Research on Legal Issues and Strategic Recommendations for National Security in the Era of Big Data and Artificial Intelligence

Yihe Gao

China University of Political Science and Law, Postal Code: 102249

Abstract. The extensive application of big data and artificial intelligence technologies has brought both opportunities and challenges to national security. Building and improving the legal system for national security is a necessary condition for a sound national security system. This article analyzes the potential data security and information security issues that may arise from big data and artificial intelligence technologies, and clarifies the deficiencies in relevant laws, systems, and policies. By comparing the legislative situations of big data and artificial intelligence technologies in China and the West, it proposes specific strategic suggestions from three perspectives: strengthening the construction of laws and regulations, establishing and improving regulatory mechanisms, and enhancing the publicity of cyber security.

Keywords: Big data, artificial intelligence, Safety legal system, laws and regulations.

1. Introduction

With the rapid development of big data and artificial intelligence (AI) technologies, their impact on the field of national security has become a highly focused topic. The widespread application of big data and AI presents new opportunities and challenges for national security. The use of these technologies brings potential risks such as privacy breaches and information misuse, which could impact individual rights and social stability. The rule of law in national security is the foundation of the national security system. Ensuring the rule of law for national security in the era of big data and AI has become an urgent and significant issue that requires thorough research and resolution.

This study aims to explore in-depth the issues and challenges faced by the rule of law in national security in the context of big data and AI. It seeks to identify the deficiencies and imperfections in relevant laws, institutions, and policies, and to propose strategic recommendations. Specifically, the research objectives include but are not limited to: analyzing the relationship between the China overall national security outlook and the rule of law in national security; examining the challenges posed by big data and AI technologies to the national security legal framework, including issues related to privacy protection and data security; exploring the evolution and development of the concepts and principles of national security law in the era of big data and AI; and proposing targeted suggestions and strategies to strengthen the construction of the national security legal system, ensuring a balance and coordination between national security and citizens' rights.

The paper first delves into the relationship between the China national security outlook and the rule of law in national security. After comparing and analyzing relevant domestic and international laws, it reveals the challenges posed by the development of big data and AI technologies to China's national security rule of law from four perspectives: overall national security, legislation, law enforcement, and compliance. It then provides relevant strategic recommendations from three aspects: strengthening the construction of laws and regulations, establishing and improving regulatory mechanisms, and enhancing cybersecurity awareness. Finally, the paper summarizes and outlines the research findings.

2. The Theoretical Foundation of the Rule of Law in National Security

2.1. The Theoretical Connotation of the China overall national security outlook

The national security outlook is the fundamental perspective of a country on what constitutes national security, why it is necessary to maintain it, and how to do so during its development process. Since the 18th National Congress of the Communist Party of China, under the leadership of Xi Jinping, the Party has adhered to the worldview and methodology of dialectical and historical materialism. It has combined Marxist national security theory with the specific realities of China's national security construction in the new era, proposing and implementing the China overall national security outlook. [1]The report of the 20th National Congress of the Communist Party of China emphasized, "We must unswervingly implement the China overall national security outlook, integrate the maintenance of national security into all aspects of the Party's and the country's work, and ensure national security and social stability." The emphasis on the China overall national security outlook highlights the holistic, comprehensive, and interconnected nature of China's national security theory, underscoring the leading role of national security throughout all aspects and processes[2].

From the perspective of the China overall national security outlook, the scope of national security has significantly expanded. the China overall national security outlook not only inherits the traditional national security theory but also enriches its connotation by incorporating changes in domestic and international circumstances in the new era. It includes information security and data security as part of national security. Under the guidance of the China overall national security outlook, building a comprehensive management system for big data and AI not only helps China seize the opportunities presented by the digital economy but also enhances the country's security governance capabilities.

2.2. The Relationship Between the National Security Legal System and the China overall national security outlook

National security plays a leading role in all aspects and processes. the China overall national security outlook provides the general direction and guidance on what constitutes national security, why it must be maintained, and how it should be protected. In today's rapidly changing global landscape, marked by unprecedented transformations and a complex international environment, the great rejuvenation of the Chinese nation has entered a critical stage. Development issues are increasingly intertwined, posing threats to national security and social stability. In response, the report of the 20th National Congress of the Communist Party of China has made specific arrangements, emphasizing the need to "improve the national security system, enhance the ability to safeguard national security, raise the level of public safety governance, and improve the social governance system." It particularly stresses the importance of "strengthening the coordination mechanism for national security work, improving the national security legal system, strategic system, policy system, risk monitoring and early warning system, national emergency management system, and the security assurance system for key areas and important special coordination and command systems. It also highlights the need to strengthen the security assurance systems for the economy, major infrastructure, finance, cyberspace, data, biology, resources, nuclear, space, maritime, and other areas." Among these, the national security legal system serves as the foundational support for the five major systems and is a crucial guarantee for advancing the modernization of the national security system and capabilities. In other words, building and improving the national security legal system is a necessary condition for enhancing the national security system, which is one of the key requirements of the China overall national security outlook. Overall, the China overall national security outlook guides

[1] Yuan Yin-chuan, Wang Xing-yue. Basic Connotation, Basic Requirements, and Realization Path of the Overall National Security Concept [J]. Research on Ideological Education, 2023, (04): 3-9.

[2] *Xi Jinping: Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects—Report to the 20th National Congress of the Communist Party of China*, The Central People's Government of the People's Republic of China, October 25, 2022.

the construction of the national security legal system, and establishing such a system is a key objective of the outlook. Therefore, maintaining data security and information security in non-traditional security areas must be carried out within the framework of the rule of law, and appropriately addressing the legal issues brought about by big data and artificial intelligence is an inevitable requirement for constructing a comprehensive national security legal system.

3. Challenges and Issues Brought by Big Data and Artificial Intelligence to the National Security Legal System

In terms of legislation, big data and artificial intelligence have opened up new ways of network application and expanded the scope of social life, making it urgently necessary to improve the relevant legislative system. From the perspective of national security legislation, the focus has traditionally been on conventional security fields, while legislation in non-traditional security fields has been fragmented, scattered, and lacks comprehensive coverage. There are two primary reasons for the inadequacies in legislation related to big data and artificial intelligence. First, the rapid development of AI and big data technologies has outpaced the legislative process, and hastily drafted laws may not adapt well to societal development. Overly detailed regulations might not only present challenges in legal application but could also hinder the development of big data and AI technologies in China. The current approach of sector-specific legislation allows for necessary adjustments in relevant fields while leaving room for further refinement and flexibility in future legislation. Second, there has been relatively low emphasis on non-traditional security by the state. National security-related legislation remains focused on traditional security areas such as political security, economic security, and cultural security. The understanding and theoretical framework regarding non-traditional security are not yet fully developed, and the state does not prioritize this area as much as traditional security, resulting in legislative gaps. Additionally, there is a fundamental issue in legislation related to big data and AI: the value conflict between security and freedom. As the application of big data and AI becomes more pervasive in people's lives, the technology increasingly infiltrates personal privacy, blurring the lines between lawful application and illegal use. How to define the legal boundaries of big data and AI usage remains an open question worthy of exploration.

In terms of law enforcement, there are two main issues. First, the enforcement agencies are not clearly defined. In China, network governance is primarily the responsibility of the Public Security, Propaganda, and Ministry of Industry and Information Technology departments, with other relevant departments such as Culture and Education participating in network cultural security management based on their respective duties. Although this management approach facilitates comprehensive coverage of network security governance, it also presents several problems. For instance, in actual law enforcement, there can be buck-passing among departments, weakening the effectiveness of network cultural security governance. The root cause of this issue lies in the overlapping administrative functions among different government departments, resulting in poor collaboration and difficulty in forming an effective joint force despite the apparent multitude of enforcement agencies. Second, the relevant technical infrastructure is relatively weak. The development of existing network reconnaissance and enforcement technologies struggles to keep pace with the rapid application of new technologies. Enforcement agencies have a relatively shallow understanding of big data and AI, with insufficient specialization. Combined with the massive scale of big data and networks, the increasing difficulty of regulation presents more challenges for network law enforcement.

In terms of compliance, public awareness of network law is weak. In recent years, China's internet user base has grown rapidly, with a large total number of users. As of June 2023, the number of internet users in China reached 1.079 billion, an increase of 11.09 million from December 2022, with an internet penetration rate of 76.4%. The expansion of the internet user base has made data sources for big data and AI more extensive, leading to an increase in legal issues. The pace of legal education and awareness regarding network laws has not kept up with the speed of network development,

indirectly causing some internet users to have their personal information rights violated or confidential information leaked online, posing risks to both personal and national security.

In summary, from a national security perspective, the development of big data and AI technologies primarily leads to issues such as improper information disclosure and disruption of social order. The "largest data leak in CIA history" mentioned how the West illegally obtained information from Chinese user databases, posing a significant threat to China's national security. At the same time, AI-driven "deepfake technology" based on neural networks continually challenges legal boundaries. Deepfake technology, enabled by AI, could be used by criminals to spread false videos, exacerbate social conflicts, incite violence and terrorism, or interfere with intelligence agencies in hostile countries. Additionally, this technology could trigger social anxiety and trust crises, deepening public distrust in the government. Given the risks of improper information disclosure and social disorder brought about by big data and AI, finding appropriate countermeasures and defensive strategies is urgent. While seeking technological responses, China should also accelerate the construction of a corresponding cybersecurity legal system to improve national security governance through the rule of law.

4. Analysis of Domestic and International Laws and Practices

4.1. Laws and Practices in Key International Countries

On March 15, 2022, U.S. President Joe Biden signed the *Strengthening American Cybersecurity Act*, which comprises three cybersecurity legislative measures: the *Cyber Incident Reporting for Critical Infrastructure Act*, the *Federal Information Security Modernization Act of 2021*, and the *Federal Secure Cloud Improvement and Jobs Act*. This act includes a series of measures aimed at modernizing the cybersecurity posture of the U.S. federal government and improving coordination among federal agencies by streamlining existing cybersecurity regulations. The passage of this act will help ensure that critical infrastructure, such as banks, power grids, water supply networks, and transportation systems, can quickly recover from cyberattacks and continue to provide essential services to the public.

The European Commission proposed the *Artificial Intelligence Act* on April 21, 2021, which was passed by the European Union on June 14, 2023. On December 8, 2023, the European Parliament, EU member states, and the European Commission reached an agreement on the *Artificial Intelligence Act*. This act aims to introduce a common regulatory and legal framework for artificial intelligence. Excluding military use, the act covers all types of AI. As part of product regulation, it governs AI system providers and professional users.

With the continuous development of big data and AI technologies, both the United States and Europe have enacted relevant laws to address new challenges. Overall, the EU's *Artificial Intelligence Act* is more targeted at regulating AI applications, while the recently enacted *Strengthening American Cybersecurity Act* focuses on traditional cybersecurity and has relatively fewer regulations addressing emerging AI technologies.

4.2. Domestic Laws and Practices

In China, laws closely related to big data and artificial intelligence include the *Cybersecurity Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, and the *Data Security Law of the People's Republic of China*.

The *Cybersecurity Law*, enacted in 2016, was introduced relatively early and provides general regulations on the lawful use of networks and the protection of personal information. The law institutionalizes some of the mature and effective practices developed in recent years and sets out general provisions for potential future innovations, offering a solid legal foundation for cybersecurity work. It also establishes three principles for governing cyberspace: the principle of cyber sovereignty, the principle of balancing cybersecurity and informatization development, and the principle of collective governance. The *Cybersecurity Law* is China's first fundamental law addressing

cybersecurity issues, marking an important milestone in the country's effort to establish the rule of law in cyberspace. It is a critical legal tool for managing online risks and ensuring the healthy operation of the internet within the framework of the rule of law.

The *Data Security Law* provides further regulation in areas such as industry-specific regulatory requirements, data export controls, classification systems, countermeasures in the data field, and government data openness. The enactment of the *Data Security Law* represents a significant advancement in China's legal framework for network information security. Although the law does not provide detailed explanations for some rules, its introduction fills significant gaps in data regulation and anticipates future developments in data, offering ample space for legal evolution. It provides legal support for protecting national sovereignty, security, and development interests, ensuring data security, and fostering the healthy development of the data economy.

Compared to the *Data Security Law*, the *Personal Information Protection Law* has more rules and a more comprehensive institutional design. This law deepens the protection of personal information rights, responding to the provisions on personal information protection set out in the *Civil Code*, and further clarifying those provisions. As China's first dedicated law on personal information protection, it integrates relevant regulations from the *Civil Code*, the *Consumer Rights Protection Law*, and the Cybersecurity *Law* regarding the definition of personal information, processing rules, and cybersecurity obligations of personal information processors. It provides general provisions on processing rules, individual rights, obligations of personal information processors, supervisory departments, and legal responsibilities. It specifically emphasizes obligations for protecting information on large internet platforms, stringent requirements for cross-border transfer of personal information, prohibition of excessive data collection by apps, and the illegal trade of personal information. This law lays the foundation for China's approach to personal information protection and establishes basic rules in this field.

In summary, China has comprehensive legal provisions regarding the classification, collection, and trade of data, which help curb external forces from stealing Chinese data and threatening national security, as well as preventing the illegal trade of personal information that infringes on individual rights and privacy. However, China's regulations on the application of artificial intelligence and AI-based deepfake technologies are relatively lacking. This deficiency can be attributed to two main factors: first, AI is a relatively advanced and novel technology with less direct impact on social life, and second, AI companies like OpenAI, which developed GPT, do not offer services in mainland China, thereby limiting the technology's influence on Chinese society. This represents a gap in China's information security and data security legislation compared to the West and indicates possible reasons for this issue.

5. Strategies and Recommendations

5.1. Strengthening Legal and Regulatory Frameworks

Based on the analysis of China's existing laws concerning big data and artificial intelligence, there is an urgent need to enhance the forward-thinking nature of relevant legislation. The governance of cyber cultural security should be more intelligent and digitized to meet the demands of the times and to reflect current trends and directions. First, legislation specifically targeting AI-driven deepfake technologies should be improved, with an emphasis on advancing criminal legislation to hold deepfake content creators legally accountable. Additionally, ethical and disciplinary constraints on government officials should be strengthened to prevent malicious exploitation. Second, there should be an accelerated effort to formulate laws and regulations governing cross-border data flows, covering all aspects of data transactions. This includes clearly defining approval and regulatory measures for data exiting the country to strengthen the protection of China's data and information security.

5.2. Establishing and Improving Regulatory Mechanisms

The effective implementation of cyber cultural security laws and regulations is key to the governance of cyber cultural security. Administrative bodies, as the primary enforcers of laws and regulations, play a role closely related to network users. The government should enhance oversight and strengthen collaboration among various departments, judicial bodies, and society at large. Local government departments should actively promote lawful administration, ensuring that administrative agencies enforce the law in a strict, standardized, impartial, and civilized manner, thereby improving the level of enforcement in the field of cyber cultural security.

To combat AI-based deepfakes, international cooperation must first be established, drawing on the successful experiences of other countries. In today's rapidly advancing world of technological innovation, which drives progress globally, building a community with a shared future for mankind requires cooperation among nations. The development of advanced technologies like AI should involve comprehensive exchanges and collaboration focused on national and societal development. AI is crucial to the future development of nations but also provides the foundation for deepfake technologies, which pose significant threats and challenges to national security. Therefore, international exchange and cooperation in this area are urgently needed. Second, governments should actively support efforts to combat deepfake activities, place importance on AI development, and bring together law enforcement and scientific research personnel to intensify the development of detection tools and technologies. Third, the government should encourage technological innovation, integrating innovation into research and development to drive advances in early warning and monitoring technologies, and continuously improve the ability to respond to and combat non-traditional national security threats.

5.3. Enhancing Cybersecurity Awareness

Comprehensive governance of cyber cultural security cannot be achieved without the involvement of the broad base of internet users. Netizens are the most fundamental and direct participants in maintaining cyber cultural security. Only by genuinely enhancing and strengthening the legal awareness of internet users and promoting the spirit of the rule of law can the level of rule of law in cyberspace be improved. This will strengthen the state's ability to manage the real-world applications of big data and AI. Meanwhile, mainstream media should leverage its vast influence to disseminate positive energy within cyberspace, thereby increasing users' awareness of adhering to, obeying, and using the law. This will guide them to consciously resist illegal online activities and uphold the authority and integrity of the rule of law. Cybersecurity and cultural departments should intensify efforts in legal education, using events like Internet Day to guide and educate users properly. These efforts should deepen public understanding of data security and information security, helping individuals learn to seek legal recourse when their rights are violated and fostering a positive legal environment.

6. Conclusion

This paper summarizes the challenges that big data and AI technologies may pose to data security and information security, and it compares and analyzes the legislative approaches taken by China and the West regarding these technologies. It then offers specific strategies and recommendations from three perspectives: strengthening legal and regulatory frameworks, establishing and improving regulatory mechanisms, and enhancing cybersecurity awareness. The significance of this research lies in providing strategic recommendations to government decision-making bodies, legislative institutions, judicial bodies, and other relevant departments, thereby promoting the continuous improvement and development of the national security legal system, balancing national security with citizen rights, and fostering social stability and sustainable development. Furthermore, this research also contributes to the healthy development of big data and AI technologies in the field of national security, facilitating the organic integration of technological innovation and legal protection. Future

research will need to focus on how to effectively implement these strategies to ensure the healthy, secure, and sustainable development of big data and AI technologies.

References

[1] Yuan Yin-chuan, Wang Xing-yue. Basic Connotation, Basic Requirements, and Realization Path of the Overall National Security Concept [J]. Research on Ideological Education, 2023, (04): 3-9.

[2] Dai Chang-zheng. Responding to New Era National Security Challenges Guided by the Overall National Security Concept [J]. People's Forum·Academic Frontier, 2023, (20): 22-31.

[3] Xiong Guang-qing, Zhang Su-min. Improving China's Data Security Management System from the Perspective of the Overall National Security Concept [J]. Journal of Harbin Institute of Technology (Social Science Edition), 2023, 25 (05): 32-40.

[4] Ma Fang. Systematically Constructing the National Security Law Implementation System [J]. Theoretical Exploration, 2022, (01): 12-22.

[5] Li Tian-ying, Zhao Ya-fang, Zhu Meng-di, et al. Legal Protection of Cyber Culture Security in China from the Perspective of the Overall National Security Concept [J]. Legal Expo, 2023, (32): 18-20.

[6] Wang Xi-mei, Ding Fu-jia. Interpretation of the Personal Information Protection Law in the Era of Big Data [J]. Journal of Jiaozuo University, 2023, 37 (02): 12-16.

[7] Guo En-ze. Response Path to the National Security Threats Posed by Deepfake under the Overall National Security Concept [C] // Collected Papers on National Security Work—Volume 3 of "Practical Law", 2023: 29-35.