PIONEER
ACADEMIC PUBLISHING LIMITED

Studies in Law and Justice
ISSN 2958-0382
www.pioneerpublisher.com/slj
Volume 2 Number 3 September 2023

The Path of Formulating the Basic Law of Artificial Intelligence in China — Analysis of the Desirability of the EU Artificial Intelligence Act

Xiaotong Bing[1]

[1] Independent Researcher, China
Correspondence: Xiaotong Bing, Independent Researcher, China.

doi:10.56397/SLJ.2023.09.09

Abstract

The European Commission released the proposed Regulation on Artificial Intelligence (the EU AI Act) on 21 April 2021, which reflects the EU's leadership orientation in establishing norms and standards in emerging fields, and also reflects the urgent need for legal unity of the EU as a unified market entity. The Act sets out harmonized rules for the development, placing on the market, and use of AI in the European Union. The ideas of a risk-based approach and experimental governance are of great significance for reference. However, with the advent of ChatGPT, the Artificial Intelligence Act has raised questions about the legal applicability of "human-computer interactive" generative AI. China's AI governance adopts scene-by-scene and field-by-field legislation, with both "hard law" such as laws and regulations, and "soft law" such as industry norms, generally presenting a vertical governance path and lacking a unified basic law guideline. With the gradual shortening of the scientific and technological innovation cycle in the field of artificial intelligence, the establishment of a unified basic law on artificial intelligence should be put on the agenda. Setting up a dual-risk categorization regulatory framework, and categorizing from both macro and micro perspectives may be a good attempt. It adopts a full chain regulatory mechanism with a full process and multiple subjects, and clarifies the rights and obligations of all legal subjects in the whole cycle, to jointly assist the development of AI "for the better".

Keywords: ChatGPT, artificial intelligence basic law, risk-based classification, experimental treatment, dual-risk categorization supervision

1. Introduction

The emergence of ChatGPT can be described as a breakthrough in the field of artificial intelligence, especially GPT-4 has been greatly improved in all aspects, showing a trend of specialization. Some scholars claim that it will shorten the implementation time of the meta-universe by at least ten years. Compared with the traditional artificial intelligence technology limited to a certain field, its audience is wider and can be spread to all walks of life, showing good human-machine interaction. And through the continuous accumulation and optimization of massive data, it presents good professionalism and is highly sought after by people from all over the world, achieving the

miracle of consumer growth rate. However, the risks behind the rapid development of new technologies cannot be underestimated. Take Western countries as an example, the discriminatory information and false information contained in ChatGPT disturb the social atmosphere and there are also problems such as infringement of personal privacy and business secrets. As a result, China does not allow the application of ChatGPT in the country at present. In addition to the above set of issues, there are also issues affecting digital sovereignty and security, such as the penetration of ideology.

It is undeniable that the emergence of generative artificial intelligence has brought scientific and technological progress, but also brought huge security risks. At this time, the law needs to play a good guiding and regulating role. To this end, the EU took the lead in issuing the AIA to establish EU-wide norms and standards, and to be at the forefront of artificial intelligence legislation, which also protects the rights of EU citizens through the principle of "long-arm jurisdiction". In the meantime, China has also made new progress in artificial intelligence legislation and issued the Interim Measures for the Management of Generative Artificial Intelligence Services based on fully soliciting opinions, which put forward clear service specifications for providers and required relevant departments to strictly follow the classification-based principle to supervise or guide. This is consistent with China's legislative approach to the field of artificial intelligence, which is based on scenarios. For example, the Data Security Law, Personal Information Protection Law, Internet Information service algorithm recommendation management provisions, etc. The absence of a legal framework for AI also lacks systematicity, in addition to which the multi-sectoral regulatory landscape may create regulatory overlap and waste regulatory costs. At the same time, rapid legislative responses to new technologies reflect the efficiency of legislation, which can solve problems to a certain extent, but cannot play a fundamental role in guiding the law, reflecting the lag of the law. In addition, there are inevitably problems of overlap and illogicality in several provisions, which increase the cost of implementation.

To sum up, in the future, artificial intelligence products like ChatGPT will emerge in large numbers, and China's artificial intelligence companies will also launch artificial intelligence products in line with socialism with Chinese characteristics. Until then, if a basic law on artificial intelligence can be enacted, legal risks can be significantly reduced and legal protection will be better provided.

2. Analysis of the Desirability of the Artificial Intelligence Act

2.1 Risk-Based Approach

The principle of risk-based classification is the core concept of the AIA, which divides artificial intelligence systems into unacceptable risk, high risk, limited risk, and minimal risk, and decreases from prohibition to non-supervision according to the degree of risk. At the same time, common application scenarios are listed into different risk levels, which are of reference significance. For example, applications that threaten people's safety, livelihoods, and rights as unacceptable risks are strictly prohibited and subject to severe fines for violators. This kind of risk regulation covers the whole process when the product is put on the market, and the risk type should be assessed quickly, and the corresponding measures should be adjusted in time when the degree and type of risk change, which shows strong flexibility and pertinence.

In general, the risk-based approach can satisfy today's AI field and its products and can also meet the general criteria of the AI fundamental law, which is informative. However, after the birth of ChatGPT, the principle of risk-based classification can not be comprehensively and accurately assessed. Unlike previous AI technologies, ChatGPT creates both internal and external risks. It is not a technological "black box" in the traditional sense, i.e., the technical principles are known only to some people, but not to regulators and the public. Generative AI has reasoning capabilities that even the R&D team cannot decipher, so internal risks are even more unpredictable. In addition, ChatGPT embodies strong human-machine interaction, even if the provider takes preventive measures to control the users' input behaviors, which can not stop them from making malicious input. ChatGPT collects and learns every interactive content, if the malicious content exists for a long time, the adverse consequences will increase significantly. Therefore, after the advent of ChatGPT, the criteria for risk classification are difficult to meet the need for universality, and further changes maybe needed.

2.2 Supervision Sandbox Mechanism

The EC aims to prevent the rules from stifling innovation and hindering the creation of a flourishing AI ecosystem in Europe, by introducing legal sandboxes that afford breathing room to AI developers. The essence of the "regulatory sandbox" is an exemption mechanism, which gives a certain fault-tolerant space to promote better development. When enterprises test innovative products, they do not need to worry about the conflict between innovation and regulatory principles. The specific operation is to establish a temporary framework for action in advance in an uncertain environment and constantly revise it through implementation. The Artificial Intelligence Act explicitly proposes to support the establishment of "regulatory sandbox" measures for SMEs and start-ups, reducing the compliance burden.

When artificial intelligence products are widely put into use, if they can be fully tested in a specific region, it is conducive to identifying risks and proposing targeted countermeasures. It is safer to have mechanisms in place to deal with risks that are difficult to predict.

In summary, the principle of the risk-based approach classifies new developments in artificial intelligence into existing classification standards and determines regulatory methods by estimating risks, but it is difficult to achieve in the innovative application of deep synthesis algorithms, and there are certain limitations. As a supervision method, the regulatory sandbox mechanism can not only help the regulated to continuously reduce risks but also provide more effective supervision methods for regulators, which is of great significance.

3. The Institutional Conception of China's Artificial Intelligence Basic Law

A good institutional design of the basic law of artificial intelligence should not only consider the algorithm governance of a single scene, which is already relatively mature but also consider the complex governance of generative artificial intelligence at present and the more intelligent products and technologies that may appear in the future. As the basic law should seek the commonness of different types of technology, the design of norms for the commonness can further reduce the lag of laws. The idea of the Basic Law mainly includes four parts: basic principles, classification standards, supervision mechanism, and responsibility.

3.1 Basic Principles

First, adhere to the overall approach to national security. In the new era, all aspects of the country's work should pay attention to both development issues and security issues, and maintaining data security is the meaning of the concept. The extraterritorial application of artificial intelligence such as ChatGPT is built on the basis of Western values and thinking orientation, which may lead to ideological penetration in China, especially affecting the value formation of minors. It may also affect China's digital sovereignty and security. Therefore, when formulating the basic law of artificial intelligence, we must adhere to the overall national security concept and try to build an active defense system with passive data exit, and especially build and strengthen the network attack monitoring platform to focus on protecting national data.

Second, attach equal importance to development and security. Legislation is to guide the goodness of artificial intelligence, and the fundamental purpose is to achieve high-quality development in the field of artificial intelligence. It is based on this principle that Article 3 of the newly issued Interim Measures for the Management of Generative Artificial Intelligence Services stipulates that inclusive, prudent, and classified regulatory methods should be implemented. In particular, technology developers should be appropriately reduced the legally binding force and give sufficient space for technological innovation development under the rule of law.

Third, adhere to ethical principles and shall not violate the mandatory provisions of state and administrative regulations and public order and good customs. AI applications must conform to human ethics before they can be launched, especially in line with Chinese values and international consensus. At present, there are existing platforms to describe human moral cognition and behavior in different scenarios, and then form ethical and moral evaluations covering human and artificial intelligence ethical and moral performance. The novelty lies in the fact that in the course of attempting to surpass the advances of the other states, each state pushes forward towards less human control, reaching potentially, the level of-almost-zero human interference in lethal weapons' functions. The endgame may be the complete collapse of human centrism and the humanization of the

international order. Therefore, the basic law should require that ethical compliance obligations must be done before the release of artificial intelligence products, and do a good job of prohibitions.

3.2 Classification Standards

At present, China's legislation in the field of artificial intelligence mainly carries out vertical governance according to different scenarios. But there are also common horizontal regulations, such as algorithm security assessment, algorithm filing system, and so on. The AIA provides targeted supervision according to the degree of risk, but with the emergence of generative artificial intelligence and the unclear definition of risk, there are difficulties in the specific application of the Act. If you want to develop a general method of artificial intelligence, this paper believes that the risk standard is a very worthy idea in the horizontal governance path, but it should not be divided into the degree of risk by enumerating. This paper believes that whether there are internal risks can be used as a criterion to judge traditional or newly developing artificial intelligence.

Traditional artificial intelligence products or services are unidirectional in the way they are provided and cannot achieve human-computer interaction, and the design risks in this process are mainly external risks such as personal information leakage. At present, China has formed a governance pattern of both "soft law" and "hard law" for external risks, which can effectively deal with external risks. However, with the emergence of generative artificial intelligence, the risk has gradually changed from external risk to both internal and external risk, and the internal has changed from a simple technical "black box" to "human common ignorance in the face of strong artificial intelligence." Not only internal risks are becoming more difficult to control but also external risks are more uncontrollable due to the differentiation of human-machine interaction. In the future, with the emergence of more and more strong artificial intelligence technologies, artificial intelligence will have higher reasoning ability, and the internal and external risks generated will gradually increase. Therefore, the simple level of risk can not cover all artificial intelligence technology. This paper believes that we can divide traditional and emerging artificial intelligence technology according to the degree of internal and external risk and carry out relevant system design to cover artificial intelligence technology more comprehensively, which plays a preventive and normative role in future artificial intelligence technology.

3.3 Supervision Mechanism

The legal governance of artificial intelligence especially new technologies should be development-oriented, but how to achieve high-quality development is more important. Most of the domestic academic supervision of artificial intelligence technology is in three ways: sub-subject supervision, whole-chain supervision, and sub-model supervision. Regarding sub-subject supervision, China has put forward the responsibility of compacting the subject in terms of data security and information content security, especially strengthening the responsibility of network service providers such as platforms. At the level of main responsibility, it shows the general direction of emphasizing service providers over technology developers and users, which effectively promotes the standardized development of the platform, but a single main responsibility cannot meet the increasing development of artificial intelligence, especially when technical personnel assumes an increasingly important role. As a scientific supervision method, full-chain supervision can cover the whole process of artificial intelligence research, development, production, and application, which is conducive to the safe development of artificial intelligence, and should be used as a basic way of supervision. The sub-model regulation is specifically proposed for generative artificial intelligence, and its underlying logic is that generative artificial intelligence is a three-in-one technology form of technical support, service provision, and content, that is, technology developers may also play the role of service providers, so it is impossible to find an appropriate legal status by simply dividing responsibilities through the subject. It is more reasonable to divide it by the basic model, professional model, and service application. Concerning the above regulatory approaches, this paper believes that a multi-body, full-chain, and dual-risk categorization regulatory mechanism can be formed.

The establishment of a regulatory framework for dual risk categorization is done through a macro and micro perspective. Firstly, from a macro perspective, it is categorized into traditional AI

and emerging AI according to whether it has internal risk and different regulatory principles are set for it. For traditional AI, the principle of safety is adopted to ensure that external risks are continuously reduced. For emerging AI, it adopts the principle of giving equal importance to development and safety, encouraging innovation, and focusing regulation on after-the-fact risk contingency. Secondly, the other criterion is to focus on the internal of traditional or emerging AI and classify different regulatory standards according to the degree of risk. Here, we can learn from the EU's categorization criteria, which strictly prohibits hazard requirements as unacceptable risks. For high-risk AI systems, the traditional AI sector will be strictly regulated throughout the entire process, including rigorous assessment beforehand as well as full-cycle monitoring. In the specific implementation process, all parties should adhere to a macro and micro-consistent regulatory approach.

Specifically, first of all, for traditional artificial intelligence in the pre-risk management stage, the regulatory authorities should strictly perform their regulatory duties and take risk control measures, such as risk assessment and filing systems to enhance the transparency and interpretability of the algorithm, which can control risks from the source. The enterprises are required to conduct regular audits and carry out security vulnerability investigation work regularly. Technology developers are required to abide by ethical rules and accept relevant ethical reviews consciously. They must not violate not only the public order and good customs but also mandatory provisions of laws and administrative regulations. At this stage, security should be the first value proposition. For emerging artificial intelligence technology, it should not be too strict, and supervision should focus on the risk emergency stage. Since China is in the early stage of generative artificial intelligence technology research and development, the top-level system design should leave enough space and time for it. A regulatory sandbox mechanism can be used to designate specific test areas and specify test times. Secondly, in the risk emergency stage, traditional artificial intelligence should respond quickly to risks: service providers should quickly establish rumor-refuting and reporting mechanisms, take restrictive measures to stop transmission of harmful products, recall defective products in time, or take compulsory destruction. At this time, strengthening the responsibility of service providers is of significance. For emerging artificial intelligence technologies, there is a lack of experience in risk so classification should be adopted. When the risk comes from the client, the service provider should actively perform the obligation of emergency remedy. When the risk comes from a non-client, it should be traced back to the upper level to further identify the source of the problem. Finally, in the post-prevention stage, technical developers should summarize their experience in time and modify technical loopholes in time making it clear that developers should fulfill their product follow-up observation obligations. With the gradual popularization of artificial intelligence, users as the audience must improve artificial intelligence literacy and strictly abide by regulations. They shall not violate public order and good customs and they are supposed to enhance security awareness and pay attention to the protection of their own personal sensitive data and business secrets.

3.4 Responsibility

In addition to clarifying the legal obligations of all parties, the formulation of the basic law of artificial intelligence needs to design relief channels to give victims adequate means of legal relief. The damage caused by artificial intelligence products mainly includes three situations: First, the damage caused by product defects. The second is the damage caused by the use of products. Third, the damage is caused by its accurate operation following the preset procedure, and there is no fault of others or intermediate links.

Given the first situation, if there are defects in the design and manufacturing of the product, the relevant personnel can be required to bear the responsibility according to the product liability, the designer, the producer, and the seller bear the responsibility first. After that the party who bears the responsibility first has the right to recover from the person who is at fault. In the second case, if the accident of the artificial intelligence is caused by the person who has the responsibility for the management and control of the artificial intelligence product, it needs to be held liable to the extent that it fails to fulfill the obligation of good management. When the third situation occurs, since the party responsible for supervision is not at fault and

there are no defects in the intermediate link, risk management methods can be considered at this time. Look at which parties in this situation can minimize risk and deal with negative impacts. If such party fails to fulfill the corresponding risk management obligations, it shall be liable for damages.

4. Conclusion

At present, the rules and systems for artificial intelligence risks are too scattered, and the legal level is low, which is not conducive to enterprises to fulfill their obligations and it may cause difficulty in the supervision of regulatory authorities. Therefore, the development of an artificial intelligence basic law should be put on the agenda. Under the background of the fourth industrial revolution, all countries are reserving sufficient legal space for the development of new technologies as much as possible. To promote the creation of technology continuously, they choose to "let the bullets fly a little longer". But through the legislation to solve this stormy interdisciplinary problems need to be courageous and creative, after all, excessive freedom of development is not real progress. The rule of the legal track to achieve high-quality development of artificial intelligence is the goal we should pursue.

References

Liu Xinyu. (2023). From the meta-universe to Law 3.0: A genealogy of artificial intelligence law. *Journal of Shanghai University*, (4), 18-28.

Liu Yanhong. (2023). Three security risks and legal regulations of generative Artificial Intelligence: A case study of ChatGPT. *Oriental Law*, 30-43.

Mauritz Kop. (2021). EU Artificial Intelligence Act: The European Approach to AI. *Stanford-Vienna Transatlantic Technology Law Forum*, (2), 1-11.

Wang Jianwen. (2023). *Cyber and Artificial Intelligence Law*. Beijing: Law Press.

Zeng Xiong, Liang Zheng & Zhang Hui. (2022). The new development of algorithm governance practice in Europe and America and the construction of comprehensive algorithm governance framework in China. *E-Government*, (7), 67-75.

Zeng Xiong, Liang Zheng & Zhang Hui. (2022). The regulation path of artificial intelligence in EU and its enlightenment to China. *E-Government*, (9), 63-72.

Zhang Linghan & Yu Lin. (2023). From Traditional governance to Agile governance: Changing governance paradigms for Generative Artificial Intelligence. *E-Government*, 136-145.

Zhang Linghan. (2023). The Legal Position and Hierarchical Governance of Generative AI. *Modern Law Science*, (4), 126-141.

Zhang Lu. (2023). A preliminary study on general artificial intelligence risk governance and supervision. *E-Government*, 107-117.

Zhang Xuebo & Wang Hanrui. (2023). Legal regulation of generative artificial intelligence. *Shanghai Legal Studie,* (6), 246-254.