Criminal Regulation of AI Crimes: The Application Dilemma and Path Optimization of the Crime of Assisting Information Network Criminal Activities

Jiaxin Shi
School of Foreign Languages and Literature, Wuhan University, Wuhan, China

Keywords: AI Crimes, Crime of Assisting Information Network Criminal Activities, Criminal Regulation.

Abstract: With the rapid development of artificial intelligence technology, its wide application in various fields of society not only promotes efficiency innovation but also provides technical tools for new types of crimes. Crime forms such as AI-driven automated fraud, deepfake, and data theft, with their concealment, high efficiency, and cross-domain nature, pose severe challenges to the traditional criminal law system. This pa-per focuses on Article 287(2) of the Criminal Law, "Crime of Assisting Information Network Criminal Activities", and explores its applicability in AI crimes. In judicial practice, this crime faces many dilem-mas. For example, the principle of technological neutrality makes the definition of criminal acts vague, the determination of subjective knowledge is difficult in the face of complex AI application scenarios, and the division of responsibilities is unclear when multiple parties are involved. This paper deeply ana-lyzes these core controversial issues and proposes suggestions for improving legal regulation and indus-try supervision, aiming to provide theoretical support for constructing a criminal governance framework adapted to the AI era.

1 INTRODUCTION

Driven by the digital wave, artificial intelligence (AI) technology has penetrated into all fields of social life, from medical diagnosis to financial transactions, from public opinion analysis to automated production. Its high efficiency and innovation have injected strong impetus into the development of human society. However, the "double-edged sword" effect of technology has also become apparent in this process. The algorithmic autonomy, data dependence, and technological generalization of AI are being used by criminals as new tools for committing crimes. Deepfake technology can generate lifelike audio and video, which can be used for slander, fraud, or interference in judicial activities. Automated algorithms push fraudulent information through precise profiling, causing the scale of victims to grow exponentially. Malicious programs, with the rapid iteration ability of AI, pose a systematic threat to the network security defense line. Such crimes not only violate personal privacy and property security but also impact the social trust foundation, disrupt the economic order, and even threaten national security. Facing this challenge, the traditional criminal law system is in a dilemma in terms of the identification of the subject of behavior, the proof of subjective intent, and the evaluation of technological neutrality, and urgently needs to explore regulatory paths that adapt to the characteristics of AI crimes.

Currently, domestic and foreign academic circles have initially explored the criminal regulation of AI crimes. Domestic research focuses on the applicable boundaries of specific crimes. For example, regarding the controversy over Article 287(2) of the Criminal Law, "Crime of Assisting Information Network Criminal Activities," scholars have analyzed the "knowledge" standard, the scope of assisting acts, and the severity of circumstances in its constitutive elements from the perspectives of norm theory and dogmatics（Zeng & Jin, 2024). Some viewpoints advocate narrowing the application scope of this crime to avoid over-generalization (Wu & Zhang, 2023). There are also studies that propose to solve the identification problems through the coordination of technical means and legal interpretation, combined with judicial practices such as the "Breaking the Card" operation (Wei & Sha, 2023).

In contrast, international research pays more attention to the global and technical characteristics of AI-driven crimes. Scholars such as Chanderprajapu point out that the existing international legal

Shi, J.
Criminal Regulation of AI Crimes: The Application Dilemma and Path Optimization of the Crime of Assisting Information Network Criminal Activities.
DOI: 10.5220/0014293300004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 27-32
ISBN: 978-989-758-785-6

framework has problems of ambiguous jurisdiction and broken evidence chains in dealing with AI-driven-cyber-crimes. The United Nations and Interpol call for strengthening governance through transnational cooperation and the unification of technical standards. However, existing research mostly focuses on a single legal provision or technical scenario, lacks a systematic response to core controversial issues such as the liability determination of "technology providers" in AI crimes and the nature definition of algorithmic recommendation behavior, and has not formed a regulatory system that takes into account both technological development and risk prevention and control.

This paper takes Article 287(2) of the Criminal Law, "Crime of Assisting Information Network Criminal Activities," as the starting point to deeply explore its application dilemma and optimization path in AI crimes. First, the article sorts out the typical types of AI crimes (such as automated fraud, data theft, and deepfake) and their multi-dimensional harms to social governance, revealing the shortcomings of the traditional criminal law in dealing with such crimes. Then, from the perspective of legal hermeneutics, it analyzes the constitutive elements of this crime, focusing on the determination standard of "subjective knowledge," the boundary division of technologically neutral behavior, and the impact of AI's autonomous decision-making on liability attribution. Finally, combined with technological characteristics and judicial practice, it proposes systematic suggestions such as clarifying the boundaries of responsible subjects, refining the rules for determining "knowledge," strengthening industry supervision, and formulating special judicial interpretations, aiming to provide theoretical support for constructing a criminal governance framework that is technically adaptable and has clear rights and responsibilities.

The full text is divided into five parts: The first part (Introduction) clarifies the necessity and innovation of the research through background analysis and literature review; the second part systematically summarizes the main types, technical characteristics, and harm evolution trends of AI crimes; the third part, based on legal texts and judicial interpretations, analyzes the constitutive elements and judicial identification difficulties of the "Crime of Assisting Information Network Criminal Activities"; the fourth part focuses on the application controversies of this crime in AI crimes, including the ambiguous liability of technology providers, the doubtful nature of algorithmic recommendation, and the impact of AI autonomy on subjective intent; the fifth part proposes improvement paths from the legislative, judicial, and industry supervision levels, emphasizing the realization of a balance between risk prevention and control and innovation protection through "technology - law" coordinated governance. This paper attempts to bridge the fragmented defects of existing research and provide reference for the scientific and refined criminal legislation in the AI era.

2 TYPES AND DEVELOPMENT TRENDS OF AI CRIMES

2.1 Typical Application Types

In current criminal activities, the application of AI is becoming more diverse and concealed. Typical examples of AI crimes include automated fraud, data theft crimes, and deepfake technology. Among them, automated fraud uses AI algorithms to accurately profile a large number of potential victims. According to factors such as different people's psychological characteristics and consumption habits, personalized fraud scripts are customized and widely spread through channels such as text messages, phone calls, and online advertisements. In data theft crimes, AI technology can quickly analyze the vulnerabilities of network systems and automatically capture massive amounts of personal information and business - confidential data, providing data support for subsequent illegal transactions or criminal activities. Deepfake technology creates false content that is enough to be confused with the real by deeply learning a large number of image, audio, and video materials, which is used for illegal and criminal acts such as slandering others, creating social panic, or interfering with judicial procedures.

2.2 Impact on Social Harmfulness

The social harmfulness of AI crimes cannot be underestimated, which is mainly reflected in the economic level, social order level, and national security level. From an economic perspective, automated fraud and data theft directly lead to a large amount of property losses. Enterprises may face problems such as damage to business reputation and economic compensation due to data leakage, which in turn affects the stable development of the industry. In terms of social order, the false information of

deepfake is extremely likely to cause public panic, disrupt the normal social public opinion environment, mislead public perception, and may even trigger mass incidents. In addition, AI crimes also pose a serious threat to national information security. The leakage of sensitive data may be used for espionage activities, cyber - attacks, etc., damaging national interests and international image.

3 LEGAL ANALYSIS OF THE CRIME OF ASSISTING INFORMATION NETWORK CRIMINAL ACTIVITIES

3.1 Analysis of Constitutive Elements

According to Article 287(2) of the Criminal Law and relevant judicial interpretations, from the perspective of the four constitutive elements, the constitutive elements of the crime of assisting information network criminal activities include the subject, subjective aspect, object, and objective aspect. The subject is a general subject, including natural persons and units. The subjective aspect requires that the actor knows that others are using the information network to commit crimes and still provides technical support, advertising promotion, payment settlement, and other assisting acts. The object is a complex object, which not only violates the management order of information network security but also infringes the legitimate rights and interests of citizens, legal persons, and other organizations. The objective aspect is manifested as providing assistance for information network crimes and reaching the level of serious circumstances.

3.2 Discussion on Key Identification Standards

The determination of the "knowledge" standard is the key to the application of this crime. As the legal proverb goes, a single piece of evidence cannot establish a fact. In practice, it cannot be judged only based on the actor's own confession. Factors such as the actor's cognitive ability, the channels of accessing information, and the abnormality of the behavior need to be comprehensively considered. Regarding the scope of "assisting acts," with the development of network technology, it not only includes traditional technical support, payment settlement, and other acts but also covers new network services such as cloud computing services and algorithmic recommendation services. The definition of "serious circumstances" needs to be judged by combining multiple factors such as the number of assisting acts, the duration, and the resulting harm consequences.

4 APPLICATION DILEMMA OF THE CRIME OF ASSISTING INFORMATION NETWORK CRIMINAL ACTIVITIES IN AI CRIMES

4.1 Liability Determination of AI Tool Providers

In AI crimes, there is a controversy over whether AI tool providers constitute "assistants." Regarding whether AI tool providers constitute "assistants," there is a controversy in the academic community. Some scholars believe that the behavior of AI tool providers is essentially a neutral technical behavior and should not be directly regarded as an assisting act (Yuan & Xue, 2024). For example, the provider of a generative AI tool may only provide a technical platform and cannot foresee the specific criminal acts for which its tool is used. Some AI tools are universal, and it is difficult for the provider to know the specific uses of the users (Jiang & Liu, 2024).

If all tool providers are identified as accessory offenders, it may limit the normal development of AI technology; but if not regulated, a large number of tools may be used for criminal activities.

4.2 Industry Supervision Failure

In the author's opinion, the problem of industry supervision failure can be mainly manifested in the following three aspects.

First, inequality between supervision responsibilities and powers. Currently, private enterprises assume a large number of obligations in network space supervision but lack corresponding power support. For example, laws such as the Anti-telecommunications Fraud Law of the People's Republic of China clearly define the responsible subjects of new business fraud-related risk safety assessment, risk prevention and control, internal control mechanisms, and security responsibility systems as telecommunications business operators,

banking financial institutions, Internet service providers, etc. However, these enterprises do not have the power to independently decide to restrict, close, prohibit, or freeze the network activities of others. Their supervision responsibility is more of an obligation to the main body of network activities rather than real power. This inequality between responsibility and power makes it difficult for enterprises to fulfill their supervision obligations and also increases their risk of being held criminally liable for insufficient supervision.

Second, mismatch between technological development and supervision capabilities. The government lags behind in the research and development and application of network governance technologies and is difficult to effectively respond to the rapidly developing information technology and AI technology. Although the government is nominally the responsible subject of network governance, it lacks the actual ability to lead the development of network governance technologies. This mismatch between technological development and supervision capabilities leads to the over-reliance on the role of criminal law in governing network crimes and increases the risk of criminal law being abused.

Third, incompleteness of industry supervision standards. Currently, there are still deficiencies in the industry supervision standards for AI technology. For example, although the Interim Measures for the Administration of Generative AI Services put forward compliance supervision requirements for the generative AI-related industries, these requirements mainly focus on the technical level, such as adding a differentiation mark to the generated images or videos and standardizing the data collection behavior of personal information. However, there is still a lack of clear legal guidance on how to determine the "knowledge" of platform or technical service providers when they know that the other party is using their technology for criminal activities and how to assume criminal liability.

4.3 Impact of AI System's Autonomous Decision-Making on "Subjective Knowledge"

The autonomous decision-making ability of an AI system may affect the determination of its "knowledge" state. If an AI system can independently judge and choose criminal acts, it may be determined to have "knowledge." However, if the decision-making of an AI system is completely based on preset algorithms and data and does not show subjective intent, it is difficult to determine that it has "knowledge." The autonomous decision - making process of an AI system is often highly complex and unexplainable, especially for AI systems based on deep learning and large models, whose internal algorithms and decision-making mechanisms are regarded as "black boxes." This unexplainability poses a huge challenge in judging whether the actor "knows" that his behavior may lead to criminal results. For example, in AI-assisted financial fraud or cyber - crimes, even if the actor uses an AI tool, it is difficult to prove his subjective knowledge of the criminal results through traditional methods.

5 SUGGESTIONS FOR IMPROVING THE CRIMINAL REGULATION OF AI CRIMES

5.1 Clarify the Liability Boundaries of AI Tool Providers

The complexity and technical dependence of AI crimes require clear definition of the liability boundaries of AI tool providers and the realization of operability in liability determination through technological transparency. On the one hand, it is necessary to clearly divide the liability levels of different subjects. The development, deployment, and application of AI technology involve multiple parties. Developers, manufacturers, and users may jointly cause criminal consequences due to technical defects or abuse. For example, if a developer deliberately reserves data-stealing loopholes in the design of an algorithm or knows that the technology may be used for illegal purposes but does not set up a risk - blocking mechanism, he should bear the main criminal liability; if the manufacturer fails to fulfill the quality review obligation for AI products with potential safety hazards, it should bear joint liability; and when the user maliciously uses the technology to commit a crime, he should bear independent liability. By distinguishing the degree of fault and the nature of the behavior of each subject in the technology chain, it can avoid the suppression of technological innovation by "one-size-fits - all" imputation and accurately combat the source of crimes. On the other hand, it is necessary to strengthen the requirements for algorithm transparency and interpretability. Currently, due to the "black-box" characteristics of

some AI systems, their decision - making logic is difficult to trace, and developers often shirk their responsibilities on the grounds of technological neutrality. In this regard, legislation should be used to force high-risk AI tools (such as deepfake programs, automated recommendation systems) to disclose the core algorithm framework and embed an interpretability module. For example, attach a "technical path description" to the output of generative AI, recording the data source and decision-making basis; introduce a third-party audit mechanism in the algorithm training stage to ensure that the development process complies with ethical norms. Only by breaking through the technical barriers can objective bases be provided for the determination of "subjective knowledge" and "assisting acts" in judicial practice and the balance between the principle of technological neutrality and the principle of liability adaptation be achieved.

5.2 Strengthen Industry Supervision

The rapid iteration and wide application of AI technology require that industry supervision must shift from passive response to active prevention and control. To achieve this goal, it is necessary to build a trinity supervision framework of "legal norms-enterprise self-discipline-technical support" and form a risk prevention and control system covering the entire life cycle of AI through multi-level system design, criminal compliance incentives, and the coordination of technology and law.

First, establish a multi-level three-dimensional supervision system to achieve comprehensive coverage from legislation to practice. At the legislative level, special laws such as the AI Law should be accelerated. The bottom-line requirements for technology research and development, data use, and product deployment should be clarified. For example, it should be stipulated that the design of AI tools must embed an ethical review mechanism, and the development of algorithm models with obvious criminal orientation should be prohibited. At the same time, industry access standards should be refined through administrative regulations, and enterprises should be required to complete safety assessment and filing before entering the market to ensure the legality of technology application. At the administrative supervision level, it is necessary to strengthen the cross-departmental cooperation mechanism. For example, the Internet Information Office, the public security organ, and the science and technology management institution jointly establish an "AI Safety Supervision Committee" to regularly conduct special inspections on high - risk areas (such as deepfake, automated recommendation systems) and impose dynamic penalties on illegal enterprises. Technical supervision needs to rely on third - party testing institutions to conduct transparent reviews of the operation logic and output results of AI systems through technical means such as algorithm auditing and data traceability to avoid supervision blind spots caused by "black-box operations."

Second, promote the corporate criminal compliance plan and internalize risk prevention and control into the conscious actions of industry development. The practical experience of the EU's AI Liability Directive can be borrowed to require AI enterprises to establish a compliance management system including risk identification, internal control, and emergency response. For example, when an enterprise develops a face recognition system, it needs to pre-evaluate the risk that it may be used for illegal monitoring or identity theft and embed a "usage scenario restriction" function in the algorithm; in the data collection link, user explicit consent and anonymization processing should be adopted to avoid privacy violations. For enterprises that actively fulfill compliance obligations, policy incentives such as tax reduction and priority in market access can be given; conversely, for enterprises that allow the abuse of technology, administrative penalty intensity should be increased, and even the criminal liability of relevant responsible persons should be investigated. In addition, industry associations should take the lead in formulating the AI Ethical Guidelines to guide enterprises to integrate the concept of "technology for good" into the entire product process. For example, generative AI tools are required to mark "deepfake risk warnings" to reduce the possibility of technology abuse from the source.

Third, strengthen the in-depth integration of technology and law to improve the accuracy and efficiency of judicial governance. On the one hand, it is necessary to improve the cognitive level of judicial personnel on AI technology through professional training and interdisciplinary cooperation. For example, when hearing cases involving algorithmic recommendation, judges should master basic machine learning principles and be able to distinguish between "technically neutral push" and "malicious inducement behavior"; when determining "subjective knowledge," technical experts can be used to analyze system logs and algorithm parameters to judge

whether the developer has criminal intent. On the other hand, the auxiliary application of AI technology in judicial practice should be explored. For example, natural language processing technology can be used to analyze a large number of judgment documents to extract the judgment rules of the "Crime of Assisting Information Network Criminal.

6 CONCLUSION

The rapid advancement of artificial intelligence (AI) technology has brought unprecedented opportunities and challenges to society. While AI continues to drive innovation and efficiency, its misuse in criminal activities has posed significant threats to personal privacy, economic stability, social order, and national security. This paper has explored the application dilemmas and optimization paths of Article 287(2) of the Criminal Law, "Crime of Assisting Information Network Criminal Activities," in the context of AI crimes.

Through an analysis of typical AI crime types, such as automated fraud, data theft, and deepfake technology, the paper highlights the multidimensional harms of AI crimes and the shortcomings of traditional criminal law in addressing these challenges. It further examines the key issues in the application of Article 287(2), including the determination of subjective knowledge, the boundary of technologically neutral behavior, and the impact of AI autonomy on liability attribution.

The paper argues that the complexity and technical nature of AI crimes necessitate a balanced approach to criminal regulation, emphasizing both risk prevention and innovation protection. To achieve this, the paper proposes several recommendations: clarifying the liability boundaries of AI tool providers, strengthening industry supervision through a "law-technology" coordinated governance framework, and enhancing the transparency and interpretability of algorithms. These measures aim to address the challenges posed by AI crimes while fostering the responsible development of AI technology.

In conclusion, this paper provides a comprehensive framework for understanding and regulating AI crimes, offering theoretical support for the construction of a criminal governance framework adapted to the AI era. By addressing the core controversies and proposing practical solutions, the paper contributes to the ongoing discourse on AI governance and legal regulation.

REFERENCES

Jiang Luoyi, Liu Shude. 2024. Examination and Regulation of Judicial Reasoning on “Knowledge” in the Crime of Assisting Information Network Criminal Activities. *Research on the Modernization of Rule of Law*, 5:124-135.

Wei Hanxi, Sha Guijun. 2023. Practical Dilemmas and Countermeasures in the Judicial Application of the Crime of Assisting Information Network Criminal Activities. *Journal of the Criminal Investigation Police University of China* 6:57-65.

Wu Dianchao, Zhang Yu. 2023. Research on Several Issues in the Application of the Crime of Assisting Information Network Criminal Activities. *Journal of Henan Institute of Education (Philosophy and Social Sciences Edition)* 3:54-57.

Yuan Bin, Xue Liming. 2024. Research on the Criminal Law Regulation of Generative Artificial Intelligence. *Hebei Law Science* 2:140-159.

Zeng Lei, Jin Yuanyuan. 2024. The Normative Attributes and Interpretive Rectification of the Crime of Assisting Information Network Criminal Activities. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)* 3:52-61.

Zhang Mingkai. 2016. On the Crime of Helping Information Network Crime. *Political Science and Law* 2:2-16.

Pi Yong. 2018. On the Legislation of New Types of Cybercrime and Its Application. *Social Sciences in China* 10:126-150.

Liu Yanhong. 2016. A Critique of the Criminalization of Cybercrime Aiding Behaviors as Principal Offenses. *Law and Business Research* 3:18-22.

Li Hong. 2017. On the Nature and Application of the Crime of Assisting Information Network Criminal Activities. *Legal Application* 21:33-39.

Jiang Su. 2020. The Interpretive Direction of the Crime of Assisting Information Network Criminal Activities. *China Criminal Law Journal* 5:76-93.