligence industry, improve the modernization of governance capacity, and standardize governance of AI development. However, effective regulation of Generative AI still confronts significant practical challenges. Therefore, this paper intends to examine the risks posed by generative artificial intelligence and enrich theoretical framework for Generative AI regulation.

2. Literature Review

Generative artificial intelligence (Generative AI) refers to a class of technologies that generate novel contents—such as text, images, audio, or video—by learning statistical patterns from pre-existing datasets. Since emerging on Gartner’s Hype Cycle for Emerging Technologies in 2020, generative AI has become a focal point of intense regulatory and academic discourse. [1]The launch of OpenAI's ChatGPT radically accelerated this trend, serving as a milestone that precipitated a wave of foundational research within the legal sphere.

Methodologically, current scholarship on the risks and governance of generative AI predominantly examines its conceptual frameworks, technical architectures, and operational mechanics. These foundational analyses serve to identify the technology's inherent vulnerabilities and formulate corresponding regulatory countermeasures. Song Huajian (2024) classified the process of Generative AI

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

into language model training and content generation, thereby systematically categorizing legal risks based on the underlying logic of AI and putting forward targeted regulatory approaches. [2] Liu Yanhong(2023) categorized risks of AI into data risks, algorithmic bias risks, and intellectual property risks, and proposed corresponding regulatory and protective measures. [3] Gu Nanfei(2023) incorporated a typological discussion on the social governance risks of Generative AI. [4] From the perspectives of the state, society, and individuals, Shang Jiangang (2023) analyzed the potential risks posed by Generative AI, such as violent conflicts, ideological infiltration, and increased criminal activities. He pointed out the existing problems, including ambiguous liability mechanisms, fragmented institutional frameworks, and the absence of a systematic legal system, and proposed constructing Meta-rules for Generative AI risk governance comprising collaborative governance, enhancement of transparency, assurance of data quality, and ethics-first principles. [5]

Extant literature on specific risks has predominantly centered on AI ethics, intellectual property, and personal data protection. Addressing the need to regulate these multifaceted challenges, Hou Dedong and Zhang Liping (2023) directed their attention toward network information ecological risks. They summarized the generation pathways of network information ecological risks as technological black boxes, gatekeeping failures, and structural embedding, advocating for regulation through due process-based algorithmic explanations and remediation via ecological impact assessments. [6]Wang Dazhi and Zhang Ting (2023) concentrated on the personal information risks of Generative AI. They highlighted the difficulties in the application of personal information protection rules[7]. Zhu Rongrong (2025) argued that Generative AI challenged the principles of informed consent, purpose limitation, and transparency at different operational stages, posing risks such as invasion of personal privacy, leakage of personal information, generation of false information, and discriminatory content. She proposed a dual approach of ex-ante prevention and ex-post compensation for damages. [8]

Regarding regulatory pathways, scholars aim to integrate agile governance and meta-regulation. Cheng Le(2023) proposed improving the legal regulation of Generative AI mainly through three approaches: revising and interpreting existing laws and regulations, issuing new general AI regulations, and promulgating specialized regulations in the field of Generative AI. [9] Combining ethics and laws, Luo Yi and Chen Jiaxing (2023) drew on Kelsen's normativity theory, advocated for the normalization of ethics to enhance its binding force and enforceability, sorted out its internal hierarchical relationships, and simultaneously used legal normalization to strengthen the regulation of the mathematical and logical operation of Generative AI. [10] Chen Bing and Dong Siyan (2023) advocated further promoting the classification and grading systems covering the entire life cycle of algorithm applications. [11]

In summary, existing research on Generative AI has systematically examined vulnerabilities across its technical lifecycle—from data collection and preparation to operation and generation—as well as domain-specific risks in various industrial applications. However, critical gaps remain. Data compliance issues, particularly concerning data provenance, usage, and accuracy, require deeper analysis. Furthermore, the specific nature of intellectual property threats must be clarified, while the broader ethical and societal trust issues induced by Generative AI urgently demand regulatory intervention.

3. Risk Analysis of Generative Artificial Intelligence

Generative AI introduces pervasive risks throughout its lifecycle, from data training to content generation. Chief among these are data compliance, intellectual property, and ethical challenges. Therefore, this study focuses on analyzing these three critical dimensions.

3.1 Data Compliance Risks

Although China maintains a robust data governance architecture spanning cybersecurity, data security, and personal information protection, AI's rapid advancement has starkly outpaced these statutory boundaries. As a result, existing legal norms are inadequate for executing effective ex-ante and ex-post regulation, precipitating the following compliance risks:

3.1.1 Compliance Risks Relating to Data Sources

The development and operation of Generative AI systems inherently depends on enormous volumes of data. Taking ChatGPT as an example, the GPT-3 language model employed over 175 billion parameters, while GPT-4 involved parameter scales several orders of magnitude larger. [12] It is evident that limited or narrowly scoped datasets are insufficient to support the development and operation of such systems, thereby compelling developers to obtain data through diverse channels.

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

One issue concerns the processing of personal information. Under China's Personal Information Protection Law, most entities are required to obtain informed consent from personal information subjects prior to processing their data. However, given the massive volume of data required for Generative AI training, it is practically impossible for developers to obtain individualized informed consent from each data subject. This creates a fundamental tension between the consent-based regulatory model and the data-intensive nature of Generative AI development, thereby generating inherent compliance risks.

Beyond the consent dilemma, legal uncertainty persists where developers rely primarily on publicly disclosed personal information. Although the Personal Information Protection Law permits the processing of public personal information, it remains unclear whether large-scale automated processing by Generative AI systems falls within the legally permissible "reasonable scope," or whether such processing may exert a material impact on the legitimate rights and interests of data subjects. These uncertainties introduce significant instability into compliance assessments throughout the operation of Generative AI systems.

Moreover, the Personal Information Protection Law of the People's Republic of China mandates compliance with the principle of data minimization, which requires that the processing of personal information should be confined to the minimum scope to achieve the intended purposes. The operational nature of Generative AI—which entails the collection and processing of enormous volumes of data—renders its practical deployment highly likely to violate the core principle of data minimization. Although developers typically formulate privacy policies stating that collected personal information will be used for contractually specified purposes, such policies rarely clarify whether personal data embedded in training datasets or model parameters are included within the contractual scope. At the same time, developers seldom provide substantive assurances that all collected personal information is genuinely indispensable to system operation, thereby exacerbating the risk of excessive data collection.

Finally, if the data utilized by Generative AI is obtained by developers through web crawling techniques, such conduct inherently entails significant compliance risks under Chinese law. Such practices directly violate China's existing cybersecurity legislation and are also highly likely to constitute acts of unfair competition as defined in China's Anti-Unfair Competition Law.

3.1.2 Compliance Risks Relating to Data Use

First, risks of data leakage permeate the entire lifecycle of Generative AI applications—from pre-training and model computation to output. [13] In practice, users often input personal information or commercially sensitive data into large language models. Such user-provided information may subsequently be incorporated into iterative training processes. How data security is ensured under this continuous learning model remains highly contested, and the effectiveness of existing safeguards is subject to significant doubt. Even where developers issue formal statements asserting that security measures are in place to protect training and input data, empirical experience demonstrates that data leakage risks persist and, in some cases, have already materialized.

Second, users' right of erasure faces substantial obstacles. Generative AI developers typically provide in their privacy policies that users retain the right to access, correct, and erase their personal data. However, an analysis of Generative AI's actual operational mechanics reveals that the model's inherent demand for massive datasets renders the exercise of the right to erasure exceptionally complex. Substantial uncertainty persists regarding whether Generative AI developers can fully erase the requested personal data and ensure no residual traces remain within the Generative AI system, even when users formally submit such deletion requests.

Third, cross-border data flows within Generative AI systems give rise to distinct legal risks. Generative AI is utilized not only by domestic users but also by international users. For domestic users, their data may be transmitted to overseas service providers via cross-border data transfer channels. Inevitably, such data interactions involve users' sensitive information, and the process of information is complex. This poses significant challenges for developers to provide comprehensive prior notification regarding all aspects of data collection, transmission, analysis, and other related activities.

3.1.3 Compliance Risks Relating to Data Reuse

The reuse of data inherently gives rise to compliance risks. As elaborated earlier, Generative AI engages in data exchange with users and relies on substantial datasets to underpin its training and learning processes. In the actual operation of Generative AI, it acquires substantial personal data or certain commercial data from users. Notwithstanding the informed consent obtained from users during their initial use of Generative AI, the reuse of such acquired data—for purposes such as self-training and

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

learning—requires notifying and obtaining renewed consent from users during the retraining phase. However, in practice, relevant enterprises or developers frequently fail to consistently comply with the principle of informed consent, thereby giving rise to compliance risks.

3.1.4 Compliance Risks Relating to Data Accuracy

Generative AI is confronted with risks associated with data accuracy. As noted previously, in the early stages of Generative AI training, the data utilized is often from publicly available online information. Nevertheless, such data may be inaccurate. Specifically, the information disseminated online does not constitute the full spectrum of relevant data, and consequently, the results derived from Generative AI's data analysis may be inaccurate. For instance, if Generative AI developers retrieve publicly accessible data from the internet—where the dataset may include false information, misleading data, or other forms of erroneous content—and input such data into Generative AI's training models without detecting the inaccuracies, the corresponding output results will inevitably be erroneous. Once the inaccurate information provided by Generative AI induces users to form erroneous perceptions, it will have profound adverse consequences.

3.2 Intellectual Property Risks

It is widely acknowledged that generative artificial intelligence, as a form of computer program, is protected by Intellectual Property Laws. [14] Nevertheless, the training of generative artificial intelligence gives rise to two distinct infringement risks.

Firstly, the training relies on massive volumes of data from diverse channels. Such datasets encompass not only third-party personal data but also copyrighted works owned by other right holders. Unauthorized use of such data—without authorization from the relevant right holder— creates a substantial risk of IP infringement. [15] An analysis of China's current IP legal framework reveals that IP protection—particularly copyright protection—hinges on the doctrine of fair use. In most cases, the inclusion of copyrighted content in generated outputs cannot readily be justified under the doctrine of fair use. The training of AI is without explicit authorization from authors when collecting or processing copyrighted information, thereby rendering their data collection practices susceptible to copyright infringement.

Furthermore, the risk of intellectual property infringement posed by generative artificial intelligence stems from lack of transparency. For example, by reassembling materials in response to specific prompts and functional demands, Generative AI systems produce new content that may be similar to prior works. Utilizing such AI-generated outputs for commercial purposes may violate the author's rights of reproduction and adaptation under Article 10 of the Copyright Law of the People's Republic of China. Moreover, the allocation of liability among developers, deployers, and end-users for IP infringement remains highly ambiguous. The complexities involved in defining legal boundaries and enforcing regulations highlight the profound challenges generative AI presents to modern intellectual property frameworks.

3.3 Social Trust and Ethic Risks

Generative Artificial Intelligence models possess the propensity to fabricate responses to queries they cannot comprehend, thereby generating substantial volumes of false information. Generative AI not only produces non-existent "facts," but also provides spurious corroboration for these fabricated claims. As reported by the Associated Press, when researchers instructed the online AI chatbot ChatGPT to compose an article "proving" a long-discredited and demonstrably false proposition, the system performed far more convincingly than anticipated. [16]This example illustrates that Generative AI systems have already acquired the technical capacity to produce false news and may, in the foreseeable future, become a major source of rumors and misinformation. Timothy Shoup, a senior advisor at the Copenhagen Institute for Future Studies (CIFS) predicted that 99% of online content will be AI-generated by 2025 to 2030[17]The influx of massive quantities of low-quality, formulaic, and erroneous texts, images, and videos produced by AI will exert a profound impact on the entire online content ecosystem, directly leading to the contamination of information sources. Concurrently, malicious actors may exploit Generative AI to generate disinformation for misleading the public or perpetrating fraudulent activities, thereby undermining information credibility and eroding public trust.

In May 2023, the Cyberspace Security Division of the Pingliang Public Security Bureau in Gansu Province uncovered China's first criminal case involving the fabrication and dissemination of false news

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

through generative artificial intelligence technology. In this case, the suspect used ChatGPT to modify and re-edit factual elements of previously published news reports and subsequently disseminated the fabricated content via self-media platforms, triggering widespread public attention and significant social controversy. Furthermore, Generative AI is increasingly being exploited for fraudulent purposes, such as generating fake social media accounts, which may facilitate identity theft, fraud, or other malicious acts that blur the distinction between genuine users and synthetic identities. For instance, Generative AI can synthesize fake voices mimicking individuals' speech patterns, generate specific facial images, or even forge videos. Such outputs not only exhibit high deceptive potential but also give rise to legal risks, including violations of personal information security and portrait rights, visual disinformation, journalistic misinformation, and systemic trust crises.

When general moral norms or core social values are inadequately embedded into the underlying algorithmic architecture of generative AI systems—or when ethical considerations are subordinated to efficiency-oriented imperatives—technological instrumentalization may occur, leading to deviations from accepted ethical standards. Because technological ethics is pivotal to the sustainable development of AI, these systems must be designed, developed, and deployed in accordance with an 'ethics-first' or 'ethics-by-design' approach to prevent misuse and safeguard human dignity.

4. Deficiencies in the Legal Regulation of Generative Artificial Intelligence

4.1 Inadequacy of Laws and Regulations

First, the legal and regulatory framework governing generative artificial intelligence (AI) remains underdeveloped in China. The primary regulatory instrument is currently the Interim Measures for the Management of Generative AI Services. Although these Measures impose formal requirements regarding the accuracy of generated outputs, the intrinsic characteristics of generative AI—most notably its reliance on opaque, "black-box" algorithmic models—severely impede effective ex-ante and ex-post regulation. In practice, not even developers can guarantee the substantive accuracy or reliability of their models' outputs. Should China enact legislation mandating the review of all AI-generated content, it would impose substantial operational costs on developers and stifle their initiative in research and innovation. Furthermore, while the Measures explicitly identify the liable parties, the operational ecosystem is complicated by the presence of individual end-users. Even if developers and service providers strictly fulfill their statutory obligations, they can neither perfectly predict system outputs nor maintain full-process oversight. Consequently, it is inevitable that some users will exploit generative AI to infringe upon the rights and interests of others.

Second, current laws and regulations remain overly broad and ambiguous. As noted, China's regulation of generative AI relies predominantly on the Interim Measures for the Management of Generative AI Services. However, significant interpretative divergences exist, particularly regarding issues arising from its application. For instance, in data processing, a major controversy is whether subjective fault must be attributed to the developer—or conceptually, the AI system itself—when data is used improperly or incompletely. Specifically, a model might be trained on flawed datasets without the developer's explicit knowledge. If the resulting output harms legitimate interests, considerable debate persists over whether liability can be lawfully attributed to the developer. Furthermore, while the Ethical Norms for the New Generation Artificial Intelligence stipulates that algorithms and training data should minimize bias and uphold inclusiveness, fairness, and non-discrimination, it merely establishes overarching principles. It fails to provide supplementary guidance for evaluating compliance or establish detailed, actionable metrics. Consequently, this regulatory gap creates tangible hurdles for both legal enforcement and practical implementation.

4.2 Ambiguity in the Liability Allocation Regime

Generative AI possesses extensive application scenarios, giving rise to a wide array of legal challenges, particularly concerning intellectual property rights. Taking copyright protection as an illustration, users may input keywords or prompts to activate the system, which then generates novel outputs through data integration and analysis. It is worth noting that the content generated by the system is inherently linked to the specific prompts entered by the user. In this context, highly contentious legal questions arise as to whether content generated by Generative AI qualifies as a "work" under copyright law, whether the AI system itself can be recognized as the legal author, and whether such outputs may constitute copyright infringement.

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

The legal complexities of Generative AI stem from its reliance on massive datasets and its processing methods, which involve rearranging and synthesizing data to generate outputs. Under current copyright doctrine, protection extends to the expression of ideas rather than the ideas themselves. Consequently, whether AI-generated outputs qualify for copyright protection remains highly debated. Some scholars argue that because these outputs are fundamentally algorithm-driven and lack the unique individuality of human expression, they cannot be regarded as copyrightable works. [18] Conversely, others contend that the algorithmic generation of content inherently constitutes a creative act, imbuing the outputs with characteristics that warrant legal recognition and copyright protection. [19]

Beyond the threshold question of copyrightability, Generative AI introduces multifaceted challenges regarding intellectual property infringement. A central controversy revolves around whether an AI system can be legally recognized as an "author," alongside concerns over tracing infringing outputs and securing practical remedies for rights holders. Driven by rapid technological iteration, the diverse infringement scenarios presented by Generative AI make backward tracing exceedingly difficult, creating substantial barriers to effective legal redress. These challenges are further exacerbated by the multiplicity of involved parties—spanning end-users, owners, developers, and service providers—which severely complicates the determination of liability. Accordingly, this landscape imposes stringent requirements for the swift refinement of China's legal and regulatory framework.

4.3 The Absence of an Effective Regulatory Regime

An analysis of China's current regulatory frameworks for artificial intelligence reveals several systemic deficiencies. First, China employs a multi-agency supervisory model for AI. Entities such as the State Administration for Market Regulation (SAMR), the Cyberspace Administration of China (CAC), and the Ministry of Science and Technology (MOST) share regulatory authority. This decentralized approach stems from AI's extensive application across market competition, data governance, and technological innovation. Consequently, different agencies formulate policies based on their domain-specific expertise. However, this fragmented structure often leads to the shirking of regulatory responsibilities. For instance, agencies may aggressively assert jurisdiction over highly profitable or high-profile AI sectors, while demonstrating bureaucratic inertia toward complex domains that offer limited regulatory dividends. Such misaligned incentives result in uneven resource allocation, conflicting regulations, and ultimately, the jeopardization of public interests.

Second, conventional regulatory frameworks are markedly outdated. The rapid evolution of Generative AI has sharply differentiated it from traditional AI. Legacy oversight methods, which heavily emphasize algorithmic interpretability, are fundamentally incompatible with the non-deterministic operational logic of Generative AI. Because outputs are highly sensitive to diverse and idiosyncratic user inputs—where even identical prompts from different users can yield varying results—regulators attempting to interpret these algorithms cannot reliably predict system behaviors, rendering traditional intervention models unfeasible. [20] Simultaneously, the dynamic expansion of training data and evolving analytical capabilities have made it exceedingly difficult for static legal norms to effectively govern constantly shifting datasets. Furthermore, existing complaint and reporting mechanisms remain inadequate. The initial Draft for Comment of the Interim Measures proposed obligating service providers to filter content based on user reports regarding non-compliant outputs. Although this provision was removed from the officially promulgated Measures, it reflects Chinese legislators' growing focus on refining grievance mechanisms. While the current Interim Measures retain provisions requiring service providers to establish and improve complaint and reporting channels, these mandates remain overly general and lack actionable guidance, severely undermining their practical efficacy. Furthermore, while the Regulations on Algorithmic Recommendation Management permit users to submit complaints directly to relevant authorities, the Regulations on Deep Synthesis Management conspicuously lack any equivalent provisions for service users.

5. Regulatory Proposals for AI Risk Governance

Generative AI has become deeply integrated into modern society. Without robust regulation, the legitimate interests of rights holders cannot be adequately protected, which, in severe cases, could disrupt public order. Therefore, this paper proposes the following regulatory recommendations to mitigate the risks associated with artificial intelligence.

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

5.1 Improving the Legal and Regulatory Framework

First, it is imperative to enact laws. While the current Interim Measures can effectively curb the disorderly development of Generative AI, the technology's inherent complexity introduces diverse and intricate risks, significantly limiting the practical implementation of existing norms. Consequently, China must thoroughly evaluate the necessity and feasibility of drafting dedicated laws and regulations. Specifically, a targeted regulatory framework should be established, categorized by the type of AI-generated content and its associated risk levels. Relevant law enforcement authorities should conduct regular data risk assessments, leveraging legislation to enforce the transparency and interpretability of Generative AI algorithms. This requires developers to explain, in accessible language, how personal data is utilized and the intended purpose of the generated outputs. Furthermore, developers must establish clear appeal channels for users facing potential algorithmic or output-related infringements. In cases involving significant disputes—such as those concerning network security—developers should be mandated to provide detailed data disclosures to judicial or regulatory bodies, provided these authorities strictly maintain data confidentiality.

Second, complementing statutory provisions, China should integrate soft law mechanisms into its governance framework. During the lifecycle of Generative AI, much of the data utilized and generated is inherently immutable; once processed, subsequent modification is often unfeasible. Consequently, China’s prevailing reliance on ex post legal remedies proves structurally inadequate for timely intervention, failing to effectively mitigate ongoing harm in cases of infringement. Furthermore, the highly technical and opaque nature of Generative AI exacerbates information asymmetry between developers and relevant stakeholders. To navigate these systemic challenges, China must formulate soft law instruments, such as normative guidelines regulating the deployment and operational application of Generative AI. Specifically, developers and service providers should be mandated to conduct rigorous data risk assessments during the pre-deployment phase, transparently articulate potential risks, and submit these evaluations to regulatory authorities. Additionally, developers must secure explicit, unbundled consent from data subjects prior to data utilization, ensuring robust safeguards against data abuse throughout the algorithmic lifecycle.

5.2 Clarifying Legal Liabilities

Determining whether Generative AI possesses quasi-human agency and the capacity for liability is a fundamental prerequisite for resolving accountability issues in AI deployment. First, regarding the attribution of volitional capacity, Generative AI has demonstrably acquired robust cognitive-like processing capabilities. While structurally distinct from human neural networks, AI decision-making algorithms produce outcomes that closely parallel human cognition; furthermore, being devoid of emotional interference, its data-driven conclusions can frequently surpass human precision in specific domains. Through advanced data synthesis and algorithmic analysis, Generative AI exhibits functional traits analogous to human volition. Its capacity for evaluative judgment is further evidenced by its efficacy in predictive modeling. Second, concerning the capacity to act (actus reus), Generative AI increasingly substitutes for human labor across various professional sectors. By executing complex, automated tasks—such as insurance claims processing and video editing—it exercises a form of functional agency, which theoretically establishes a foundation for attributing proportional legal responsibilities. Constructing a liability framework for Generative AI necessitates clarifying several core dimensions. Primarily, it must be established that any liability capacity attributed to Generative AI is inherently limited. Throughout the AI lifecycle, specific legal entities—encompassing developers, controllers, operators, and potentially the AI system itself—must be designated to bear commensurate responsibility. Crucially, while Generative AI might be accorded a nascent form of legal recognition (e.g., limited electronic personhood), it does not constitute a full legal entity.

The mechanism of liability attribution should formally integrate the doctrine of "piercing the artificial intelligence veil." Assessing the liability capacity of Generative AI requires a holistic evaluation of variables, particularly the degree of human control and intervention during its operation. If erroneous or harmful outputs stem directly from the AI's autonomous systemic malfunctions or algorithmic opacity (the "black box" effect), the AI system itself should be assigned limited liability, with developers and controllers assuming supplementary liability. Conversely, if damages result from an operator's malicious input or intentional misuse, primary liability must strictly rest with the human operator.

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

5.3 Establishing an Effective Regulatory System

The risks associated with Generative AI are multifaceted, stemming from diverse sources that need cross-sector collaboration among stakeholders.[21] To mitigate these risks, the state should establish a dedicated AI regulatory authority and implement a regulatory sandbox.

In the long term, as AI integration becomes more pervasive, the current multi-agency supervision model—which often lacks efficiency and risks infringing upon legitimate rights—will become inadequate. A dedicated department, staffed by professionals with a robust technical understanding of AI, can provide more focused governance. This agency should also recruit and train legal experts to bridge the gap between technology and law. Furthermore, an expert database should be maintained to provide authoritative guidance and resolve disputes in highly technical or specialized AI domains.

Second, a regulatory sandbox should be implemented to ensure the safe deployment of Generative AI. This mechanism allows licensed developers to test AI systems within a controlled environment during the training and experimental phases. By temporarily lowering entry thresholds and relaxing certain restrictions, the sandbox fosters an ideal space for innovation. It enables developers to evaluate data protection efficacy and potential risks before market launch. Ultimately, the regulatory sandbox harmonizes innovation with supervision, allowing authorities to gain a comprehensive understanding of AI risks while facilitating information exchange between regulators and developers.

6. Conclusion

Despite its manifest benefits, Generative AI presents profound risks that need an adaptive legal response. Policymakers should integrate Generative AI -specific oversight into current legal systems, adopting a governance stance that balances innovation with accountability. Such a dual-pronged approach must prevent both regulatory overreach and the erosion of stakeholders' interests. Concurrently, Generative AI developers should establish formal appeal channels to provide right holders with viable pathways for legal relief and restorative justice in the wake of infringements.

Acknowledgement

Funds:

1) Shenzhen Polytechnic University Research Fund (No. 6026310006S);

2) Funded by the Phase III Program (Grant No. 6025310002Q) of the Institute for Economic and Social Development at Shenzhen Polytechnic University.

References

[1] Chen, J. F. (2023, January 11). Generative AI continues to explode: Industrial opportunities are expanding infinitely. Communication Information News, 008.
[2] Song, H. J. (2024). Legal risks and governance path of generative artificial intelligence. Journal of Beijing Institute of Technology, (3), 134–143.
[3] Liu, Y. H. (2023). The three major security risks and legal regulation of generative artificial intelligence: Taking ChatGPT as an example. Oriental Law Review, (4), 29–43.
[4] Gu, N. F. (2023). The emergent intelligence, risk regulation and industrial regulation of generative artificial intelligence. Jingchu Law Review, (3), 70–83.
[5] Shang, J. G. (2023). On the meta-rules for risk governance of generative artificial intelligence. Oriental Law Review, (3), 4–17.
[6] Hou, D. D., & Zhang, L. P. (2023). Legal regulation of network information ecological risks in the context of generative artificial intelligence. Social Sciences Research, (6), 93–104.
[7] Wang, D. Z., & Zhang, T. (2023). Risks, dilemmas, and countermeasures: Personal information security challenges and legal regulation caused by generative artificial intelligence. Journal of Kunming University of Science and Technology (Social Sciences Edition), 23(5), 8–17.
[8] Zhu, R. R. (2025). Challenges and responses of generative artificial intelligence to personal information protection. Journal of Chongqing University (Social Science Edition), (4), 222–235.
[9] Cheng, L. (2023). Legal regulation of generative artificial intelligence: From the perspective of ChatGPT. Journal of Political Science and Law, (4), 69–80.

ISSN 2706-6827 Vol. 8, Issue 2: 11-19, DOI: 10.25236/IJFS.2026.080202

[10] Luo, Y., & Chen, J. X. (2023). Legal response to the anomie risks of generative artificial intelligence from the perspective of Kelsen's normative theory. Journal of Guizhou University (Social Science Edition), 41(5), 98–108.
[11] Chen, B., & Dong, S. Y. (2023). Algorithmic risks and governance bases of generative artificial intelligence. Study and Practice, (10), 22–31.
[12] Guo, C. Z. (2023). The coherent legal governance of generative AI: Taking the generative pre-training model (GPT) as an example. Modern Law Review, 45(3), 88–107.
[13] Zhao, Z. Y. (2024). Data security and countermeasures of generative artificial intelligence. Information and Documentation Services, 45(2), 30–37.
[14] Chen, B. (2023). Risk challenges arising from the innovative development of artificial general intelligence and their legal responses. Intellectual Property, (8), 53–73.
[15] Zheng, X., & Zhu, S. R. (2023). Legal risks and regulation of generative artificial intelligence. Changbai Journal, (6), 80–88.
[16] China Youth Network. (2023, February 5). AI's alternative talent: Creating and spreading falsehoods. http://news.youth.cn/gj/202302/t20230205_14298793.htm
[17] Hood, L. L. (2024, March 5). Experts say that soon, almost the entire internet could be generated by AI. Futurism. https://futurism.com/the-byte/ai-internet-generation
[18] Li, R. Y., Wang, L., & Jia, J. Y. (2023, February 21). The intellectual property risks behind ChatGPT. China Youth Daily, 06.
[19] Wu, H. D. (2020). The copyright law questions of AI-generated works. Peking University Law Journal, 32(3), 653–673.
[20] Jiang, Y. C. (2024). Legal regulation of data risks of generative artificial intelligence. Journal of Taiyuan University of Technology (Social Science Edition), 42(1), 29–35.
[21] Cai, S. L., & Yang, L. (2023). Research on the risks and collaborative governance of ChatGPT intelligent robot applications. Information Studies: Theory & Application, 46(5), 14–22.