ISSN: 2710-0170

Risk-Based Regulation of Generative Artificial Intelligence

Zijin Huang

Law School of Beijing Normal University, Beijing, China

Abstract

The emergence of Generative Artificial Intelligence (Generative AI) has transformed the operational mechanisms of traditional artificial intelligence, and advances in AI technology have rendered conventional regulatory rules increasingly inadequate to address the technological development of Generative AI. Regulatory frameworks therefore need to be optimized and expanded on the basis of actual legal risks, as a response to both technological progress and practical regulatory demands. The sound and orderly development of Generative AI depends upon the safeguards provided by regulatory rules. In light of the technical characteristics of Generative AI, regulation should be grounded in an analysis of its operational mechanisms and legal risks.

Keywords

Generative Artificial Intelligence, Technological Regulation, Legal Liability.

1. Operational Mechanisms of Generative Artificial Intelligence

With the continuous advancement of artificial intelligence technologies, Generative Artificial Intelligence (Generative AI) has been widely applied across diverse fields. Owing to its scalability and general-purpose applicability in multiple domains, Generative AI possesses broad application potential and promising prospects for future development. The operational mechanisms and technical characteristics of Generative AI differ fundamentally from those of traditional artificial intelligence, and conventional regulatory rules exhibit inherent limitations in addressing the risks posed by Generative AI, thereby giving rise to new regulatory challenges. The risks associated with the application of Generative AI are distinctive in nature. Accordingly, regulatory analysis should be conducted from the perspective of the operational mechanisms and technical features of Generative AI, with a comprehensive consideration of relevant factors—such as system operation and technological attributes—in order to refine and improve regulatory approaches. In practice, Generative AI is capable of efficiently generating various forms of content, including text, images, and videos, based on user instructions. From a technical standpoint, it demonstrates strong data collection capabilities and self-reinforcement mechanisms, enabling systems to autonomously evolve to complete designated tasks, while the quality of generated outputs continues to improve through iterative processes.

The operational mechanisms of Generative Artificial Intelligence (Generative AI) are, in essence, a form of logical and computational processing, characterized by a high degree of technical specialization. The first component involves the collection of training data and preliminary data analysis, whereby the quantity and quality of collected data directly affect the accuracy of generated outputs. Generative AI is driven by large-scale models, which rely on massive volumes of training data to optimize system performance, enhance interaction with users, and improve the precision of generated content. The second component lies in the self-iterative capabilities of Generative AI. Through machine learning, algorithms are able to engage in autonomous learning based on data analysis without direct human or programmatic intervention, thereby generating new algorithmic models and independently determining how to execute specific tasks. [1] Large-scale models employ algorithmic processing to conduct deep learning on collected data without direct human intervention, continuously optimizing their

ISSN: 2710-0170

intelligence levels and decision-making frameworks. Through this process, they acquire the capacity to accurately interpret the meaning of user instructions and to generate appropriate responses.

Improving the regulation of Generative Artificial Intelligence should take its operational mechanisms as the logical point of departure, be grounded in the technological development of Generative AI, and enhance the functions of risk prevention and risk mitigation by addressing relevant legal risks and legal issues. Within the operational mechanisms of Generative AI, the refinement of regulatory approaches should give due consideration to both the comprehensiveness and effectiveness of regulation, so as to ensure the safe and orderly development of Generative AI. The prerequisite for regulation and legislation lies in a thorough understanding of artificial intelligence technologies and industrial development practices, as well as a profound grasp of their underlying patterns of development. [2] The underlying logic of data- and algorithm-driven technologies in Generative Artificial Intelligence is not directly observable during system operation. Users therefore often passively accept AI-generated outputs without a meaningful understanding of the underlying operational mechanisms. The risks associated with Generative AI permeate all stages of its lifecycle, including data collection, algorithmic training, and content generation. Moreover, the operation of Generative AI involves the participation of multiple actors, and risks arising across different stakeholders or at different stages of research, development, and application are characterized by mutual interaction and spillover effects. In the absence of effective liability attribution and accountability mechanisms, such risk interdependencies give rise to significant legal risks and regulatory challenges in practice. These challenges exert a structural impact on existing regulatory rules, rendering current regulatory regimes incapable of direct application to the operational mechanisms and technological characteristics of Generative Artificial Intelligence.

2. Legal Risks of Generative Artificial Intelligence

Regulation of Generative Artificial Intelligence requires a careful balance between technological development and legal risk control. Risk-based regulation of artificial intelligence may be regarded as a legislative technique designed to ensure the proportionality between responsibilities and obligations. Within this framework, risk functions as a regulatory tool, on the basis of which enforcement priorities and regulatory objectives are determined in accordance with the severity and likelihood of actual or potential harm. [3] The legal risks associated with Generative Artificial Intelligence (Generative AI) permeate the entire lifecycle of artificial intelligence, encompassing the stages of research and development, content generation, and user utilization. As such risks predominantly arise within the virtual and networked environment, they are often difficult to detect in a timely manner. Accordingly, these risks are characterized by a high degree of pervasiveness and systemic interdependence.

2.1. Data Risks

Generative Artificial Intelligence relies on the continuous collection and analysis of raw data to learn and optimize large-scale models, thereby adapting to diverse application scenarios. The data collected and processed in this context are marked by features of large-scale aggregation and automation. From a regulatory perspective, data risks in Generative AI may be classified into three primary categories: data collection risks, data analysis risks, and data leakage risks. Such risks extend across multiple stages of the data lifecycle, including data collection, use, and storage, and are manifested in the following respects:

Data Collection Risks. The data collected by Generative Artificial Intelligence (Generative AI) systems are predominantly sourced from publicly accessible channels and are characterized by a high degree of diversity. Such data may include publicly available information, user behavioral data, corporate data, and personal data involving privacy interests. The complexity and

ISSN: 2710-0170

heterogeneity of data sources increase the likelihood that datasets contain erroneous, inaccurate, or unverified information. Once incorporated into training datasets, such defects may be implicitly carried forward into subsequent stages of analysis and content generation, thereby giving rise to risks of data contamination. Moreover, as the training data of Generative AI are largely derived from public sources, risks of excessive data collection and improper or unreasonable data use are inherent. In the course of data collection and processing, Generative AI systems may also encompass personal data collected without proper authorization, ultimately infringing upon individual privacy rights and compromising personal information security.

Data Analysis Risks. The data used to train Generative Artificial Intelligence models are predominantly unlabeled and lack manual verification. Where such data contain false, inaccurate, or unverified information, the authenticity and accuracy of generated outputs may be adversely affected, thereby undermining the credibility and reliability of Generative AI systems and giving rise to data bias risks. In addition, because AI-generated content typically does not disclose the sources of the underlying data, effective traceability of data origins is impeded, rendering the composition of training datasets uncertain. Generated outputs may further contain personal information that has not been properly identified, filtered, or processed. Compared with traditional artificial intelligence, Generative AI involves a significantly expanded scale and diversity of data collection, which substantially increases the difficulty of regulatory oversight. From a legal perspective, the use of collected data to train large-scale models constitutes an act of data processing. Where such analysis is conducted without appropriate authorization, it may infringe upon the lawful rights and interests of others and give rise to data security and compliance risks.

Data Leakage Risks. During interactions between users and Generative Artificial Intelligence (Generative AI) systems, significant data security risks may arise. Owing to users' limited understanding of the operational mechanisms of Generative AI, individuals may inadvertently disclose sensitive personal information in the course of use, such as identity data, contact information, or other confidential details. Such information may be collected, stored, or processed by the system without the user's full awareness, thereby increasing the likelihood of unauthorized access, misuse, or leakage of personal data. [4] The memory and data retention functions of such systems may further result in the repeated storage and utilization of user data. Moreover, through continuous data analysis, Generative AI can construct detailed user profiles for targeted content delivery or recommendation, thereby intensifying the risk of data leakage. In addition, Generative AI systems may be exposed to malicious cyberattacks, and vulnerabilities in their data storage or processing mechanisms could be exploited by hackers, leading to serious data security breaches.

2.2. Algorithmic Risks

Technical Risks of Algorithms. In the commercial context, algorithms constitute core trade secrets of artificial intelligence developers. Driven by market incentives, enterprises are generally unwilling to fully disclose the internal operational mechanisms of their algorithms. As a result, at the technical level, natural persons face substantial difficulties in understanding the decision-making logic of Generative Artificial Intelligence algorithms. Moreover, the lifecycle of an algorithm—from development to deployment—is inherently iterative, involving multiple intermediate stages and derivative outcomes. Continuous iteration and optimization further exacerbate the opacity of algorithmic decision-making, thereby increasing the unpredictability of algorithmic behavior and the difficulty of effective regulatory oversight. Between algorithmic inputs and outputs, there often exists a non-explainable "black box," within which the reasoning process of algorithmic decisions cannot be clearly articulated or verified, giving rise to significant technical and regulatory risks. [5] The technical risks of

ISSN: 2710-0170

Generative Artificial Intelligence algorithms arise from both the intrinsic complexity of the algorithms and the concealed nature of their operational mechanisms. Difficulties in algorithmic explainability constitute a latent and inherent deficiency in the current development of Generative AI. Due to the technical limitations of algorithmic systems, such opacity gives rise to implicit and potential technological risks that are not readily observable, verifiable, or controllable.

Derivative Algorithmic Risks. First, during the stages of data collection and processing, Generative Artificial Intelligence may be exposed to data contamination. Owing to the non-traceability of data sources and the opacity of algorithmic operations, erroneous information embedded in generated outputs may exhibit a high degree of deceptiveness and is difficult to detect. As a result, algorithms may present false information in a manner that appears authentic. Errors arising in the course of algorithmic operation may lead users to form incorrect judgments regarding generated content, thereby giving rise to trust-related risks.Second, algorithms may be maliciously exploited for the generation of false or misleading information, and may even be employed to facilitate unlawful activities. Given the lack of transparency in algorithmic logic and the high level of technical specialization involved, regulatory authorities face significant difficulties in accurately identifying and allocating risks across different stages of algorithmic operation once such risks materialize. Moreover, algorithm development may reflect the subjective preferences or biases of developers, giving rise to risks of algorithmic discrimination. Finally, during the process of autonomous learning, if algorithms are trained on erroneous or misleading data, they may internalize biased value orientations, thereby adversely affecting the accuracy and reliability of generated content.

3. Regulatory Dilemmas of Generative Artificial Intelligence

In light of the operational mechanisms and risk profile of Generative Artificial Intelligence (Generative AI), traditional regulatory frameworks have difficulty achieving effective governance and therefore require further refinement in response to the specific risks posed by Generative AI. The risks associated with Generative AI not only encompass those of traditional artificial intelligence, but also give rise to novel risks as a result of its disruptive technological nature. Consequently, the scope and boundaries of regulation are in a constant state of flux. The forms of harm and technological risks generated by Generative AI are often concealed, making it difficult to detect and accurately identify the sources of risk, which in turn exacerbates regulatory challenges. Risk-based regulation seeks to regulate artificial intelligence in the course of technological development, while simultaneously safeguarding innovation through regulation. The governance of Generative AI involves a multiplicity of stakeholders and complex legal relationships, and the continuous iteration of AI technologies further complicates the identification and allocation of rights and responsibilities among different actors. As Generative AI technologies continue to evolve, their impact on regulatory rules is not limited to technological upgrading, but entails a fundamental transformation of regulatory philosophy. Regulatory rules that are incompatible with technological development should therefore be revised in a timely manner. Accordingly, regulatory approaches should shift from predominantly ex post regulation to a full-process regulatory model, encompassing supervision from the research and development stage, appropriate intervention during system operation, and legality review of generated outputs. On the one hand, legal issues arising from artificial intelligence implicate both public law and private law, and manifest differently across diverse application scenarios, giving rise to varied regulatory challenges. [6] On the other hand, the development of artificial intelligence technologies is characterized by a high degree of uncertainty and ambiguity. When combined with the aforementioned legal complexities, these factors render traditional regulatory rules ill-equipped to respond effectively to the risks

ISSN: 2710-0170

arising from the rapid iteration of Generative Artificial Intelligence (Generative AI). As Generative AI continues to evolve, its technological capabilities may outpace the scope of existing regulatory frameworks, preventing regulators from responding to emerging risks in a timely manner. Accordingly, regulatory rules should take into account future trends in artificial intelligence development as well as the evolving landscape of legal risks, so as to enhance regulatory foresight, adaptability, and responsiveness.

There exists a concomitant relationship between legal risks and technological development. Accordingly, regulatory rules should be contingent upon the prevailing technological conditions of artificial intelligence and be flexibly adjusted in response to technological evolution and changes in the risk landscape. Generative Artificial Intelligence (Generative AI), as a form of deep synthesis technology, is characterized by cross-domain generality and strong generative capacity. As a result, risks intersect across multiple sectors and exhibit multidimensional complexity, making fragmented or sector-specific regulation insufficient to effectively address systemic risks. Effective regulation therefore requires regulators to possess specialized expertise in order to keep pace with developments in AI technologies and related industries. However, owing to the high degree of technical specialization inherent in Generative AI, government regulation may face regulatory gaps in certain professional domains, giving rise to the risk of regulatory absence or insufficiency. Moreover, due to the general-purpose nature of Generative AI, risks originating at the research and development stage may propagate into the application and deployment stages, thereby generating potential security risks. Regulatory rules must therefore be aligned with downstream application scenarios. The technical characteristics of Generative AI necessitate a flexible regulatory framework capable of adapting to diverse use contexts. From a technological perspective, risks associated with Generative AI are highly dynamic and unpredictable. Such risks do not arise solely within isolated domains but rather constitute systemic risks spanning multiple fields, with close interconnections among different risk categories. These risks are marked by uncertainty and latency, remain in a constant state of evolution, and are difficult to anticipate or prevent ex ante.

Data-related risks and algorithmic risks may undermine social equity, placing certain actors at a structural disadvantage in the use of Generative Artificial Intelligence (Generative AI) and thereby giving rise to digital divide risks. From research and development to deployment and application, Generative AI involves the participation of multiple actors. Once such systems enter the market, they may operate beyond the direct control of their developers and enter a stage of autonomous evolution. At this stage, the allocation of responsibilities among relevant actors becomes increasingly ambiguous. Accordingly, regulatory rules should take into account the distinct roles played by different actors at different stages of the Generative AI lifecycle, and clearly delineate their respective responsibilities. Moreover, the risks associated with Generative AI are inherently interconnected and are often difficult to identify at any single stage in isolation. Effective regulation therefore requires a comprehensive consideration of upstream–downstream relationships spanning the entire lifecycle from research and development to application, as well as the allocation of rights and obligations among different actors. Within the regulatory framework, stage-specific regulatory measures should be designed in accordance with the risk profiles of different phases, and a collaborative governance mechanism should be established in which multiple stakeholders jointly participate in oversight. While such an approach is necessary to address the systemic nature of Generative AI risks, it also significantly increases the complexity of regulation.

Data and algorithms constitute the core of the operational mechanisms of Generative Artificial Intelligence (Generative AI). However, both are subject to inherent technical limitations, and the regulation of data and algorithms inevitably involves the balancing of interests among multiple stakeholders. Moreover, the technical characteristics of Generative AI may be maliciously exploited for criminal purposes, further increasing the difficulty of regulation.

ISSN: 2710-0170

Generative AI is highly data-dependent, and data-related risks exhibit characteristics of contagion and amplification. At the data level, regulatory dilemmas arise because data risks permeate the entire lifecycle of Generative AI, encompassing data collection, data processing, and data output. Data risks occurring at any single stage may affect downstream operational mechanisms and generated outputs, thereby undermining users' trust in Generative AI systems. Owing to the lack of unified standards for data collection and processing, multiple latent risks are embedded in data practices. In response to such risks, regulatory rules should be enhanced in terms of both comprehensiveness and effectiveness. Furthermore, the manner in which Generative AI processes data is characterized by a high degree of opacity, including practices such as secondary data use, which makes it difficult to trace the sources of risk and to accurately identify responsible actors. At the algorithmic level, regulatory dilemmas stem from the combined effects of the high degree of technical specialization of Generative AI algorithms and the opacity of their operational mechanisms. These factors may lead to a loss of algorithmic control and create severe information asymmetries between regulators and regulated entities, resulting in insufficient institutional constraints on algorithmic operation standards. Algorithms are inherently dynamic and capable of autonomous evolution. Once deployed in real-world applications, they may deviate from preconfigured parameters, rendering risks difficult to predict accurately. The opacity of algorithmic decision-making processes and logic further complicates regulatory oversight, contributes to legal uncertainty, and limits the effectiveness of regulation in preventing and mitigating legal risks.

4. Optimization of the Regulatory Framework for Generative Artificial Intelligence

4.1. Risk-Based Tiered Regulation

Generative Artificial Intelligence (Generative AI) remains at a stage of continuous development. Accordingly, regulatory rules must adapt to the evolving trajectory of AI technologies. The primary objective of regulation is risk prevention, so as to ensure the safety of Generative AI applications and the orderly development of artificial intelligence technologies. Risk-based tiered regulation emphasizes an overall and holistic assessment of application risks associated with Generative AI. It treats risk as a regulatory instrument and takes risk assessment as the foundation of regulatory intervention, adopting differentiated regulatory approaches in accordance with the severity and likelihood of risks, and allocating regulatory resources in a targeted manner across diverse application scenarios. Given the high degree of technical specialization inherent in the operational mechanisms and technological characteristics of Generative AI, tiered regulation may be structured around two principal dimensions: technical risks and social equity. This dual-dimensional framework facilitates more precise identification and localization of risks. On the basis of clear risk categorization, differentiated regulatory measures should be adopted. Regulatory strategies should vary in accordance with the degree of potential harm, the probability of risk occurrence, and broader trends in AI technological development, thereby enabling precision regulation. In relatively low-risk and safety-assured domains, a more permissive regulatory approach should be applied to promote technological innovation and development. In such contexts, regulatory intervention should be limited to ensuring compliance with relevant technical standards, avoiding excessive interference. By contrast, in high-risk domains, more stringent regulatory measures should be imposed, including rigorous risk assessment procedures. Regulatory authorities should retain the discretion to dynamically optimize and adjust regulatory strategies in response to evolving risk assessment outcomes, thereby ensuring both effective risk control and regulatory adaptability.

Adopting regulatory and risk-prevention measures from multiple perspectives constitutes a flexible regulatory approach. Such an approach is capable of safeguarding safety and

ISSN: 2710-0170

controllability while simultaneously preserving adequate space for the development of artificial intelligence technologies, and is therefore consistent with prevailing trends in AI innovation. A tiered regulatory model should be dynamically adjusted in response to changes in the risk profile of Generative Artificial Intelligence (Generative AI), thereby enhancing regulatory adaptability and ensuring alignment with ongoing technological development. At different stages of the Generative AI lifecycle, differentiated regulatory measures should be applied, with the objective of establishing a full-process regulatory framework encompassing research and development, data processing, and content generation. Through appropriate institutional design of tiered regulation, regulatory effectiveness can be improved. Risk-based tiered regulation follows the operational mechanisms of Generative AI and is not confined to ex post control of manifested harms; rather, it emphasizes ex ante risk prevention through regulatory intervention. In this manner, it helps maintain the overall stability of the regulatory system and its capacity to adapt to technological evolution. Regulatory rules should not be excessively stringent. On the premise of ensuring safety and controllability, a flexible regulatory approach grounded in risk classification and risk grading should be adopted, so as to create a favorable institutional environment for the sustainable development of Generative Artificial Intelligence.

4.2. Strengthening Multi-Stakeholder Collaborative Regulation

From research and development to deployment and application, Generative Artificial Intelligence involves multiple actors and diverse application scenarios. Legal risks arising from Generative AI generate linkage effects across upstream and downstream segments of its operational mechanisms. The complexity and diversity of such risks make it difficult for any single actor to comprehensively identify and regulate them. Accordingly, it is necessary to expand the scope of regulation, give due consideration to the differentiated regulatory needs of various actors, and fully leverage the specialized regulatory functions of different stakeholders. The risks associated with Generative AI are highly technical in nature, rendering it difficult for non-specialists to accurately understand its operational mechanisms and the underlying causes of risk. Multi-stakeholder collaborative regulation should therefore broadly incorporate relevant social actors—such as AI developers, industry associations, and research institutions—into the governance framework for Generative AI. By aggregating professional expertise and regulatory consensus among diverse stakeholders involved in the research, development, and application of Generative AI, such collaboration enables the realization of flexible and dynamic regulation grounded in specialized knowledge. Moreover, newly emerging technological forms, application models, and potential risks often exceed the scope of foresight and coverage of existing legal frameworks. In this context, multi-stakeholder participation can compensate for the inherent limitations of formal legal regulation by enhancing regulatory responsiveness and adaptability, thereby contributing to more effective governance of Generative Artificial Intelligence. [7] The risks associated with Generative Artificial Intelligence are characterized by uncertainty and dynamism. Regulation conducted by a single actor is often unable to promptly identify risk sources or respond effectively to emerging risks. By contrast, multi-stakeholder regulation enables different actors to complement one another in both risk perception and the selection of regulatory approaches. Such collaboration allows for the dynamic adjustment of regulatory strategies, facilitates the rapid identification and correction of risks, and enhances the capacity to respond to the accelerated development of artificial intelligence technologies. The principal advantage of multi-stakeholder collaborative regulation lies in the interconnection and mutual supplementation of regulatory mechanisms, which helps to remedy the inherent limitations of single-actor regulation. By integrating the specialized expertise of different actors into the governance of Generative Artificial Intelligence, a multi-layered regulatory toolkit can be formed, enabling regulators to better address the uncertainty and variability of Generative AI risks. At the same time, the involvement of multiple

ISSN: 2710-0170

actors in regulation may lead to regulatory overlap and inefficient use of regulatory resources. To mitigate such concerns, it is necessary to clearly define the statutory rights, responsibilities, and regulatory scope of participating actors. Procedural mechanisms for multi-stakeholder participation should be established to perform cross-sectoral coordination and integration functions, prevent the emergence and escalation of risks, and ensure the efficient allocation of regulatory resources, thereby enhancing overall regulatory capacity. In addition, multi-stakeholder participation in regulation contributes to the construction of trust in Generative Artificial Intelligence technologies. Through engagement in regulatory processes, different actors can develop a deeper understanding of the technical characteristics of Generative AI and articulate their respective interests and concerns. Regulatory rules formulated through such inclusive processes are therefore more likely to adapt to the ongoing evolution of artificial intelligence technologies.

4.3. Improving Data Security Regulatory Rules

Data-related risks permeate the entire lifecycle of Generative Artificial Intelligence, from research and development to deployment and application. Fragmented or partial regulation is therefore insufficient to address the practical demands of data risk governance. It is necessary to establish full-process data security regulation covering data collection, processing, storage, and output. From the perspective of legal attributes, data involved in Generative Artificial Intelligence implicate the rights and interests of multiple stakeholders. Accordingly, the fundamental principle of data security regulation should be to balance data-related rights and interests with the broader public interest. Generative Artificial Intelligence is inherently data-driven, and data can only realize their maximum value through circulation and utilization. However, data collected and used by Generative Artificial Intelligence systems must be subject to prior screening and regulatory oversight. Regulatory emphasis should be placed on the controllability and legitimacy of data, with careful adherence to the principles of lawfulness, legitimacy, and security. These principles serve to constrain both data collection and subsequent data use, thereby reducing the risk of generating false or misleading information. The optimization of data governance rules for Generative Artificial Intelligence should aim to ensure the legality and authenticity of original data sources, maintain data collection and use within a controllable scope, and conduct systematic assessments of data quality. In particular, regulators should prevent the collection of non-public data or data that pose potential infringement risks, in order to ensure the accuracy and reliability of training data used for large-scale models. Safeguarding data security further requires clear identification of data sources, explicit definition of the purposes and scope of data use, and the adoption of appropriate technical and organizational measures to ensure data security. Relevant actors should bear corresponding data security management obligations and take effective measures to prevent unauthorized access and illegal intrusion. In addition, regulatory efforts should strengthen oversight of data provenance and the authenticity of generated content, while attaching greater importance to the technical dimensions of regulation. By leveraging artificial intelligence technologies themselves to mitigate the risks posed by Generative Artificial Intelligence, a flexible data governance framework can be constructed in which institutional regulation and technical regulation operate in a complementary and coordinated manner. Through such an approach, regulation can function not only as a mechanism for risk prevention, but also as a means of promoting the sustainable and orderly development of artificial intelligence technologies.

Regulatory oversight of data security is essential at the data collection stage. However, overly stringent regulatory rules may impede the development of artificial intelligence technologies. Accordingly, a tiered regulatory approach should be adopted, distinguishing between general data and high-risk data. Specifically, data with relatively low risk coefficients—such as publicly

ISSN: 2710-0170

available data—may be classified as general data and subject to more relaxed regulatory requirements. By contrast, data with higher risk coefficients, including personal privacy information and corporate operational data, should be subject to stricter standards emphasizing the legality and security of data collection and processing. The data collection stage constitutes a critical phase in the data processing lifecycle of Generative Artificial Intelligence. The legality of data sources and the traceability of data should serve as core criteria for assessing the lawfulness of data collection. While fully exploring the value of data, regulatory frameworks should simultaneously prevent application-related risks and safeguard subsequent data analysis activities. Regulatory rules should therefore be grounded in the principles of legality and legitimacy in data collection and analysis, with the overarching objective of ensuring the secure circulation of data. To this end, a comprehensive data circulation traceability and regulatory mechanism covering the entire data lifecycle should be established. Such a mechanism can prevent the illegal collection and misuse of data, clarify the rights, obligations, and boundaries of relevant actors, and prevent abuses of power in data collection and analysis processes. Responsible entities should ensure the quality of data collection and establish data security assessment rules to verify the security and authenticity of collected data, thereby ensuring data source traceability and controllability of data use. Given that data-related risks cannot always be accurately identified at the data collection stage, it is necessary to establish a data provenance monitoring mechanism to enable continuous oversight of data risks throughout subsequent stages of application. At the data analysis stage, unified processing standards should be formulated, with explicit limitations on the purposes and scope of data analysis. Developers should also be required to conduct comprehensive risk assessments of data analysis methods. In addition, regulatory frameworks should refine rules concerning data storage in Generative Artificial Intelligence, clearly specifying storage methods, responsible entities, and the allocation of rights and interests, and establishing secure standards for data storage, use, and deletion. Through these measures, a secure and trustworthy data storage environment can be provided to support the safe operation and sustainable development of Generative Artificial Intelligence.

4.4. Establishing an Algorithmic Regulatory Framework

Algorithmic regulation does not involve a single or unilateral value choice. Rather, it requires a careful balancing between multiple legally protected interests affected by algorithmic systems and the interests in the free use and deployment of algorithms. [8] Accordingly, it is necessary to effectively balance the dual demands of safety and development in relation to Generative Artificial Intelligence. The objective of algorithmic regulation is to establish due process for algorithmic operation through mandatory regulatory rules, to implement requirements of algorithmic explainability, to enhance algorithmic transparency, and to reduce uncontrollable factors in algorithmic operation. Given the technical and commercial attributes of algorithms, regulatory frameworks should not require developers to fully disclose algorithmic source code or internal mechanisms, as such requirements may undermine intellectual property protection, technological innovation, and the commercial value of algorithms. Instead, regulators should adopt algorithmic explainability as the core regulatory standard and require a limited and proportionate degree of disclosure. Such disclosure should enable regulators to understand algorithmic decision-making processes and operational logic to the extent necessary to identify potential risks arising during algorithmic operation. In addition, an algorithmic accountability and traceability mechanism should be established to clarify the allocation of rights and responsibilities among relevant actors. In light of the risks associated with Generative Artificial Intelligence, an algorithmic regulatory framework should be constructed by combining full-lifecycle algorithmic governance with enhanced algorithmic transparency. Although algorithms function as auxiliary technical tools and do not inherently possess value orientations, they are inevitably influenced by the subjective intentions of designers during the stages of research,

ISSN: 2710-0170

development, and application. In response, the self-regulatory capacity of artificial intelligence enterprises should be strengthened, with the objective of leveraging industry-specific expertise to prevent and mitigate risks through internal governance mechanisms. Algorithm designers should bear proactive duties, including obligations of risk prevention and the timely correction of erroneous algorithmic decisions. Regulatory approaches should emphasize guidance rather than excessive intervention. Clear standards of legality and duties of care for algorithmic development should be articulated. Algorithmic technologies should adhere to the principle of neutrality, and designers should incorporate principles of fairness into algorithmic design, establishing normative constraints on algorithmic operation. This approach enhances fairness in decision-making and allows elements that may undermine algorithmic fairness to be identified, corrected, or removed at an early stage, thereby advancing the temporal point of regulatory intervention. Within the field of Generative Artificial Intelligence research and development, a baseline standard for algorithmic disclosure should be established. Through binding standards governing algorithmic operation, algorithmic regulatory rules can be refined to prevent both technical algorithmic risks and derivative algorithmic risks. At the same time, prohibited practices should be clearly identified, serving as a supplementary and elaborative function to mandatory regulatory rules. Furthermore, the scope of information disclosure obligations imposed on algorithm designers in the event of risk occurrence should be clearly defined, including duties to explain algorithmic mechanisms and to provide technical assistance with respect to specialized content. This provides an institutional basis for regulatory intervention. Finally, algorithmic accountability mechanisms should be strengthened by clarifying the allocation of responsibility and corresponding liability standards among different actors based on their degree of control over Generative Artificial Intelligence systems. The review obligations of responsible entities should be further specified to prevent improper or abusive use of algorithms. Through the optimization of regulatory rules, different stakeholders can be guided to fulfill their respective obligations in algorithmic safety management.

5. Conclusion

This article analyzes the operational mechanisms and legal risks of Generative Artificial Intelligence and summarizes the key risks arising from its technical characteristics, including data contamination, data leakage, algorithmic technical risks, and derivative algorithmic risks. It clarifies that the core problem of existing regulatory frameworks lies in the need for regulatory rules to evolve continuously alongside the development of artificial intelligence technologies. Given the unpredictability and rapid iteration of Generative AI, regulation must maintain dynamic adaptability and accurately identify the sources of risk. The article further argues that risk-based regulation is a regulatory approach that aligns with the developmental trajectory of Generative Artificial Intelligence. Specifically, such an approach traces potential risks and actual harms by examining application scenarios and technical characteristics of Generative AI, conducts risk assessment and tiered classification, and treats risk as a regulatory tool. On this basis, differentiated regulatory models are constructed according to varying levels of risk, thereby enhancing regulatory effectiveness while preserving regulatory flexibility. Through risk-based classification, rights and obligations can be appropriately allocated among relevant actors, and a multi-stakeholder, full-lifecycle regulatory system can be established to address Generative Artificial Intelligence risks at different stages. In addition, regulation should take into account the broader public interest implications arising from the development of artificial intelligence technologies. With the dual objectives of safeguarding security and promoting innovation, regulatory frameworks should reserve sufficient space for the sustainable and innovative development of artificial intelligence technologies.

ISSN: 2710-0170

References

[1] Y. Tang and C. Tang: Risk-Based Artificial Intelligence Regulatory Governance, Social Science Journal, Vol. 2022 (2022) No.1, p.114–124, 209.

[2] Z. Zhi: Major Concerns and Future Trends of Global Artificial Intelligence Legislation, Journal of Comparative Law, Vol. 2025 (2025) No.6, p.17–36.

[3] H. Jiang: Risk-Based Artificial Intelligence Regulation—An Analysis from the Perspective of the EU Artificial Intelligence Act, Law Forum, Vol. 40 (2025) No.5, p.83–95.

[4] X. Zhang: Data Risks of Generative Artificial Intelligence and Paths of Governance, Legal Science (Journal of Northwest University of Political Science and Law), Vol. 41 (2023) No.5, p.42–54.

[5] X. Hu: An Outline of Legal Regulation of Algorithmic Risks in the Era of Artificial Intelligence, Journal of Hubei University (Philosophy and Social Sciences), Vol. 48 (2021) No.2, p.120–131.

[6] X. Ding: China's Artificial Intelligence Legislation in a Global Comparative Perspective, Journal of Comparative Law, Vol. 2024 (2024) No.4, p.51–66.

[7] T. Zhang: Regulating Artificial Intelligence through Technical Standards: A Jurisprudential Analysis Based on Cooperative Regulation, Journal of Comparative Law, Vol. 2025 (2025) No.4, p.169–187.

[8] Y. Su: The Genealogy of Algorithmic Regulation, China Legal Science, Vol. 2020 (2020) No.3, p.165–184.