Security Issues in Commercial Application of Artificial Intelligence

Hongzhen Lin*
School of Hengda Management, Wuhan University of Science and Technology, Wuhan, China,
996672199@qq.com, corresponding author

Zhipan Yu
School of Hengda Management, Wuhan University of Science and Technology, Wuhan, China
937672021@qq.com

Shiqi Peng
School of Hengda Management, Wuhan University of Science and Technology, Wuhan, China
1321248247@qq.com

Bo Bian
School of Hengda Management, Wuhan University of Science and Technology, Wuhan, China
543182731@qq.com

ABSTRACT

This research aims to explore the security issues of artificial intelligence technology in commercial applications. Use literature research methods to correctly understand and analyze the commercial security issues brought about by artificial intelligence. The problems mainly include personal security issues, data security issues and privacy security issues. The main reasons for these problems include the inadequacy of relevant legal systems; the insufficient maturity of artificial intelligence security technology; and the insufficient standardization of artificial intelligence security standards. The effective solutions derived from this research mainly include: accelerating artificial intelligence legislation; strengthening artificial intelligence safety technology; and improving artificial intelligence safety assessment management.

CCS CONCEPTS

• **Computing methodologies**; • **Artificial intelligence**;

KEYWORDS

Artificial Intelligence, Security, Design

ACM Reference Format:
Hongzhen Lin*, Zhipan Yu, Shiqi Peng, and Bo Bian. 2021. Security Issues in Commercial Application of Artificial Intelligence. In *2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM2021), October 23–25, 2021, Manchester, United Kingdom.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3495018.3495359

1 INTRODUCTION

In recent years, with the advancement of science and technology, artificial intelligence technology has taken a huge step in many aspects, such as speech recognition and military applications. But so far, there are two biggest problems facing us with regard to artificial intelligence. One is that technological development is not enough, and the other is that many practical problems will arise in the application process. However, the application of artificial intelligence is becoming more and more extensive, and the resulting security risks have become issues that we have to pay attention to [1]. However, in our real life, the application scenarios are very open and relaxed, and traditional artificial intelligence is based on big data and empirical rules, which makes artificial intelligence easily affected by the outside world [2]. This topic selection is mainly aimed at the primary price range of the development of artificial intelligence, and analyzes from the perspective of the safety of artificial intelligence in commercial applications. On the one hand, I want designers to aim at practicality while not ignoring the safety issues of artificial intelligence. On the other hand, only by having a deeper understanding of the shortcomings of artificial intelligence can we be able to treat intelligent machines more objectively and calmly, lay the ideological foundation for the long-term development of artificial intelligence, and give corresponding thoughts on the problems at this stage.

AIAM2021, October 23–25, 2021, Manchester, United Kingdom

ACM ISBN 978-1-4503-8504-6/21/10…$15.00
https://doi.org/10.1145/3495018.3495359

2 LITERATURE REVIEW

2.1 *Review of Foreign Research*

Before 1956, people began to explore how machines could replace manpower. In Aristotle's syllogism, Bacon gave a relatively systematic research idea based on induction, and these have had a significant impact on the subsequent research on artificial intelligence. In the summer of 1956, McCarthy used the term "artificial intelligence" for the first time at an academic seminar [3]. The expert system studied by Feigenbaum has an analytical ability even surpassed that of chemical researchers in Western countries during the same period. However, after the 1970s, human beings have been relatively lagging behind in the development of computers, which makes artificial intelligence research practically useless. Scientists call this period the "Winter of AI." In 1997, the computer system Deep Blue successfully won the game with the World Go Championship, which also marked that artificial intelligence can really achieve a large number of tasks belonging to the human mind [4].

2.2 *Domestic Research Review*

In the 1950s and 1960s, artificial intelligence was just born, but when New China was just established, no one was doing research in China. Until March 1978, the National Science Conference was

held. After that, Qian Xuesen and others advocated research on artificial intelligence. Unfortunately, because the research was just starting at that time, many people conflated artificial intelligence with special functions and the development was slow. After the reform and opening up, in order to develop artificial intelligence, our country has sent many young scholars to study advanced theoretical knowledge abroad. However, "artificial intelligence" was not directly mentioned at the time. After entering the 21st century, more research topics on artificial intelligence and intelligent systems have received key and major projects from the National Natural Science Foundation of my country. Research in the field of artificial intelligence in China has also been promoted to the level of national strategy. Opportunities and challenges have also been adequately prepared [5].

3 MAIN ISSUES IN THE COMMERCIAL APPLICATION OF ARTIFICIAL INTELLIGENCE

3.1 *Personal Safety Issues*

In 1978, the world's first robot "killing" occurred in Hiroshima, Japan. When a factory worker was on duty, the robot broke down and cut it as a steel plate. Unfortunately, this happened. In 1985, in a human-machine chess match, Gudkov, who won the former Soviet Union chess champion, was electrocuted by a high-voltage current released by a robot chess player. The robot became angry because of three consecutive victories. The program there was an abnormality that caused this tragedy to happen.

In 2018, the world's first driverless car caused a personal death in Arizona, the United States. An Uber driverless car broke down during driving and could not accurately identify pedestrians outside the crosswalk, causing a woman to die on the spot. Accidental injuries caused by the use of artificial intelligence weapons in wars are also very common. For example, when a drone is hitting a target, if it uses scattered warheads and multiple warheads, it cannot accurately lock the target for precise strikes, or the lock target is pretended to be disguised, and artificial intelligence weapons cannot accurately identify it. These recognition errors will Cause a wide range of accidental injuries. Between 2004 and 2012, the United States used artificial intelligence weapons to strike about 400 air strikes against terrorist organizations in Afghanistan. The number of children and civilians killed by artificial intelligence weapons has reached tens of thousands. The application of artificial intelligence equipment in war has made the country humanitarian. Doctrine has fallen into an endless abyss [6].

3.2 *Data Security Issues*

Artificial intelligence is a new generation of weather vane presented by the superposition of the Internet, big data and machine intelligence. When governments, enterprises and social organizations rely more and more on large-scale data collection, analysis and use when maintaining their respective operations, the operation of the entire society is also It is proceeding smoothly in the form of digitization and transparency. The advent of the artificial intelligence era exposes personal privacy to the sun or indulges in the darkness, and turns the figurines on people into transparency, which also puts a big exclamation mark on the necessity of "privacy protection"[7].

In daily life, it is no longer uncommon for people to serve artificial intelligence products. Such as map navigation, face recognition, language assistant functions, etc., all reflect the close relationship between artificial intelligence and humans. Large-scale intelligent machines collect and organize your personal data information on the Internet 24 hours a day, including your name, age, phone number, address, location, etc. Through simple analysis and generalization, the user's personal habits, eating habits, and shopping preferences can be depicted. And, by further depicting personal information such as the individual's action track, communication range, sexual orientation, etc., a user's portrait can be generated. Due to system security vulnerabilities, hacker attacks and other reasons, the personal data of some informal professional websites are facing potential security risks such as leaking, stealing, and being traded [8].

3.3 *Privacy and Security Issues*

In March 2018, according to British and American media reports, Cambridge Analytica obtained unauthorized access to the information of more than 50 million users on the American social media Facebook, designed software to analyze users' political intentions, and predict and influence voter votes. The negative effects of this blockbuster incident greatly reduced Facebook's business reputation, severely infringed on the legitimate rights and interests of the public, and aroused public reflection on privacy. In the era of rapid development of artificial intelligence, it is not uncommon for companies to misuse user data without permission to mine commercial value. Privacy protection suffers from unprecedented crises [9].

The development of modern human civilization is increasingly inseparable from data, and the generation and progress of artificial intelligence is also closely related to big data. When these data are collected and summarized, they will inevitably involve all aspects of people's daily life, work, and interpersonal relationships, which poses a great threat of personal privacy leakage. Most users will provide corresponding information as required out of trust when using smart software, but users are not aware that their information may be collected and used. These are the behaviors of data collectors or controllers leaking personal information without user authorization during the development of artificial intelligence. Therefore, data security and privacy protection in the era of artificial intelligence are very critical core issues. As Iris said: "Personal privacy is not a problem of data analysis to a certain extent, but the dark side of the digital process"[10].

3.4 *Legal Dilemma*

With the steady development and maturity of artificial intelligence technology, although it has greatly facilitated people's daily life and promoted the normal operation of the social system, it has always been a hidden danger to personal privacy leakage and the threat of data leakage. Some legal systems have brought huge impacts and challenges.

When robots can completely replace humans in certain tasks, and when robots are increasingly recognized, who should be responsible for the mistakes made by robots? Is it the developer of the robot or

the robot itself? Can the robot bear the blame? If they can't do or do something wrong with people's responsibility, who should bear the responsibility? [11]

In October 2009, a driver in the United Kingdom drove normally following the route planned by GPS navigation, but accidentally rushed down the cliff and crashed the fence of someone else's manor. Although the British court finally attributed the accident to GPS, it still held that the driver was at fault for careless driving. Although this is a traffic accident caused by technology rather than man-made, the current laws and regulations do not match it, but the courts tend to make judgments against humans. Obviously, the advent of the era of artificial intelligence has put into question the applicability of the original blunt legal provisions: why should the evil consequences created by humans' faults be borne by humans? Contemporary artificial intelligence is very different from traditional ones. It is no longer for human use only, but is deployed by humans [12]. Once deployed, artificial intelligence machines will no longer operate independently according to instructions based on the collected and analyzed data. In this sense, the previous concept of not being able to sue robots needs to be changed according to the development of artificial intelligence.

4 MEASURES TO SOLVE THE SECURITY PROBLEMS OF ARTIFICIAL INTELLIGENCE

4.1 *Strengthening Artificial Intelligence Security Technology*

Strengthen information encryption technology. The degree of encryption of information is closely related to the security of artificial intelligence devices [13]. For the data processing and calculation quantity of artificial intelligence, the solid state hard disk of traditional computer system can not bear the huge amount of computation caused by artificial intelligence complexity, and the degree of information encryption will also be reduced. Traditional computers can not meet the needs of artificial intelligence security maintenance. But if the data is processed and presented by quantum computer, on the one hand, quantum encryption can be obtained to ensure the security of artificial intelligence maintenance, on the other hand, it can improve the efficiency of data transmission and improve the stability of data system. Determine the appropriate system carrier. The system carrier is the foundation and guarantee of the security of artificial intelligence information. However, there are obvious operating system loopholes in all kinds of known systems, which need to be upgraded and modified in the subsequent maintenance service. Therefore, only using the operating system on the market can not ensure the security of AI devices, and there is no risk. This fundamentally determines that AI needs to develop a new programming language and establish an independent database to obtain information. In addition to reserving information interface and resource data sharing, the machine system needs to be able to receive external information, such as voice, touch and so on, through its unique sensor, so as to carry out normal data processing and interaction, and ensure the security of artificial intelligence information.

Improve the controllability of artificial intelligence. The goal of AI is to learn deeply and control independently, which makes it possible to cause uncertainty risk to human society. In order to reduce this risk to an acceptable range, artificial intelligence devices need human control and intervention. Therefore, the design experts of artificial intelligence need to take the adjustment and control of artificial intelligence ideology into consideration in the process of R & D, realize the effective management of artificial intelligence equipment, and ensure that artificial intelligence can play its advantages in the appropriate fields without abuse.

4.2 *Establishing the Safety Standard Specification of Artificial Intelligence*

The control of artificial intelligence equipment is the key to ensure the security of artificial intelligence. In order to ensure the human control over artificial intelligence equipment, relevant departments need to establish the artificial intelligence security standard and specification. Researchers should report to relevant departments before researching artificial intelligence, obtain corresponding certification and approval before conducting research and development of artificial intelligence, so as to ensure that the work does not violate the basic rules of society and maintain the safety of artificial intelligence equipment. At the same time, the solution measures are provided for the defects and errors in the operation of AI equipment, and further escort the safety of AI.

Improve the management of artificial intelligence security assessment. Improving the management of artificial intelligence security assessment is an effective way to reduce the security problems of AI equipment. In the process of R & D, artificial intelligence researchers should constantly improve and improve the evaluation and management of artificial intelligence. Through the safety assessment, researchers of artificial intelligence should find out the shortcomings and defects in the system in time, and avoid the artificial intelligence in the production process the security problems in it. therefore, air & D personnel need to adopt dynamic management method in daily design research and production process, strengthen supervision of artificial intelligence equipment, constantly adjust assessment management, build artificial intelligence security assessment model and simulation mechanism, and pre predict the possible safety problems of AI in various design and production links through the knowledge of Statistics Measure and formulate corresponding solutions in advance to reduce the risk of artificial intelligence security problems.

Design the moral mechanism of artificial intelligence. Researchers should be highly alert to moral risks in the process of designing artificial intelligence, and formulate relevant artificial intelligence moral mechanism, endow basic moral evaluation and judgment ability of artificial intelligence, and ensure that the evaluation and judgment made by AI in the process of interaction with human beings meet the current social moral standards. Meanwhile, in the case that AI cannot reasonably and accurately judge whether the behaviors of the other party and itself conform to the basic moral standards, the automatic stop function of artificial intelligence is added to avoid the wrong behavior caused by the wrong judgment or malicious control and utilization of the other party during the interaction with human beings. By increasing the design of artificial intelligence moral mechanism, not only give the maximum autonomy of AI within the controllable range, but also ensure the use safety of artificial intelligence.

4.3 *Improving the Relevant Laws of Artificial Intelligence*

With the continuous innovation and development of artificial intelligence, a series of legal problems have been brought. For example: artificial intelligence causes information leakage and personal injury of the issue of responsibility. At present, there are still many gaps in the law of our country in artificial intelligence. Therefore, the relevant departments should attach great importance to the work of artificial intelligence legislation and arrange macro legislation in time. Legal personnel can start to formulate laws and regulations from some relatively mature technical fields, gradually form a complete artificial intelligence legal system, and lay a solid foundation for the existing legal problems in the future development of artificial intelligence.

5 CONCLUSION

With the continuous advancement of science and technology, artificial intelligence has entered a stage of rapid development. The in-depth research and extensive application of artificial intelligence has also caused more people to pay attention to the safety of artificial intelligence. Although there may be security risks in the use and operation of artificial intelligence, we must not choke and kill artificial intelligence in the cradle. Instead, we should actively take effective measures to avoid artificial intelligence from legal, technical, institutional, and ethical aspects. Safety issues in various production and application links have made artificial intelligence play an important role in its superior areas and become a good helper for mankind.

ACKNOWLEDGMENTS

This research was supported by the National Social Science Foundation of China Name of the project: "Entrepreneurial law education research based on risk control in science and Engineering University" (Grant No. BIA170192)

REFERENCES

[1] Chen Yufei, Shen Chao, Wang Qian, *et al.* Security and privacy risk of artificial intelligence system. Computer research and development, 2019, 56 (10): 111-126
[2] Yuan Li Ke. AI security risk challenge and legal response. China Science and Technology Forum, 2019, 274 (02): 9-10
[3] Xu Dahai. Security and privacy risk of artificial intelligence system. Electronic technology and software engineering, 2020, No. 176 (06): 236-237
[4] Wei Wei, Jing Huiyun, Niu Jinxing. Artificial intelligence data security risk and Governance . China information security, 2020, No. 123 (03): 83-86
[5] He Zhe. Towards the era of artificial intelligence. Electronic Government Affairs, 2016(12): 9
[6] Liao Tianxiang. Analysis of artificial intelligence security. China Science and Technology Investment, 2018(5):291
[7] Ailun. Dafu. Artificial Intelligence Security and Governance. Information Security and Communication Secrecy, 2019(10):13-15
[8] Bi Zhonghao. Research on artificial intelligence security issues and countermeasures. China New Telecommunications, 2019(1):136
[9] Yi Kai fan, Shao Qian, Chen min. artificial intelligence security: analysis of counterattack . Computer science and application, 2019, 9 (12): 10
[10] Chen Weijie. Research on Design of network security defense system based on artificial intelligence. China new communication, 2019, V.21 (15): 154-155
[11] Wan HAOGE. Discussion on the combination of artificial intelligence technology and Internet Security. Science and information, 2019, (02): 52-52
[12] Wang Xingwei, Li Dan, Su Jinshu, *et al.* Introduction to 2019 intelligent network theory and key technologies . Computer research and development, 2019, 56 (5): 907-908
[13] Liu Donghai, Fang Chao, Leng Zhenghua. Application of artificial intelligence in safety management. Building safety, 2020 (9): 31-34