International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 4, Jul-Aug 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Study on Legal Regulation of Artificial Intelligence under a Holistic Approach to National Security

Zhang Qi, Li Junhuan, Abi Nuer, Cai Xinying, Zhou Yingting

Beijing Wuzi University, Beijing, China

ABSTRACT

The development of artificial intelligence (AI) technology poses challenges to national political security, data sovereignty, and social stability. This study, grounded in a holistic approach to national security, analyzes the risks of AI in areas such as data breaches and algorithmic bias. By comparing the EU's Artificial Intelligence Act, the U.S. AI Bill of Rights, and China's existing legal regulations, the paper proposes a trinity regulatory framework of "risk classification-a balance of rigidity and flexibility-domain-specific governance." This includes a dynamic evaluation model for risk classification, a balanced approach combining algorithm registration and sandbox regulation, and differentiated strategies for domain-specific governance. This framework provides a core pathway for China's AI legal governance and contributes Chinese wisdom to global governance.

KEYWORDS: *A holistic approach to national security; AI regulation; Risk classification; Data dominance.*

How to cite this paper: Zhang Qi | Li Junhuan | Abi Nuer | Cai Xinying | Zhou Yingting "A Study on Legal Regulation of Artificial Intelligence under a Holistic Approach to National Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-4, August 2025, pp.919-923, URL: www.ijtsrd.com/papers/ijtsrd97340.pdf

IJTSRD97340

INTRODUCTION

Under the iteration of AI technology, the adaptability of security and regulation is facing new challenges. Generative AI, represented by the explosive growth of ChatGPT, brings three major security challenges: First, data risks, as large model training relies on cross-border data flows, which exacerbates the leakage of sensitive information, such as the tampering of personal data[1]; second, political risks, where deepfake technology generates false political discourse and disrupts the order of public opinion; and third, governance risks, as algorithms penetrate national governance systems and become a core issue of technological security.[2]

China has proposed a strategy that "balances development and security." However, laws such as the Cybersecurity Law and the Data Security Law show a lag in regulating AI risks and struggle to balance algorithmic supervision with data development and utilization[3]. There is an urgent need to build a governance system that is compatible with these challenges.

In terms of theoretical significance, the study of the legal regulation of AI under a holistic approach to national security can enrich the connotation of AI governance within this framework and promote interdisciplinary integration of law and computer science.

In terms of practical significance, the study of the legal regulation of AI under a holistic approach to national security can fill the legislative gap in AI regulation, provide a basis for government regulatory decision-making, and promote the integration of data security into the entire process to guide enterprises to comply with regulations in research and development.

Multidimensional Risk Analysis of Artificial Intelligence to National Security

Artificial intelligence technology possesses a dual nature: while it can empower national security, it also introduces systemic risks. External forces may exploit AI to interfere in politics, erode data sovereignty, and undermine social stability, posing potential threats to the long-term stability of the nation.

A. National Political Security

In the context of global competition, AI may intensify technological monopolies and data rivalries, leading to imbalanced competition among nations. At the same time, cybersecurity becomes increasingly vulnerable to cybercrime, as technological loopholes may be exploited, thereby threatening information sovereignty. Moreover, AI could impact political fairness, bringing multiple challenges to the overall security of the state.

1. Risks of Technological Monopoly and Gaps

Developed countries dominate the core technologies and standards of AI, such as chips and algorithms, forming a “technological power” barrier. There have been incidents in China where imported equipment was found to contain spying chips, leading to the leakage of national defense parameters [3]. The widening technological gap continuously marginalizes developing countries in the global division of labor, threatening their technological sovereignty and strategic autonomy [1].

2. Ethical and Legal Risks

First, ethical risks arise when data bias leads to algorithmic decisions that violate human ethics, such as racial discrimination. Generative AI may also be maliciously used to produce attack code or spread disinformation. Second, there exists a legal vacuum: current laws struggle to define liability in AI-related infringements, such as accountability in autonomous driving accidents. The lag in legislation results in regulatory failure, exacerbating disorder in the market [4].

B. Data Sovereignty

1. Data Security and Privacy Risks

Frequent cases of corporate sensitive data leakage via tools like ChatGPT [5] highlight the regulatory loopholes in cross-border data flows. The “Cambridge Analytica” scandal, a tool for political manipulation, has proven that big data profiling and algorithmic recommendations can precisely interfere with elections [7], turning politics into “computational politics.”

2. Data Weaponization

Artificial intelligence can accelerate the weaponization of data. For example, by targeting vulnerable social groups and precisely disseminating false information or inflammatory content, it can trigger social unrest [8]. In addition, terrorist organizations and individuals use generative AI to create violent and terrorist materials and write attack programs.

C. Social Order Stability

Artificial intelligence technology is developing rapidly. It has become more than just a tool; it is a powerful force that is profoundly changing society. It can determine who has a job, what information is spread, and even influence political choices. While this transformation brings efficiency gains, it also carries hidden risks of disrupting the existing social order.

1. Job Replacement

Artificial intelligence is mainly applied to jobs with high repetitiveness and a high degree of standardization [4]. This has led to the replacement of many traditional job positions. According to a report from the International Monetary Fund, nearly 40% of the global workforce is at risk of being replaced by AI. The replacement of job positions by AI may lead to waves of unemployment, which can easily widen the wealth gap and increase social security risks [7].

2. Loss of Technological Control

In some critical areas, such as transportation, energy, and finance, failures of artificial intelligence systems can cause severe social disruption and economic losses. For example, in 2018, an Uber self-driving car struck and killed a pedestrian in the early morning. The cause was that the Uber system misidentified the pedestrian as a floating object like a plastic bag, leading to a failure to brake in time [8].

International Experience in AI Legal Regulation and Its Implications for China

A. The Logic Behind the EU Artificial Intelligence Act’s Risk Classification

According to the composite function of “hazard probability × consequence severity” (Article 3 of the Act), the following risk levels are classified: First are unacceptable risks, such as social scoring systems. Next are high-risk systems, which include applications in critical sectors such as healthcare and the judiciary. Then come limited or minimal-risk systems, which are subject to mandatory transparency obligations. Finally, systemic risks, which are used to separately classify risks arising from specific technological characteristics [10].

1. Mandatory Registration for High-Risk AI

The EU Artificial Intelligence Act defines high-risk AI systems in two categories: The first includes AI systems used in critical sectors, such as education, employment, judiciary, public safety, healthcare, transportation, and energy. The second covers systems with specific technical characteristics, including biometric identification, critical infrastructure management, and law enforcement applications. These high-risk AI systems are mandated to submit full life-cycle technical documentation and are subject to compulsory data traceability requirements [11].

2. Insights from Full Life-Cycle Regulation of Foundation Models

Full life-cycle regulation means supervising every stage of an AI system, from research and development to decommissioning. The EU Artificial Intelligence Act takes a forward-looking approach by shifting regulation from “post-incident accountability” to “pre-incident prevention," ensuring the reliability of AI systems from the very beginning [9].

Drawing from the EU's experience, a regulatory direction suitable for China can be outlined: placing "pre-incident prevention" at the core and building a regulatory chain covering the entire lifecycle from R&D to decommissioning, ensuring that full life-cycle regulation has a legal basis.

B. The Flexible Regulatory Path of the U.S. AI Bill of Rights

1. Sandbox Pilot Mechanism

The concept of the "sandbox" originates from the field of computer science and essentially refers to a security isolation mechanism. It creates an independent operating environment for untrusted programs, strictly limiting access to resources and achieving physical separation from real systems. In security testing scenarios, this mechanism effectively intercepts potential risk programs, preventing them from causing damage to the actual system.

Currently, the United States does not have a unified, nationwide AI sandbox system. Instead, it adopts a regulatory model based on a division of responsibilities between the federal and state governments. This means that individual states can establish domain-specific initiatives. For instance, in the field of healthcare, Utah's Medical AI Lab allows limited trial-and-error for algorithms managing chronic diseases. It requires the disclosure of data and algorithmic explanations to reduce compliance costs while enabling real-time, dynamic risk monitoring.[14]

2. A Combined Model of Ethical Review and Industry Self-Regulation

The U.S. Blueprint for an AI Bill of Rights is built on five core principles, prioritizing fairness and privacy protection to guard against the misuse of AI systems. Among these principles, "algorithmic discrimination protection" and "explainability of decisions" are directly tied to ethical review. [13]

For example, experts have been invited to simulate attacks on GPT-4 to identify potential loopholes. Another example includes the requirement for municipal AI tools to disclose their logic and undergo ethical review.

C. Localization Adaptation in China

China's AI governance prioritizes data sovereignty at its core and builds a three-dimensional regulatory system:

First, in the dimension of data sovereignty, legislation ensures the localized storage of core data and strictly restricts the cross-border transfer of sensitive data. Second, in the dimension of risk warning, a tiered response mechanism is established, namely "national security-level risk-high-risk industries -low-risk livelihood sectors." Third, in the dimension of technological autonomy, efforts focus on breakthroughs in "bottleneck" technologies such as chips and algorithms, aiming to reduce foreign dependency [12].

Under the concept of "proactive risk precautionism," China can integrate the advantages of the EU tiered regulation and the U.S. flexible governance. On the rigid level, algorithm registration and ethical review are enforced in key AI sectors. On the flexible level, sandboxes are set up in critical areas (e.g., smart governance) to allow for controlled trial-and-error. At the international coordination level, China promotes alignment of cross-border data flow rules and exports its approach characterized by a "bottom-line mindset + inclusive innovation."

Building a Regulatory System under a Holistic Approach to National Security

A. Tiered Risk Regulation Framework

Based on a holistic approach to national security, building a scientific and efficient AI regulatory system hinges on implementing a risk-based tiered regulatory framework with targeted and precise measures.

1. Three-tier Risk Classification and Dynamic Assessment

A three-tier dynamic assessment system is established, namely "national security-level risk-high-risk industries-low-risk livelihood sectors." National security-level risk: This includes military systems and critical infrastructure. Mandatory security reviews, domestication of core code, real-time monitoring, and strict data localization are required. [17]

Second, for high-risk industries: This includes medical diagnosis [15] and financial risk control. [16] Algorithm registration, ethical review, third-party auditing, and major accident traceability are conducted.

Third, for low-risk livelihood level: This includes smart home systems and entertainment recommendations. It ensures users' right to be informed and to choose, and complies with baseline regulations such as the Personal Information Protection Law.

2. Embedding the Cybersecurity Review Measures in the Full-Lifecycle Algorithm Management

Risk-based tiered regulation is not a static label; it must permeate the entire lifecycle of algorithms, namely "design-development-training-deployment-operation - decommissioning," and be deeply integrated with the national cybersecurity review mechanism. Initiate security pre-assessments during the design phase, implement dynamic monitoring and threshold-based early warning after deployment, and conduct root cause analysis and algorithm iteration in the post-incident phase. Meanwhile, risks such as cross-border data transfers and supply chain security should be included as mandatory check items.

B. Regulatory Innovation through a Balance of Rigidity and Flexibility

Based on a risk-tiered framework, it is necessary to innovate a combination of regulatory tools that both establish clear and non-negotiable hard boundaries to safeguard security and ethics, and provide flexible space to encourage innovation, promote technological advancement and beneficial use, thereby achieving a dynamic balance between development and security.

1. Reinforcing Rigid Bottom Line: Legalizing Core Safeguard Mechanisms

AI systems at the national security level or classified as high-risk are required to submit core information such as basic principles and data sources to ensure the legal formalization of algorithm registration. Ethical reviews are mandatory, particularly for AI used in sensitive sectors like healthcare and justice. These systems must undergo assessments for fairness and explainability [18], with legal responsibilities clearly defined for developers, operators, and other key stakeholders.

2. Expanding Flexible Space: Empowering Innovation through Sandbox Mechanisms

Pilot programs for AI sandboxes in public governance allow smart government applications to be tested in controlled scenarios. For example, Shenzhen's exploration of "sandbox regulation" [19] tolerates non-critical and correctable deviations by designing fault-tolerant boundaries. In sectors such as healthcare and finance, co-governed sandboxes between "regulation and industries" are being established to promote collaborative industry-wide implementation.

3. Enhancing Legal Alignment: Building a Collaborative Governance Network

Introduce the Artificial Intelligence Promotion Law to establish core mechanisms such as risk classification and registration, ensuring alignment with existing laws. Integrate it with the Cybersecurity Law to clarify obligations related to algorithm security, and coordinate with sector-specific regulations such as the Regulations on Medical Devices to refine technical standards. This will help build a trinity governance model and form a coordinated system of "law-regulation-standard.[20]

C. Domain-Specific Precision Governance Mechanism

1. Infrastructure Layer: Strengthening Legal Safeguards for Core Data Localization Storage

Legislation should clearly stipulate the requirements for the localization of core data storage and severely punish violations that lead to data leaks. Security guidelines should be detailed for the entire data lifecycle, including acquisition, processing, storage, and output [21]. Legal gaps related to generative AI must be addressed dynamically.[22]

2. Industry Application Layer: Implementing Differentiated Risk Regulation Strategies

Taking the healthcare and education sectors as examples: In healthcare, mandatory double-blind testing should be enforced to ensure patient safety and privacy. In education, laws should restrict AI from replacing core teaching functions to prevent misuse of educational data and the weakening of students' creativity. [23]

3. International Coordination Layer: Aligning Cross-Border Data Flow Rules with Global Standards

A legal risk control system should be established for the entire process of cross-border data flow. This includes ex-ante legal framework design, dynamic regulation of cross-jurisdictional risks during implementation, and post-incident judicial accountability and redress mechanisms [24]. The cross-border transfer of confidential data must be strictly regulated to balance security with international collaboration

Conclusion

By conducting an in-depth study of the field of AI legal regulation related to previous documents such as the EU Artificial Intelligence Act and the U.S. AI Bill of Rights, this paper employs comparative research and questionnaire survey methods to conduct a profound analysis of the national security risks associated with AI. Faced with severe challenges such as technological monopolies, erosion of data sovereignty, and social disorder, the secure development of AI technology is significantly constrained. Therefore, to promote the improvement of the AI governance system, it is particularly urgent to establish and refine a trinity regulatory platform, namely "risk classification -a balance of rigidity and flexibility-domain-specific governance."

In response to the above-mentioned challenges, a holistic approach to national security should be integrated with dynamic tiered regulatory technology. By employing a combination of rigid registration and review mechanisms and flexible sandbox pilots, it is possible to coordinate the interconnectivity between security baselines and innovation space. A comprehensive assessment of its impact on political security, data sovereignty, and social stability should be conducted to provide solutions for building an AI governance system with Chinese characteristics and to promote the robust development of global AI governance.

References

[1] Xu Yi. Personal Data Security Risks and Legal Regulation Paths in the Application of Generative Artificial Intelligence [J]. Credit Reference, 2025, 43 (05): 9-16 +28.

[2] Wang Han, Zhang Longhui. The "Function-Structure" Disturbance of Algorithms to

National Security and Countermeasures [J]. International Security Studies, 2025, 43 (03): 132-153 + 158.

[3] Deng Jinting. On the Internal Path of Legal Regulation of Artificial Intelligence [J]. Hebei Law Science, 2025, 43 (08): 100-121.

[4] Li Heng, Guo Zongkai. The Manifestation, Generation Reasons and Coping Strategies of Artificial Intelligence Security Risks in the Digital Age [J/OL]. Journal of Henan Police College, 1-22 [2025-07-17].

[5] Cai Huaitao. Multidimensional Challenges and Responses to Data Security of Generative Artificial Intelligence [J]. Jiangxi Social Sciences, 2025, 45 (06): 125 -134.

[6] Li Zhong. Risks and Challenges to Confidentiality Rule of Law in the Age of Artificial Intelligence and Coping Strategies [J]. Rule of Law Times, 2025, (04): 26-30.

[7] Wang Ming, Li Tao, Luo Qingping, et al. National Security in the Age of Artificial Intelligence [J]. Social Governance Review, 2025, (02): 4-15.

[8] Yang Xiaoguang, Chen Kaihua. Risks and Governance of Artificial Intelligence from the Perspective of National Security [J]. Governance, 2024, (13): 49-53.

[9] Xu Linfang. The EU Artificial Intelligence Act and Its Implications for China's AI Regulation: From the Perspective of Risk Classification and Multi-Stakeholder Collaboration [J]. Modern Marketing, 2025, (18): 72-74.

[10] Huang Haiying, Yang Xu. Interpretation of the EU Artificial Intelligence Regulatory System Based on the AI Act [J]. Library Development, 2025, (03): 12-24.

[11] Zhao Yong, Wang Zhongying. Core Regulatory Concepts and Implications of the EU Artificial Intelligence Act [J]. Cross-Strait Legal Science, 2025, 27(02): 22-35.

[12] Gao Zhihong. Response and Beyond: Legal Regulation of Generative Artificial Intelligence-From the Perspective of the Interim Measures for the Management of Generative AI Services [J]. Social Science Journal, 2024, (05): 121-130.

[13] Zhong Xinlong, Peng Lu. Comparative Study and Suggestions for Insights on AI Legislation in the U.S. and the EU [J]. Science and technology of China, 2023, (06): 32-35.

[14] Li Fangtian. Legal Research on the Sandbox Regulatory System [D]. Zhengzhou University, 2021.

[15] Liu Ying, Yin Wanyi, Yuan Qing, et al. Study on Tiered Regulation Based on the Potential Risks of Medical AI [J]. Journal of Community Medicine, 2025, 23(05): 141-145. DOI: 10.19790/j. cnki. JCM. 2025.05.01.

[16] Zi Weiyu, Shu Zhongping. Construction of an AI-Driven Financial Regulatory Early Warning Mechanism [J]. Encyclopedic Knowledge, 2025, (18): 65-67.

[17] Wu Shaolong. Building a Dimensional Governance System to Balance AI Regulation and Development [N]. Securities Times, 2025-06-16 (A01).

[18] Jiang Hui. On National Security Review of Generative Artificial Intelligence Applications [J]. Social Sciences in Yunnan, 2024, (04): 72-79.

[19] Xu Xuanhe, Liu Yueya, Tang Zizi, et al. Shenzhen to Explore "Sandbox Regulation" Mechanism in Fields such as AI [N]. Southern Daily, 2025-06-14 (004).

[20] Hong Yanqing. Data Scraping Governance in the AI Era: Legal Conflicts and the Way to Balance Interests [J]. Journal of Political Science and Law, 2025, (03): 105-122.

[21] Guo Ruyuan. Legal Risk Prevention in Generative AI Data Processing-From the Perspective of ChatGPT's Handling of Copyrighted and Non-Copyrighted Data [J/OL]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 1-17 [2025-07-18].

[22] Wang Haoquan. Coordinated Development of Data Security Risk Prevention Mechanisms and Legal Regulations in Generative Artificial Intelligence [J]. Industrial Innovation, 2025, (12): 28-30.

[23] Su Rui. Opportunities and Challenges for Talent Cultivation in Universities Amid the Generative AI Wave [J/OL]. Heilongjiang Education (Theory and Practice), 1-5 [2025-07-18].

[24] Rao Chuanping, Zheng Zeyu. On the Legal Governance of Cross-Border Data Security [J]. Journal of Nanjing University of Aeronautics and Astronautics (Social Science Edition), 2025, 27(04): 81-89.