Risk Analysis and Countermeasure Research on the Development of Artificial Intelligence Industry

Xiaofeng Zhang

College of Management, Shanghai University, Shanghai 200444, China

Abstract. *With the rapid development of artificial intelligence, it brings great convenience to social life. On the other hand, the development of artificial intelligence will bring certain risks to society. Therefore, we need to face up to the development of artificial intelligence, and at the same time, we need to solve the existing risk problems, so that artificial intelligence can serve human life better.*

Keywords: *artificial intelligence, data security, privacy risk*

1. Introduction

The fourth industrial revolution is coming, and artificial intelligence has gradually entered the reality from science fiction. Now artificial intelligence is leading a new round of scientific and technological revolution and industrial revolution, which is making a significant and far-reaching impact on economic development, social progress, and national governance. [1] The world's major countries and the global industry have attached great importance to and actively deployed, and artificial intelligence will usher in a new wave of development. However, technology is often a "double-edged sword". It has its technical limitations and wide application, which brings many challenges to network security, data security, algorithm security and information security. [2]

2. Artificial intelligence and data

Artificial intelligence and data complement each other and promote mutual development. On the one hand, massive amounts of high-quality data help artificial intelligence develop. At this stage, the design and optimization of artificial intelligence algorithms represented by deep learning needs to be driven by massive quality data. Google research suggests that as the magnitude of training data increases, the performance of the same machine vision algorithm model rises linearly. On the other hand, artificial intelligence significantly improves data collection management capabilities and data mining utilization. Artificial intelligence is applied on a large scale in people's daily life and enterprise production and management. It acquires, collects and analyzes more user and enterprise data, and further promotes the technical capabilities of artificial intelligence semantic analysis, content understanding, pattern recognition, etc., to better achieve Massive data collected for rapid analysis and classification management. Moreover, artificial intelligence performs in-depth mining analysis on seemingly unrelated massive data, and can discover new knowledge such as economic and social operation rules, user psychology and behavior characteristics. [3]

3. Artificial intelligence data security risk

3.1 Data security risks faced by AI

Training data contamination can lead to erroneous decision making by artificial intelligence. Data poisoning destroys the integrity of data by adding dummy data, malicious samples, etc. in the training data, which leads to deviations in the training algorithm model decision. With the deep integration of artificial intelligence and the real economy, the construction of training data sets in medical, transportation, finance and other industries is urgent, which provides an opportunity for the injection of malicious and forged data, making it the most direct and effective to launch cyber attacks from the training sample. The method is potentially harmful.

Data anomalies during the run phase can cause the intelligent system to run incorrectly. First, artificial construction against sample attacks leads to intelligent system decisions that result in errors. Second, unconventional inputs to dynamic environments can cause intelligent systems to run incorrectly.

3.2 Data security risks caused by AI applications

Artificial intelligence applications can lead to excessive data collection and increase the risk of privacy breaches. With the popularization of various types of smart devices (such as smart bracelets, smart audio) and intelligent systems, artificial intelligence devices and systems are more direct and comprehensive for personal information collection. Artificial intelligence can collect biometric information with strong personal attributes such as user face, fingerprint, voiceprint, iris, heartbeat, and genes. This information is unique and non-deformive, and once it is disclosed or abused, it will have a serious impact on the rights of citizens.

Artificial intelligence amplifies data biased discrimination and threatens social justice. At present, artificial intelligence technology has been applied in the fields of smart government and smart finance, and has become an important auxiliary means of social governance. However, artificial intelligence training data tends to be biased in distribution, hiding specific social value trends, and even social prejudice. For example, massive Internet data more reflects the characteristics of China's economically developed regions and young and middle-aged netizens, but also for remote areas and young and old. The characteristics of the poor and the poor cannot be effectively covered. If the artificial intelligence system is affected by the potential social prejudice or discrimination of the training data, the decision-making result will threaten the fairness and justice of human society.

3.3 The privacy risks of AI

The universal use of artificial intelligence has caused a trend change in "human-machine relationship", and people and machines interact frequently. It can be said that a new type of relationship that is embedded is formed. The boundaries between time and space are broken, and virtual and real are switched at will. The unpredictability and irreversibility under this trend are likely to trigger a series of potential winds. Unlike "information leaks" that people tend to ignore, artificial intelligence techniques may also be purposefully used by a small number of people with ulterior motives for criminal activities such as fraud. For example, personal information obtained based on improper means forms a “data portrait” and fraudulently engages in acquaintances through social software. For example, using artificial intelligence technology to learn and simulate, generate information including images, video, audio, biometrics, and break through the security barrier. Last year, it was reported that the new Apple mobile phone "brush face" boot function was cracked. Example. From the perspective of potential risks, drones, unmanned vehicles, intelligent robots, etc., are subject to illegal intrusion and control, resulting in property damage or the possibility of being used for criminal purposes.

4. Measures

4.1 Establish artificial intelligence data security laws and regulations

The first is to promote legislation related to artificial intelligence and data security. At the national level, the “Data Security Law”, “Personal Information Protection Law” and artificial intelligence related laws were promoted, the legal principles of artificial intelligence data security were clarified, and the data rights and commitments of different participants in the various stages of the artificial intelligence life cycle were established. Safety responsibility set up artificial intelligence data security accountability system and relief system, and regulate the over-collection of artificial intelligence-related data, prejudice discrimination, resource abuse, deep forgery and other prominent issues, and provide basic legal basis for artificial intelligence data security management. [4] The second is to improve the regulations of the relevant departments of artificial intelligence data security. According to the relevant laws of the country, combined with the characteristics of artificial intelligence in different fields, it focuses on the key artificial intelligence data security risks in various fields, formulates and refines relevant departmental regulations, and proposes artificial intelligence algorithm design, product development and application of results in its field. Data security requirements in the process. [5]

4.2 Improve artificial intelligence data security supervision measures

The first is to carry out artificial intelligence data security supervision and punishment. In accordance with national laws and regulations, government departments have implemented artificial intelligence data security risks such as excessive data collection, data bias discrimination, and data resource misuse, and implemented supervision and inspection in various ways through online and offline to timely detect and prevent potential safety hazards. For serious bad behaviors such as cyberattacks based on artificial intelligence and deep forgery, using technical means of monitoring and public supervision, early detection, reducing harm and strengthening punishment. [6] The second is to carry out artificial intelligence data security testing and evaluation. Relying on industry organizations or third-party organizations, build artificial intelligence data security testing and evaluation platform, formulate data security testing and evaluation methods and index systems for artificial intelligence products, applications and services, develop safety testing and evaluation tools, and improve the safety of artificial intelligence products through testing and verification. Sex and maturity, reducing the risk of artificial intelligence data security. Through testing and evaluation to strengthen the data security and privacy protection of enterprises, it provides massive data support for the development and wide application of artificial intelligence.

References

[1] Zhang Zemin. Risk Analysis and Countermeasure Research on the Development of Artificial Intelligence Industry [J]. Modern Business, 2018 (30): 36-37. IResearch: 2019 China Artificial Intelligence Industry Research Report. [EB/OL]. 2019.

[2] Wang Yawei, Zhou Yuan, Chen Yiyi. Identification and Analysis of Technology Innovation Path of Artificial Intelligence Industry in China——Based on Patent Analysis Method [J]. Science and Technology Management Research, 2019, 39 (10): 210-216.

[3] China Zhitong Institute: 2019 Artificial Intelligence Data Security White Paper. [EB/OL]. 2019.8.14

[4] Zhu Xi, Chen Huihui, Tian Siyuan, Wang Hongwu. Artificial Intelligence: From Scientific Dream to New Blue Ocean——Analysis and Countermeasures of Artificial Intelligence Industry Development[J].Science & Technology Progress and Policy, 2016, 33 (21): 66-70.

[5] Ning Zhaoshuo. Analysis and Countermeasure Research on the Development of Artificial Intelligence Industry in China [J]. Journal of Shandong Administrative College, 2018 (01): 69-75.

[6] Gao Shanxing, Liu Jiahui. The Impact of Artificial Intelligence on Enterprise Management Theory and Its Countermeasures [J]. Science Research, 2018, 36(11): 2004-2010.