Vol.5 No.5(2019)

INTERNATIONAL
SECURITY AND STRATEGY STUDIES

REPORT

AI Data Security Governance and Ethics in China: A Piece of the Puzzle in "Fragmented Governance"

清华大学战略与安全研究中心
CENTER FOR
INTERNATIONAL SECURITY AND STRATEGY
TSINGHUA UNIVERSITY

AI Data Security Governance and Ethics in China: A Piece of the Puzzle in "Fragmented Governance"

Zhu Rongsheng[1] Yu Yang[2]

With the large collection of personal data by various intelligent devices and intelligent systems, data security risk has become a key factor that affects each country to develop artificial intelligence(AI) safely. Apple, which has traditionally emphasized to protect customer's data, is accused of violating customer privacy. In July 2019, apple was found to have let its contractors use customers' voice messages without their consent. The content of conversations are clear and easy to listen to, along with personal information such as location and contact information are exposed. This arouses the public concerns about Apple ,and "Hi Siri, are you spying on me" has become a hot word. Another well-known example was the "Facebook breach" in 2016. Cambridge Analytica collected data from more than 87 million Facebook users, and used artificial intelligence to target political advertisements that influenced voters' ideology and political views in the 2016 election of United States. This incident not only reflects the risk of data leakage and data security in AI application scenarios, but also shows that this technology may increase the challenges of social governance and national security.

In the era of artificial intelligence, how to deal with the challenge of data

1 Tsinghua University Center for International Security and Strategy, research fellow

2 Tsinghua University Institute for Interdisciplinary Information Sciences, assistant Professor

security has become an important issue for all countries including China. Can we find some useful lessons for global AI data security governance from China's governance experience? An app named "zao", which uses Deepfake technology, went on sale in the Chinese app store on Aug 30, 2019. By submitting a clear picture of user's face, users can replace the faces of actors in movies or TV shows with their own. Zao's score in the app store rose quickly and once occupied the top of the hot search list within one day. However, the popularity didn't last long that outside world began to question the risk of data breach of zao, and complained about the terms of data can be used "completely free, irrevocable, permanent, sublicensing worldwide". On September 3rd, the Ministry of industry and information technology met the company's officials and asked them to make corrections in strict accordance with national laws and regulations and the requirements of relevant authorities. This case shows that in the lack of a systematic legal system of artificial intelligence in China, enterprises that violate ethical norms and relevant laws and regulations are not only unable to make profits sustainably, but also will be punished by both the market and regulatory authorities.

The data security failures of Facebook and Zao show that if companies can't protect people's privacy in the age of artificial intelligence, they will lose their customers. When companies pursue the interests, they need to abide by ethics and laws and regulations. In China, companies are among the first to use artificial intelligence technology to conduct in-depth analysis of data in the internet, mining harmful information to provide support for social governance. Tencent claimed in September 2018 that its "bingo" a system ,which provides services to 31 Chinese provinces and cities for anti-fraud prevention has saved Chinese people 2 billion yuan in total by providing more than 50,000 alerts with an accuracy rate of over 99 percent since it was put into use. According to a report released by Baidu

"comprehensive management of information security in the first half of 2018", Baidu processed 14.54 billion pieces of harmful information in the first half of 2018, among which pornographic and gambling information accounted for 51.04% and 16.63% respectively.

In addition, Chinese companies are also important actors to promote the construction of ethical norms for data security governance. By issuing ethical principles, they could regulate their productions and build a trustworthy image so that strengthening their competitiveness in domestic and international markets. While demonstrating social responsibility, they also use it to shape industry norms and lead the construction of "soft law". Baidu put forward four ethical principles of artificial intelligence, taking safety and controllability as the highest principle. Tencent and the Chinese Academy of Sciences jointly released the six principles of AI in 2017, namely freedom, justice, well-being, ethics, safety and responsibility. It is emphasized that the development of AI should strengthen the protection of privacy, strengthen the control of personal data, prevent data from being abused, and the collection and use of personal data should conform to norms and legal systems.

Now, the discussion of AI principle is a hot topic in Chinese society. Not only enterprises, but also academia, industry and the Chinese government have issued the AI principles, emphasizing that data security protection should be strong when using ai. In May 2019, China's universities, research institutes and industry alliance jointly released the "Beijing consensus on artificial intelligence", which put forward 15 principles for the development, usage and governance of artificial intelligence.In terms of data security protection, the consensus proposes to "realize the data security of artificial intelligence system", "encourage the establishment of an artificial intelligence open platform to avoid data and platform

monopoly", and "establish a reasonable data and service cancellation mechanism to ensure that users' rights and interests are not infringed". In June 2019, China artificial intelligence industry alliance released "the self-regulation convention on artificial intelligence (consultation draft)", which specifically lists the principles of privacy protection. Released at the 2019 world artificial intelligence conference, "the 2019 Shanghai declaration on artificial intelligence innovation governance for young Chinese scientists "calls for the formulation of relevant laws and regulations, strengthening of privacy protection awareness, and the development of privacy protection algorithms and technologies. The positive action of the industry and academia on building the ethical norms reflects that Chinese society is willing to accept the extensive application of artificial intelligence technology and also hopes to establish norms to ensure safe use.

In June 2019, the national professional committee on new-generation AI governance released the "new generation AI governance principles", which makes respect for privacy as one of the eight principles. According to the principles, the development of AI should respect and protect the privacy of individuals and fully protect their right to know and choose. Meanwhile, the Chinese government is speeding up the legal process. In 2016, China's "Cyber security law" added new provisions such as the right to delete information, the right to know, and the right to correct. Since 2018, China has been strengthening the relevant legislation on the protection of personal data for "Data security law" and "law on the protection of personal information", and has issued draft opinions on the "Management measures on data security" and "Measures on the assessment of the exit security of personal information" to the public.As the concerns about the Deepfake rise, China amended the "Civil code of personality (draft)" in 2019, which stipulates that no organization or individual shall infringe upon the right of portrait of others by means of information technology forgery. This means

the use of the Deepfake will be banned by law in the future.

From a perspective of global governance, major countries have put forward governance plans, yet worked together to establish an international cooperation mechanism. This makes AI governance appear to be fragmented. global governance is influenced by domestic governance. The AI data security governance is to deal with the problems faced by countries as well as the ethics reflects their own values. Moreover, there is no common technical standard for artificial intelligence. This makes global governance solutions more diverse. And it makes a global governance become a "fragmented governance". The development of AI is still "Narrow AI". The outstanding performances in the field of commercial application are mainly image recognition, voice recognition, natural language and other aspects. According to scientists,the existing algorithm applies to the theories that came up years ago, it will take time to create new theory to achieve "Super AI". That is to say, the science fiction scenario of artificial intelligence replacing humans is still a long way off. It might be one of the reasons that Countries may not feel the urgent need to take action to accelerate the establishment of relevant international mechanisms.

China's experience comes from its complex governance realities. It appears that China is taking a market-oriented and government-guided approach. Chinese people are happy to use AI to make life convenient, but also worry about the potential risk of data leakage. Many cases have shown that enterprises' violation of social values and ethics will damage their brand image and face punishment from the market, law, public opinion and other aspects. Therefore, it becomes a part of self-interests that enterprises should participate in AI governance and regulate their behavior along with the ethics. Like many other countries, China has recognized that AI could poses challenges to national security and has taken various measures

to improve system of laws and regulations and promoting the form of AI ethics. However, the rapid development of artificial intelligence and extensive social impact makes the legislation lag behind the emergence of problems. This grave challenge is not unique in China. Europe recently published a review of GDRP over the past year. What has been called the most stringent data security regulations in history does not fully respond to expectations. It is not to say that EU's effort is failed nor china's, rather it should be deemed as a dynamic process. Some claims that AI governance is part of power competition and makes it harder for cooperation , but what we can see now is that the competition actually has the effect of making a complementary global governance from "fragmented governance".

Center for International Security and Strategy of Tsinghua University

Address：Room 217,Mingzhai,Tsinghua University

Tel：+010-62771388

E-mail：ciss_thu@163.com