International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 6, Nov-Dec 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# Research on the Construction of the Prevention System of Artificial Intelligence Legal Risks

**Chen Mengyao, Jia Yichu, Zhang Juyuan**

Beijing Wuzi University, Beijing, China

## ABSTRACT

The rise of generative AI is profoundly changing people's lifestyles and work patterns. This technological innovation comes with a complex and urgent set of legal risks and challenges. Therefore, it is necessary to deeply analyze the current development trend and research status of artificial intelligence. Relevant laws and regulations at home and abroad show that the technology is not yet mature, and there are still problems such as risk intrusion. Based on this, a comprehensive and effective AI legal risk prevention system should be built to make it a tool to ensure the healthy development of technology and maintain social order and stability. Then, the theoretical basis and practical path of AI legal risk prevention are discussed in depth.

***KEYWORDS:*** *artificial intelligence; risk prevention; legal security*

***How to cite this paper:*** Chen Mengyao | Jia Yichu | Zhang Juyuan "Research on the Construction of the Prevention System of Artificial Intelligence Legal Risks" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-6, December 2024, pp.694-701, URL: www.ijtsrd.com/papers/ijtsrd71591.pdf

IJTSRD71591



## INTRODUCTION

### A. Project content

The project is dedicated to researching and dealing with the risk of AI, focusing on the controversial aspects and legal risks of AI serving the public. This project will provide legal analysis and protection of rights and interests in the interpretation of several issues arising from artificial intelligence, the doubts and infringement judgments of the public using artificial intelligence, etc., and write academic reports on them.

Mr. Gong Fuwen said: "As a new technology, artificial intelligence (AI) has huge moral concerns, ethical deficiencies, and security risks once it is born. [1] With the improvement of artificial intelligence and big data, life is convenient and efficient, and some unavoidable legal problems have arisen. Determination of infringement of sharing, excerpting, and secondary creation in the use of AI-generated data; In the process of artificial intelligence data transmission and storage, user and enterprise privacy protection and security issues; The attribution of liability and the risk of later compensation caused by copyright confusion are closely related to public life, and these legal interpretations still need to be improved. This project provides some suggestions and insights through academic research, aiming to make artificial intelligence better serve people's life and learning work while effectively avoiding legal risks.

### B. Purpose of the Study

At the national level, it is currently considered that the development trend of artificial intelligence is becoming more and more difficult to control. This project closely follows the national hot issues, and in order to cope with the challenges, academic research should be carried out to avoid risks as much as possible and ensure national security; At the societal level, it has become the norm for companies and corporations to monetize through artificial intelligence. Therefore, accelerating the construction of a safe employment environment and promoting social development is also one of the objectives of this project. At the individual level, a series of problems arising from artificial intelligence are also a part of the public's life. Based on this, in order to

reduce a series of problems of artificial intelligence and promote social stability and high-quality development, we have carried out the investigation and research of this project.

### C. Significance of the study

In a theoretical sense, firstly, this project will help to enrich and improve the theoretical system of artificial intelligence legal risks. With the development of artificial intelligence, traditional legal theories are also facing new challenges. Secondly, this project contributes to the development of interdisciplinary research. It provides new perspectives and methodologies for interdisciplinary research such as law, computer science, and sociology, and contributes to a more comprehensive understanding of AI technology and its impact on society. Finally, the project is expected to be a precursor to legal regulation. Theoretical research provides a precursor to legal regulation and a basis for decision-making for legislators, which is conducive to guiding the formulation of reasonable laws and regulations and ensuring the sustainable and healthy development of society.

In a practical sense, first of all, this project contributes to the improvement of legal planning and risk management. This project can better ensure that the development of artificial intelligence technology will not harm social value. Secondly, the project is conducive to promoting public education and awareness. The study of the legal risks of AI will not only help policymakers and legal professionals understand the challenges posed by AI and analyze them deeply, but also enhance the public's understanding of these issues and legal interpretations, and enhance the legal awareness and self-protection ability of society as a whole. Finally, the project is conducive to providing security. With the wide application of artificial intelligence technology in various fields, security cannot be ignored. For example, intelligent systems such as robots can be exploited by criminals, causing security issues such as information leakage. Studying the legal risks of AI can help prevent and reduce such security threats, protect the data security of individuals and enterprises, and promote industrial innovation and sustainable development.

## Market Research and Analysis

### A. The current status of domestic research and the general development trend of the research project

At present, there is still a long way to go to achieve real prevention and ensure that technological security and national and social interests are not violated. At present, artificial intelligence is widely used in China, and there are traces of the existence of generative AI in different fields. With its rapid development, China also attaches great importance to the ethical and legal mechanisms of AI. In terms of the current situation of China's legislation in the field of artificial intelligence, in 2022, Shenzhen issued China's first local regulation on artificial intelligence, "Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations"; In June 2023, the State Council released the 2023 legislative work plan, and the draft AI Law was included, and in July of the same year, the Cyberspace Administration of China, together with the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration of Radio, Film and Television, issued the Interim Measures for the Management of Generative AI Services. [2] These documents clearly put forward the requirements for improving the capacity of ethical governance of science and technology and accelerating the construction of the legal system for ethical governance. Let the field of AI make breakthroughs in theoretical research such as fairness, explainability, and privacy. However, there are still deficiencies in detection, protection, monitoring and early warning technology. When Lu Peng of the Chinese Academy of Social Sciences released the "Report on the Value of Security Technology in the Digital Age", he pointed out that AI security risks call for turning them into public goods [3], but the plan is not yet mature, the risk is large, and the human error in the middle is immeasurable. At the same time, many experts pointed out that they hope to promote the development of new quality productive forces, stimulate innovation, and encourage innovation. The development trend of domestic artificial intelligence prevention is also gradually moving towards a complete state. But what is unavoidable is that there are many AI intelligence that will grasp the needs of the public and "tempt deliciously" them. At present, the artificial intelligence technology represented by ChatGPT has attracted widespread attention, and the journal of Zhengzhou University of Light Industry pointed out that the popularization of artificial intelligence will weaken the dominant position of human beings in society and replace part of human work. For example, writing speeches and even graduation theses has turned many research results that should be of high value into a fixed string of code, which has no new ideas, and even destroys people's most essential imagination and creativity. An online store with "AI writing papers" as its main business has received 555 orders in the past three

months, including undergraduate thesis writing and plagiarism checking services. Once this kind of unearned thinking becomes a habit, it will curb technological progress and even harm the interests of the country and society.

**B. Lack of foreign experience and systems**

In terms of foreign experience, the United States enlisted its allies to announce the field of lethal autonomous weapon systems at the July 2022 meeting of governmental experts on the Convention on Certain Conventional Weapons, and the alliance of developed countries emphasized good practice of fully autonomous lethal autonomous weapons, and the current lethal autonomous weapons have not yet appeared, and they are under meaningful human control, even if they are lethal autonomous weapons, there are still some technical risks. These risks will also be mitigated by advances in technology. [4] This shows that the emphasis on "human will control" in foreign countries can be mitigated even if the risk of lethal autonomous weapons is under meaningful human control. Conversely, fully autonomous lethal weapons should not exist. This completely subverts human control over it, but some developed countries will have expectations and even dependence on complete autonomy. In terms of institutional deficiencies, in November last year, 28 countries and regions, including the United States, the United Kingdom, China, and the European Union, signed the "Bletchley Declaration" at the Security Summit hosted by the United Kingdom, calling for and advocating people-oriented, hoping that AI research institutions and related enterprises will design, develop and use AI in a responsible manner. [5] After the summit, local governments and economic institutions in various countries have introduced measures, but the degree of supervision has varied, and some serious risks have not been avoided in time. Microsoft recently shared a new large-scale intrusion technology called Skeleton Key, which can bypass the built-in protections in mainstream large language model (LLM) applications to generate harmful or illegal content. The technology has successfully hacked OpenAI's GPT-4.0 and GPT 3.5 Turbo, Google's Gemini Pro base model, Meta's Llama3-70B instruction fine-tuning and base model, Anthropic's Claude 3 Opus, etc. [6] Although the model security strategy was refined in the later stage, the intrusion had already occurred and was not successfully avoided. In terms of foreign experience system, the risk prevention system is not yet perfect and the risk control awareness is relatively weak, although there are corresponding plans and measures, they are not yet mature, and the risk of mistakes is greater. Therefore, in the face of domestic and foreign experience systems, we must take the essence of it and eliminate its dross. Dialectically formulate a corresponding prevention system.

**C. Demand analysis**

The power of AI relies heavily on data, so data security and privacy protection are key to preventing risks. At the same time, in terms of transparency and bias of algorithms, the opacity of algorithms may lead to difficulties in understanding and tracing the decision-making process, which can lead to a crisis of trust, such as unfair treatment based on gender, race, age, and other factors. The People's Think Tank mentioned that 96.5% of respondents in the survey on the public's perception of the development of artificial intelligence said that they usually pay attention to the development of artificial intelligence. Among the "post-00s" and "post-90s" respondents, 91.1% and 96.4% of the respondents paid attention to its development, respectively. 66.8% of respondents believe that it is necessary to "accelerate the development of a new generation of artificial intelligence and strengthen the analysis and prevention of potential risks". 4.5% of respondents believe that "AI may have some adverse effects on human society". [7] These are some convincing statistics in China, showing the public's attention to AI and the need for risk prevention. Wu Jiangxing, an academician of the Chinese Academy of Engineering, once mentioned in an interview that the problem of generative AI is much bigger than that of traditional AI. In terms of generative AI, many netizens pointed out that most of the texts and pictures generated by generative AI will make people feel uncomfortable. Including many AI paintings on the market today, some body paintings will have one more finger or one finger less, the text is not in the right place, and the shape of the pseudo-human picture appears. These images are generated by reading the works and styles of different artists, and it is stated that in the event of use by a third party, the responsibility lies with the user. In addition to these known risks, the current AI is gradually changing from a tool to help people in their lives to a product that can be used by people with good intentions to cheat and trade with money. CCTV Finance "First Time" column reported that a college student in Qingdao had a video chat with a "girlfriend" he met on the Internet, and the other party said that he needed capital turnover, and the boy found that he had been defrauded after making money. Forensics found that the person chatting with him was a fraud carried out by the fraudsters through a virtual camera through "AI face swapping". Recently, a number of fraud cases using iPhone "Face Time" video calls have been reported across the country, and the means are also using "AI face

swapping". Even in daily life, many people will change their faces to short videos for entertainment. In fact, it is very risky, when you enter your real facial information, the platform will save it and synthesize it. If these facial information are transplanted into some horror, violence, and pornographic videos, it will infringe on the personality rights of the public. The Civil Code prohibits anyone from forging portraits with computer technology, which shows that this kind of problem is a very serious problem and has seriously threatened the rights and interests of citizens and information security. It can be seen that on the demand side, we must face up to the public's doubts about AI and make a value system for the prevention that the public needs.

**Design and Construction of the Prevention System**

**A. Analysis of the prevention system**

In the design of the AI legal risk prevention system, the core lies in building a multi-level and all-round protection network to deal with the legal risks that may arise in all aspects of data generation, transmission, storage and application. This system will focus on data privacy protection, copyright ownership, division of responsibilities and protection of user rights and interests, etc., to ensure that the development of AI technology can not only promote social progress, but also effectively avoid legal risks. At the same time, it also needs to be highly adaptable, able to continuously adjust and optimize with the evolution of technology and the update of laws to form a dynamic balance.

1. **The legal and regulatory framework is the cornerstone of the prevention system**

Currently, with the promulgation of a series of laws and regulations such as the Personal Information Protection Law and the Data Security Law, China has initially established a legal framework for the AI field. However, in the face of the rapid development of AI technology, laws often have a certain lag. Therefore, the prevention system must be forward-looking, not only following existing laws, but also anticipating possible legal trends in the future, taking into account potential legal risks, and ensuring the compliance of AI technology. For example, in the development of autonomous driving technology, companies not only need to comply with current traffic regulations, but also pay attention to potential legal provisions regarding the division of responsibilities for autonomous driving in the future, and prepare technical design and legal response strategies in advance. At the same time, the legal framework should also pay attention to the ethical issues of AI technology. It is explicitly stated that AI technology shall not infringe upon basic rights such as human dignity, privacy, and autonomy. It is stipulated that the application of AI technology in fields such as healthcare, education, and employment should follow the principles of fairness, impartiality, and transparency, and an AI ethical review mechanism should be established to rigorously review AI projects involving major ethical disputes. [8]

2. **Strengthening technical security controls is an important component of the prevention system**

The legal risks of AI technology are often closely linked to data security. Therefore, building an unbreakable data security defense line through technical means such as data encryption, access control, and audit tracing is an indispensable part of the prevention system. Taking medical AI as an example, patients' medical records and genetic information are extremely sensitive, and once leaked, it will cause serious consequences. Therefore, medical institutions and AI companies must use high-strength encryption technology to ensure the security of data during transmission, storage, and processing when utilizing this data for research and development. At the same time, establish strict access control mechanisms to finely manage data access permissions and prevent unauthorized access and leakage. In addition, through audit trail technology, every operational behavior of data can be recorded, providing strong evidence for post event responsibility tracing.

3. **Establishing a rapid response mechanism is the key to the effective operation of the prevention system**

In the practical application of AI technology, security vulnerabilities and infringement are difficult to completely avoid. Therefore, when security vulnerabilities or infringements are discovered, being able to respond quickly and take measures to minimize losses is an important goal of the prevention system. This requires enterprises to establish a dedicated security monitoring team to monitor the real-time operation status of AI systems. Once abnormalities are detected, emergency plans should be immediately activated for emergency repairs and disposal. At the same time, strengthen cooperation with external institutions such as government regulatory departments and industry associations, form a linkage mechanism, and jointly address security risks. For example, in the event of a data breach, companies should immediately notify affected users, cooperate with regulatory authorities to investigate, and strengthen technical protection to prevent similar incidents from happening again.

### B. Information source search

As the foundation of the prevention system, the quality and security of information sources have a crucial impact on the overall effectiveness of the system. In order to ensure the stability and efficiency of the prevention system, we must strictly screen and control the information sources to ensure their legitimacy and reliability.

In terms of data generated by artificial intelligence, we must clarify its source, scope of use, and permissions. This requires us to strictly comply with relevant laws and regulations during data collection and use, ensuring that all operations are carried out within the scope permitted by law. At the same time, in order to avoid unauthorized data collection and use, we need to establish a strict data management system to monitor the entire process of data collection, storage, and use.

In addition, for third-party data providers, we also need to strengthen auditing and supervision. This includes a comprehensive evaluation of their qualifications, reputation, data quality, and other aspects to ensure that the data they provide is legal, accurate, and free from infringement risks. Through this process, we can effectively reduce legal risks caused by data issues and lay the foundation for the stability of the prevention system.

#### 1. Legal regulations and policy documents

In terms of research on AI, we need to closely monitor relevant laws, regulations, policy documents, and standards related to the development of artificial intelligence both domestically and internationally, such as data protection laws (such as GDPR in the European Union, China's Data Security Law and Personal Information Protection Law, etc.), intellectual property laws, and liability attribution regulations. These laws and regulations provide us with a clear legal framework and guidance, helping us ensure that all activities are conducted within a legal and compliant framework. [9]

#### 2. Industry reports and research results

Industry reports and research results provide theoretical support and practical references for research, including reports, papers, and case studies on legal risks of artificial intelligence published by academic institutions, research institutions, industry associations, etc. They not only reveal the current problems and challenges, but also provide us with ideas and methods to solve them. By delving into these materials, we can better understand and respond to legal risks in the application of artificial intelligence.

#### 3. Enterprise Practice and Experience

Artificial intelligence is a huge engine for enterprise development, and many companies cannot avoid using AI technology in their production and operation processes. Therefore, corporate experience is an indispensable part of building a prevention system. The practical experience of enterprises in the application of artificial intelligence technology, including compliance practices in data collection, processing, and use, as well as legal issues and solutions encountered, has provided us with valuable references. By learning and drawing on these practical experiences, we can more effectively construct and improve the prevention system.

#### 4. Technological development and trends

The rapid development and continuous updates of artificial intelligence technology have put forward higher requirements for the construction of prevention systems. We need to closely monitor the latest developments and trends in areas such as algorithm optimization, model training, and data security technology in order to adjust and improve prevention strategies in a timely manner. At the same time, we also need to actively explore the application of new technologies in the prevention system to improve its efficiency and security.

### C. Division of Prevention Architecture

#### 1. Legal and regulatory module

The legal and regulatory module is a core component of the prevention system, responsible for collecting, organizing, and analyzing relevant laws, regulations, policy documents, and standards related to the development of artificial intelligence at home and abroad. The work of this module is not only limited to collection and sorting, but more importantly, it is necessary to conduct in-depth interpretation and analysis of these laws and regulations in order to provide legal support for other modules of the system. The importance of laws and regulations in the field of artificial intelligence was emphasized, and the key roles of data protection laws (such as GDPR, China's Data Security Law, Personal Information Protection Law) and intellectual property laws in building a prevention system were pointed out. By continuously updating and improving the legal and regulatory database, we can ensure that the prevention system is always synchronized with the latest laws and regulations, thereby avoiding risks caused by lagging laws and regulations. [10]

#### 2. Data Security Management Module

The data security management module is responsible for security control during data generation, transmission, and storage processes. In artificial intelligence applications, data security and privacy

are crucial. Therefore, this module needs to adopt advanced data encryption technology, access control mechanism and audit tracking means to ensure data security. At the same time, we should establish strict data management systems and processes to standardize the collection, storage, and use of data. This includes establishing data classification standards, clarifying data access permissions, implementing data backup and recovery strategies, etc. Through these measures, we can effectively reduce the risk of data leakage and abuse, and protect the privacy and rights of users.

### 3. Copyright management module

The copyright management module aims to clarify the copyright ownership of content generated by artificial intelligence. With the continuous development of artificial intelligence technology, more and more content is generated by machines. However, the issue of copyright ownership of these contents often sparks controversy. Therefore, we need to establish a copyright registration and licensing mechanism to ensure that the content generated by artificial intelligence can be legally protected and used. We can also see the negative impact of copyright disputes on artificial intelligence applications. Through the work of the copyright management module, we can prevent infringement, protect the legitimate rights and interests of innovative achievements, and promote the healthy development of artificial intelligence technology.

### 4. Responsibility allocation module

The responsibility allocation module clarifies the scope of responsibilities for each participant based on the different application scenarios of the artificial intelligence system. In artificial intelligence applications, multiple parties are involved, including data providers, algorithm developers, system operators, etc. Each participant should bear corresponding responsibilities and obligations. Through the work of the responsibility allocation module, we can ensure that in the event of legal disputes, the responsible party can be quickly identified and corresponding legal measures can be taken. At the same time, this also provides a clear basis for later compensation. We can see the importance of responsibility allocation in reducing legal risks and protecting the rights and interests of all parties.

### 5. User Rights Protection Module

The user rights protection module focuses on the protection of users' rights and interests during the use of artificial intelligence services. With the widespread application of artificial intelligence technology, users' privacy, right to know, and right to choose are receiving increasing attention. Therefore, we need to establish privacy policies, provide protection for the right to know, respect users' right to choose, and other measures to ensure that users' legitimate rights and interests are fully protected. We can see the importance of protecting user rights in enhancing user trust and promoting the promotion of artificial intelligence applications. Through the work of the user rights protection module, we can establish good user relationships and provide strong support for the sustainable development of artificial intelligence technology.

## Specific Issues in Project Implementation

### A. Implementation difficulties

In terms of implementation, there are mainly five difficulties. Lagging of laws and regulations: The rapid development of artificial intelligence technology often exceeds the update speed of laws and regulations, leading to legal gaps or ambiguous areas and increasing legal risks; Technical complexity: Artificial intelligence systems involve complex algorithms and data processing techniques, with high requirements for security control and difficulty in technical implementation; Cross disciplinary collaboration: The prevention system involves multiple fields such as law, computer science, sociology, etc., requiring cross disciplinary collaboration and making coordination difficult; Insufficient public awareness: The public's insufficient understanding of the legal risks of artificial intelligence may affect the promotion and implementation effectiveness of the project; The contradiction between data privacy and transparency: There is a contradiction between protecting user data privacy and improving algorithm transparency. How to ensure the fairness and interpretability of algorithms while protecting privacy is a major challenge.

### B. Research risks and mitigation measures

#### 1. Research risks

1. Adaptation challenges caused by rapid technological updates

The rapid development of artificial intelligence technology means that new legal risks are constantly emerging, and research often struggles to keep up with these changes immediately. For example, new algorithms or models may bring about new bias issues, and existing research may not yet cover these emerging fields.

2. Diversity of Legal Interpretation

The legal systems of different countries and regions may have significant differences in the regulation of artificial intelligence, and even within the same country, different judicial rulings may provide

different interpretations of the same legal issues. The diversity of legal interpretations increases the uncertainty of the applicability and universality of research results.

3. Social Ethics and Public Acceptance

In addition to legal risks, the widespread application of artificial intelligence may also trigger a series of social and ethical issues, such as employment substitution and privacy infringement. The public's attitude and acceptance towards these issues can also affect the assessment of legal risks and the development of prevention strategies. [11]

**2. Avoidance measures**

1. Strengthen legal research and publicity

Pay close attention to domestic and international legal and regulatory developments, adjust and improve the prevention system in a timely manner, and ensure consistency with laws and regulations. Increase investment in technological research and development, introduce advanced security control technologies and algorithms, and improve the technical level of the prevention system. Strengthen cooperation and exchanges with experts, scholars, and institutions in the fields of law, computer science, sociology, etc., and jointly promote the construction and improvement of the prevention system. Raise public awareness and importance of the legal risks of artificial intelligence through media promotion, public lectures, and other means, and create a positive social atmosphere. [12]

2. Establish mechanisms and promote innovation in legal policies

To cope with the challenges of rapid technological updates, a dynamic monitoring mechanism can be established to regularly track the development trends and emerging risk points of artificial intelligence technology, and adjust research directions and strategies in a timely manner. This can be achieved by forming interdisciplinary research teams and combining the strengths of technical and legal experts. Meanwhile, in the face of new challenges and problems brought by artificial intelligence, traditional legal and policy frameworks may no longer be able to meet practical needs. Therefore, promoting innovation in laws and policies has become an inevitable choice. This includes developing legal provisions specifically for artificial intelligence, revising existing laws and regulations to adapt to the development of new technologies, and so on. At the same time, it is also possible to explore the establishment of cross departmental collaboration mechanisms, strengthen communication and coordination between different fields, and jointly address the legal risks brought by artificial intelligence. [13]

3. Strengthen international cooperation and exchanges

Given the diversity of legal interpretations, strengthening international cooperation and exchange is particularly important. By participating in international legal forums, seminars, and other activities, we can understand the legal regulatory dynamics and best practices in different countries and regions, and provide reference for developing more comprehensive and effective prevention strategies.

**Project Summary**

**A. Research Conclusion**

The use of artificial intelligence is becoming increasingly widespread, but it also brings many controversial aspects and legal risks. In order to better serve people's learning, life, and work, and promote the further development of artificial intelligence, it is particularly important to build an AI legal risk prevention system. On the basis of a profound analysis of the challenges faced by current artificial intelligence, this project proposes new thinking and practical directions, providing useful reference and guidance for legal risk prevention of artificial intelligence. The aim is to ensure the healthy development of artificial intelligence and safeguard social public interests by establishing a legal risk prevention system for artificial intelligence under the premise of its development.

**B. Future prospects**

**1. At the national level**

After the successful implementation of this project, it will enrich and improve the theoretical system of legal risks in artificial intelligence, make the laws in the field of artificial intelligence more specific and in-depth, strengthen national supervision of the field of artificial intelligence, provide a good legal environment for the development of artificial intelligence technology, encourage technological innovation, and avoid unnecessary legal risks, which can better safeguard national security. With the deepening of international exchanges and cooperation, establishing a legal risk prevention system is also an important way to adapt to international regulatory requirements and enhance a country's participation and influence in global artificial intelligence governance.

**2. At the societal level**

This project will clarify the responsibility boundaries of all parties to prevent the infringement of personal privacy, intellectual property and other legitimate rights and interests due to improper use of technology, while avoiding social order chaos and

public safety threats caused by technology abuse, and better safeguarding social public interests and social order. Various industries and association organizations will further develop industry guidelines and standards for artificial intelligence, enabling enterprises to develop and use artificial intelligence in a more legal and compliant manner, and promoting the sustained and healthy long-term development of the artificial intelligence field.

### 3. On a personal level

This project will enhance public awareness and raise awareness and understanding of the legal risks associated with artificial intelligence through promotional and educational activities. Let the public understand the current development status, potential risks, and their own rights and obligations of artificial intelligence technology, and enhance their self-protection awareness and supervision ability. Encourage public participation in the governance of artificial intelligence, and create a good atmosphere for the whole society to pay attention to and prevent legal risks of artificial intelligence.

### Reference


[1] Zhang Xinyu. China News Weekly[J].2024

[2] Zhang Xinyu. China News Weekly[J].2024

[3] Hua Qingjian. "The team of the Chinese Academy of Social Sciences released a report on the value of security technology: artificial intelligence and security technology are the two major general technologies in the future (2024)" [R].China Economic Net

[4] Zhu Rongsheng, Qiao Guangyu, Su Shi. "The Alliance Politics of "Human Control" in the Global Governance of Lethal Autonomous Weapons", Center for Strategic and Security Research, Tsinghua University, No. 1, 2023

[5] Jiang Yue. "The first artificial intelligence security summit was held in the UK, signed by 28 countries and the European Union<Bletchley Declaration>"[C].21st Century Business Herald 21 Finance APP.2023

[6] Zhang Xue. The white paper "Large Model Security Practice (2024)" was released. AI security applications and risk management need to keep pace with the times and innovate and upgrade.2024

[7] People's Think Tank. Survey of public perception of the development of artificial intelligence. National Governance, No. 13, 2024

[8] Legal Risks of Artificial Intelligence and Its Prevention[D].Graduation Project (Thesis) of School of Modern Distance Education, Beijing Institute of Technology

[9] "2024 Two Sessions Artificial Intelligence and Intelligent Manufacturing Policy New Chapter" Sohu (Sohu.com)

[10] "2024 Global Artificial Intelligence Legal and Legal Issues", renrendoc.com Humanities Database

[11] "Artificial Intelligence Data Security Risk and Governance" original document (E-book Alliance)

[12] "2024 Legal Exploration Report on Artificial Intelligence" [R]. Sohu (Sohu.com)

[13] "2024 Artificial Intelligence Security Governance Framework Version 1.0 (Chinese Edition) - National Cybersecurity Standardization Technical Committee" Sohu (Sohu.com)