Criminal Law Responses to Artificial Intelligence Fraud Crimes: Research on Practical Dilemmas and Regulatory Paths

Zhuoren Zhou
School of Law, Harbin University of Commerce, Harbin, Heilongjiang, China

Abstract: This paper focuses on the criminal law response to AI fraud crimes and systematically analyzes the theoretical and practical dilemmas in terms of the responsible party, behavior determination, subjective intent, causality, etc. The study points out that traditional criminal law has application difficulties in the face of problems such as multi-subject participation, behavioral independence and ambiguous intent brought about by AI technology. The article presents a "compromise" view, advocating the combination of technological governance and criminal law regulation to construct a four-in-one criminal law regulation path: improving criminal legislation, clarifying judicial responsibilities and evidence rules, promoting social co- governance, and using AI technology to combat fraud. The conclusion suggests that effective regulation of AI fraud should be achieved through the combined efforts of law, technology and social governance.

Keywords: AI Fraud; Criminal Law Doctrine; Responsibility Allocation; Criminal Law Regulation; Technological Countermeasure

1. Ask Questions

1.1 Research Background and Purpose

The rapid development of artificial intelligence technology is profoundly changing social production and lifestyle. While bringing technological dividends, it also provides new tools and means for criminals to commit crimes. AI fraud crimes are on the rise and have become an important challenge for the criminal justice system [1]. Such crimes rely on cutting-edge technologies such as deep learning, natural language processing, and image generation to make fraud more covert, intelligent, and capable of large-scale dissemination, seriously threatening citizens' property rights and social order.

When dealing with this new type of crime, the traditional criminal law system has exposed many theoretical and practical predicaments, such as the ambiguity of the subject of responsibility, the difficulty in determining subjective intent, and the breakage of causal relationships, which urgently need a systematic reconstruction from the perspective of criminal law doctrine. This study focuses on the criminal law application predicament of AI fraud crimes, clarifies the impact of technological intervention on the elements of traditional crimes, proposes operational regulatory paths, and promotes the adaptive adjustment and modernization transformation of China's criminal legal system in the era of artificial intelligence. By constructing a four-in-one regulatory framework of "legislation - judiciary - society - technology", it provides theoretical support and institutional recommendations for governing AI fraud crimes and enhances the capacity and effectiveness of criminal law in dealing with emerging technology crimes.

1.2 Research Significance and Current Status

Artificial intelligence fraud crimes have drawn attention from the criminal law theory and practice circles, and the academic circle has formed three theoretical positions. The positive regulation theory advocates expanding the scope of application of criminal law, strengthening the crackdown, emphasizing legislative foresight and judicial initiative, and advocating the addition of specific charges and the clarification of constitutive elements to curb new types of crimes [2]. This theory is prone to causing premature and excessive criminal intervention in practice, which affects the balance between technological innovation and social freedom.

The negative limitation theory advocates criminal law restraint, emphasizes formal rationality and procedural justice, holds that criminal law should not easily intervene in the field of technology, strictly adheres to the principle of legality of crimes and punishments,

and prevents excessive criminalization. This view emphasizes procedural passivity and the mechanism of conviction, and holds that conviction and punishment should only be imposed when the act fully meets the constitutive requirements of the current criminal law provisions [3]. Although it helps to safeguard human rights and judicial justice, it lags behind in the face of new criminal patterns brought about by technological development and is difficult to effectively deal with the complexity and concealment of AI fraud.

As Professor Wang Wenhua of Beijing Foreign Studies University argues in the Legal Daily, the technology governance theory, as a compromise position, advocates for a dynamic balanced regulatory system that combines technological means and legal norms, emphasizes the principle of technology neutrality, and suggests that the boundaries of technology use should be defined through legislation and substantive judgment mechanisms should be introduced into judicial practice. This paper advocates the adoption of this theory because it can both avoid the risk of criminal law expansion and effectively respond to the real challenges of AI fraud, achieving a positive interaction between criminal law modernization and social governance [4].

2. Core Analysis of AI Fraud Crimes

2.1 Essential Analysis of AI Fraud

2.1.1 Definition and classification of AI fraud

AI fraud refers to the fraudulent crime of illegally obtaining property or information by using deep learning, natural language processing and other means to generate false content. It relies on technology to break through the limitations of traditional fraud in terms of time, space and interpersonal interaction, and its methods are more covert and efficient [22].

AI scams are diverse in types. In terms of technical means, voice simulation fraud uses deep learning algorithms to model the target voiceprint and generate realistic voice; video scams use deepfake techniques to replace synthetic facial images and create fake videos; image generation scams use technologies such as generative adversarial networks to synthesize fake images to create false scenarios; text scams rely on natural language processing technology to generate false information to imitate scams. In terms of target and scope, targeted scams target specific individuals and use social data for precise modeling; non-targeted scams target a wide range of people and use platform algorithms to deliver content; mass scams use commercial packaging to cover up illegal purposes and induce irrational consumption or investment [23].

These types of AI scams have different technical implementation paths, but all have low technical thresholds, spread quickly and are difficult to identify, posing a serious challenge to the traditional criminal law system.

2.1.2 Technical characteristics of AI fraud

With the deep development of artificial intelligence technology, AI fraud crimes present significantly different technical features from the past, posing a challenge to the current criminal law system. The content generated by AI fraud is highly realistic. With the help of deep learning and other model technologies, it automatically generates realistic text, images, audio and video, etc., reducing the cost of false information production. The content is highly realistic, making it difficult for the general public to distinguish the true from the false, increasing the risk of fraud. Such as deepfake technology, which can simulate the characteristics of a specific person and create highly deceptive false information to carry out precise fraud [5]. This not only challenges the criteria for identifying "false information" and "deceptive means" in traditional criminal law, but also poses higher technical requirements for evidence collection and identification.

AI fraud dissemination methods are highly automated and intelligent, breaking through the limitations of traditional manual operations and presenting batch, immediate and cross-platform characteristics. Through machine learning algorithms, fraudsters can precisely screen the target audience, distribute fraud information on a large scale, and dynamically adjust the dissemination strategy based on user behavior data to increase reach and acceptance, making the dissemination path more complex and judicial authorities face difficulties in obtaining evidence and tracking [24].

2.2 Significance and Status of the Study

There are three main viewpoints in the academic community in the face of legal issues arising from the rapid development of artificial intelligence technology. The positive regulation theory advocates strengthening the regulatory function of criminal law, strictly controlling AI-

related criminal acts, emphasizing the role of criminal law in maintaining order, clarifying legal boundaries through legislation and ensuring social order through strict judicial application [6]. For instance, in new types of crimes such as AI fraud, there is a tendency to expand interpretations or add charges to prevent governance gaps caused by legal lag. The negative limitation theory emphasizes the restraint of criminal law, arguing that the law should not overly intervene in technological development, especially when the social impact of artificial intelligence is not fully manifested, to avoid premature criminal law intervention.

When there is a lack of clear harmful consequences or the boundaries of the act are ambiguous, the application of criminal law should be strictly limited. For example, in cases of AI-generated content fraud, if it is difficult to prove subjective intent or direct causality, caution is advocated for criminalization. Technology governance is a compromise, arguing that criminal law response strategies should be both forward- looking and flexible, legislation should respond to real needs, and the judiciary should introduce technology assessment and ethical considerations, such as supporting the establishment of a tiered accountability system in AI fraud regulation [7]. This article tends to adopt this position, arguing that the key lies in establishing an institutional framework that is both normative and adaptive.

3. Conflict and Reconstruction of the Core Elements of Criminal Law Doctrine

3.1 The Ambiguity of the Subject of Liability

3.1.1 Insufficient legal basis for liability attribution

The current criminal law faces the problem of insufficient legal basis for liability attribution when dealing with AI fraud crimes involving multiple parties. Traditional criminal law builds the liability system with natural persons as the main subjects, but AI fraud often involves multiple subjects such as developers, platform operators, users and algorithms, forming a complex liability network, and the logic of single- subject liability is difficult to apply, causing confusion in liability determination in judicial practice. For instance, AI algorithms' autonomous decisions may deviate from the intentions of developers or users, and the provisions of criminal law on joint crimes do not cover the particularity of technical subjects, resulting in a broken or mismatched chain of responsibility. AI technology is highly specialized and concealed. In scenarios where platform responsibility and user behavior are intertwined, criminal law lacks clear criteria for distinguishing between technical control and behavioral dominance, which increases the difficulty of identifying responsible subjects. This not only affects individual justice, but also weakens the deterrent and preventive effect of criminal law on AI fraud [8]. To address this, there is an urgent need to reconstruct the legal framework of liability attribution, incorporate the technical subjects, define the criminal liability boundaries of the subjects at each stage, and provide precise liability attribution paths for AI fraud crimes involving multiple subjects.

3.1.2 Division of responsibility with multiple parties involved

In AI fraud cases, the division of responsibilities among multiple parties is a core challenge in the application of criminal law [9]. Developers, platforms and users have different roles in the technology chain, and the determination of responsibility should be based on subjective fault, technical control and the actual impact of the behavior on the harmful consequences.

Developers are the creators of technology, controlling the core links of algorithm design and training data. If they deliberately leave vulnerabilities, neglect security testing, or do not impose restrictions on high-risk features, they may constitute an accomplice to fraud or a principal offender to related computer crimes. The platform, as a technology application intermediary, has obligations for content review, risk prevention and control, and user management. If the necessary technical regulatory duties are not fulfilled, resulting in AI technology being used on a large scale for fraud, it may constitute the crime of assisting information network criminal activities or the crime of refusing to perform information network security management obligations. If a user, as the end user, uses AI-generated content knowing it is deceptive for illegal profit, he or she shall bear the main criminal responsibility as the direct perpetrator of fraud. In specific cases, the proportion of responsibility should be dynamically adjusted based on the degree of fault of each subject, the causal relationship between the act and the result, and the actual control ability of the technical risk to ensure the

fairness and effectiveness of criminal regulation [10].

3.2 The Separation of Time and Space between "Acts" and "Intentions"

3.2.1 Independence and controllability of AI behavior

The development of artificial intelligence technology has made the independence of AI-generated behavior an important issue in criminal law. Technically, AI relies on deep learning algorithms and large-scale data training to simulate human intelligence to perform multiple tasks, and its output does not require real-time human intervention, seemingly "independent". But criminal law requires subjective will to govern and control, and AI behavior is essentially the product of program code and algorithmic logic, lacking autonomous consciousness and subjective intent, and thus cannot be regarded as an independent act in the sense of criminal law [25].

In judicial practice, the independence of AI-generated acts affects the determination of liability [11]. If it is determined to be an independent act, it may separate the responsibility of the actor from that of the AI, providing the user with grounds for conviction. But the current legal framework generally regards AI as a tool, and the consequences are attributed to the developers, users, or operators. If AI automatically generates false information or fraud, the responsibility lies with the developers or deployers. This suggests that AI's "independence" is unlikely to be a cause for users to be criminalized; instead, it may be a basis for conviction. If developers or platforms fail to exercise reasonable care, they may be found guilty of negligence or assistance in committing a crime.

The controllability of AI-generated behavior also affects the application of criminal law. Although AI is "autonomous", its operating logic is constrained by algorithms, data, and system settings. Judging its controllability requires a comprehensive consideration of the developer's control ability, the user's intervention space and the platform's regulatory responsibility [26].

3.2.2 Difficulties in intent determination and alternatives

Subjective intent determination is a difficult point in judicial practice in AI fraud cases. AI technology is highly intelligent and automated, and the subjective intent of the perpetrator is often concealed, making traditional methods of inferential behavior difficult to apply. Deepfake technologies such as AI face-swapping and voice synthesis can simulate real identities, making fraud seem like real communication, and the real intentions of the actors are hidden by the technology and difficult to identify directly. Moreover, the "black box" nature of AI algorithms exacerbates the difficulty of identification. Deep learning models make decisions that are complex and unexplainable, developers do not understand the operating logic, and judicial authorities face technical obstacles when reviewing evidence, making it difficult to trace true intentions [27].

Legal presumption is feasible as an alternative form of proof [12]. It reasonably presumes the subjective intent of the actor through the logical connection between the underlying facts and the presumed facts. In an AI fraud case, if the perpetrator uses deepfake techniques, combined with objective facts such as the transfer of funds and the standardization of fraud patterns, it can be presumed that he has the purpose of illegal possession. This helps to solve the problem of proof and provides an operational path. But the statutory presumption should be based on sufficient factual basis, supplemented by strict evidence examination to prevent misjudgment.

Procuratorial organs should strengthen supervision to ensure that conclusions are reasonable and legal and avoid "objective imputation" [28].

To enhance the accuracy of the determination, it is necessary to improve the relevant technical appraisal system and legal norms.

3.3 The Difficulty of Proving Subjective Intent

3.3.1 Criteria for determining intent in AI fraud

In AI fraud crimes, the determination of intent is the key to determining whether the perpetrator constitutes a crime. In traditional criminal law, "knowing" and "hoping or allowing" constitute the basic elements of intent, but the intervention of AI technology brings new challenges. When an actor uses AI to carry out automated deception, subjective intent is often hidden behind the technology, increasing the difficulty of judicial determination. If the perpetrator denies intent on the grounds of "technology neutrality," but abuses the potential of AI deception despite knowing it, criminal intent should be determined. It is also difficult to determine the purpose of illegal possession. The

way of transferring funds through AI fraud is concealed and requires a comprehensive judgment based on the flow of funds, and the concealment of technical means adds to the difficulty [29].

In judicial practice, the determination of criminal intent in AI fraud is constrained by evidence collection and technical appraisal [13]. Electronic evidence is prone to tampering and loss, making it difficult to prove the subjective intent of the perpetrator, and judicial personnel often lack an in-depth understanding of the principles of AI technology, making it difficult to determine whether the perpetrator knew the consequences. If the actor claims that he was not directly involved in the content generation, it is necessary to prove the extent of his involvement through technical analysis, etc. [30]

3.3.2 Completeness and reliability of the chain of evidence

In the judicial practice of AI fraud crimes, there are huge challenges to the integrity and reliability of the chain of evidence. The traditional criminal evidence system is centered on physical objects, verbal evidence and expert opinions, but the intervention of AI technology has made the evidential attributes and validity of electronic data, especially AI-generated content, the focus of controversy. The credibility of AI-generated content is questionable, its authenticity is difficult to verify directly, deep learning models are complex, the output results are affected by multiple factors, and the output of the same input varies greatly in different scenarios, making it difficult to meet the objective requirements of criminal evidence. Moreover, AI- generated content lacks traceability and veriability, such as forged chat records that look no different from real data but have difficulty tracing their sources and formation processes, challenging the rules of original evidence and best evidence [31].

The difficulty in constructing the chain of evidence exacerbates the problem of judicial determination. AI fraud cases involve multi-link, cross-platform data interaction and fragmented evidence. Criminals use AI to forge information, and key evidence extraction and fixation face technical obstacles. Even if data is obtained, proving that it has not been tampered with is also a key point. The current regulations are not targeted at the particularities of AI-generated content. For example, in AI voice synthesis fraud cases, there are no specific identification standards, and traditional review methods have difficulty determining the authenticity of the voice. There is also a lack of clear legal guidance on whether technical materials generated by the operation of AI systems are qualified as evidence and how to incorporate them into the evidence system [32].

3.4 The Issue of Blocking Causality

3.4.1 The causal relationship between AI behavior and results

In AI fraud crimes, the determination of the causal relationship between the act and the harmful consequences is complex. In traditional criminal law theory, the establishment of a causal relationship depends on the directness and predictability of the act and the result, but this standard is challenged in the context of AI fraud [14]. The behavior of AI systems is highly autonomous and unpredictable, making it difficult to outline the causal chain. When AI generates fraud content, it may self- optimize and deviate from the intentions of developers or users, making it difficult for traditional causal theories to apply directly. Its "black box" nature increases the difficulty of judicial determination and raises disputes over liability attribution.

In judicial practice, whether the active intervention of AI constitutes a cause for the interruption of causality is the key to determining liability. As a technological tool, AI is often regarded as an extension of human will, but when it has the ability to make autonomous decisions, whether it can still be fully attributed to the human subject becomes a point of contention. Some views suggest that AI's autonomous behavior may disrupt the causal relationship and weaken the connection with harmful consequences; There are also views that even if AI is autonomous, it is essentially a human tool and the consequences should be borne by the responsible party, unless the operation of AI is completely out of human control [33].

The determination of causality in AI fraud cases is also affected by the difficulty of collecting and fixing evidence.

3.4.2 Application of indirect liability and joint liability

In AI fraud crimes, traditional criminal law attribution logic is difficult to apply directly due to complex causal relationships. When AI systems have the ability to make autonomous decisions, their actions may deviate from the

intentions of the designers or users, forming independent causal chains. If we adhere to the traditional "behavior-result" direct causal relationship determination standard, there will be loopholes in accountability. At this time, the application of indirect liability and joint liability becomes an important way to make up for the deficiencies in the accountability system. Indirect liability refers to the situation where an actor does not directly commit a harmful act, but a previous act or violation of obligation provides conditions for the harmful result. For example, an AI developer's failure to exercise reasonable care to use the system for fraud, even if not directly manipulated, can still be held accountable due to technical flaws or security loopholes [34].

Joint liability is applicable to AI fraud involving multiple parties, especially when the boundaries of liability among platforms, developers, and users are ambiguous and difficult to precisely define. At this point, joint liability can protect the rights and interests of the victims and prompt all parties to strengthen compliance review and risk control. If the AI platform fails to effectively review the fraud model and it is used to generate false information, it may share the responsibility with the user, which has a compensatory, preventive and deterrent effect. The application of both should be combined with the technical characteristics and behavioral patterns of the case, and reasonable allocation of responsibility can be achieved through the construction of comprehensive judgment criteria, which will help to build a criminal law accountability system that ADAPTS to the development of AI technology and effectively regulate AI fraud crimes [35].

3.5 Judicial Practice Dilemmas

3.5.1 The complexity of investigation and evidence collection

Ai-induced fraud crimes, as a new type of crime relying on emerging technologies, pose a huge challenge to judicial investigation and evidence collection. AI fraud is carried out through complex algorithms, encrypted communications and distributed networks. The criminal process is covert, and the evidence shows electronic, fragmented and cross-border characteristics. Traditional investigation methods have many obstacles in evidence collection, fixation and identification [15]. During the evidence collection stage, AI-generated content is dynamically concealed, such as deepfake voice and video fraud. Data transmission may be encrypted, tampered with or destroyed, and the original evidence is easily lost [16]. And AI fraud relies on overseas servers, etc. Investigators face technical barriers and conflicts of legal jurisdiction when retrieving data, and the efficiency of evidence collection is greatly restricted in the absence of international judicial collaboration. In terms of evidence fixation, AI-generated content is complex, traditional methods are difficult to effectively extract and preserve, deepfake content identification verification requires professional institution appraisal, but the procedures are cumbersome, time- consuming and there is no unified standard. In the evidence appraisal process, AI fraud techniques are constantly evolving, and the requirements for the professional capabilities and equipment of judicial appraisal institutions are extremely high. China lacks systematic and standardized judicial technical support for the identification and appraisal of AI-generated content, and some key evidence cannot be effectively appraised and is excluded, affecting conviction and sentencing. For this reason, there is an urgent need to improve the system in terms of technology, law, judicial capacity, etc., to enhance the response capacity [36].

3.5.2 Uncertainty in the application of the law

The rapid development of artificial intelligence technology has given rise to a new type of crime called AI fraud. Under the current criminal law framework, there are many uncertainties regarding the application of law to AI fraud cases. AI fraud relies on technologies such as deepfakes, which are highly concealed and deceptive. When the current criminal law provisions were formulated, the complexity of such technological crimes was not fully anticipated, resulting in differences in the characterization of related acts in judicial practice. There is controversy over whether false information generated by AI constitutes "fabricating facts" or "concealing the truth", and how to determine the subjective intent of the perpetrator. Moreover, AI fraud involves multiple links, the responsible subjects are scattered, and provisions such as joint crimes in traditional criminal law are difficult to effectively deal with, and the boundaries of legal application are unclear [37].

In specific application, provisions such as fraud may be invoked, but the standards of application

and the paths of interpretation are not uniform. In the case of fraud, whether false information generated by AI constitutes the core element of "defrauding property" depends on the circumstances of the case. The judicial interpretation does not clearly define the legal nature of such technical means. AI fraud is carried out through online platforms and involves the application of the crime of assisting information network criminal activities, which has a vague standard for determining the degree of "knowledge".

4. The Four-in-One Criminal Law Regulation Approach

4.1 Build a Model of Criminal Legislation that Combines Macro and Micro Perspectives

4.1.1 The necessity of legislative improvement

The rapid development of artificial intelligence technology has given rise to new types of fraud crimes, which are covert, technically demanding and widely harmful, posing a challenge to the traditional criminal law system. The current criminal law mainly targets traditional frauds directly committed by natural persons, and it is difficult to deal with the problems of the interweaving of technical subjects and natural persons' behaviors and the blurred boundaries of responsibility in AI frauds.

Such as deepfake technology for identity fraud and AI-generated content misleading victims, although they meet the constitutive elements of fraud, the technical intervention complicates the responsible subjects, and judicial practice faces difficulties in determining responsibility. Therefore, there is an urgent need for specialized legislation to fill legal loopholes, clarify the composition of AI fraud crimes and the boundaries of criminal law regulation, and enhance the pertinence and effectiveness of the application of the law [38].

Specialized legislation can clarify the responsibilities of multiple parties involved in AI fraud. Under the current legal framework, developers and others often evade criminal responsibility due to the lack of guidance, and the crackdown is limited [17]. The addition of specific charges such as "fraud using artificial intelligence technology" can precisely combat crimes, strengthen the compliance obligations of technology providers, and promote full-chain governance [18]. Provide a uniform standard of judgment for judicial authorities, reduce differences in the application of law, and enhance the effectiveness of crackdowns.

Specialized legislation on AI fraud crimes is an important manifestation of the modernization of criminal law. Although China has issued relevant normative documents, there is still a lack of targeted provisions at the criminal regulation level.

4.1.2 Feasibility analysis of the legislative model

When designing the legislative framework for AI fraud crimes, it is necessary to balance technological innovation and legal regulation to ensure that the law effectively addresses new types of crimes while leaving room for technological development. The legislative framework should be flexible and forward-looking, adapting to rapid technological iterations and effectively regulating potential criminal risks [19].

Establish a combination of "risk-oriented" and "technology-neutral" principles. Risk-oriented management requires stratified and categorized management based on the degree of harm caused by the application of technology, while technology-neutral emphasizes that laws focus on the consequences of actions and avoid the invalidation of laws due to changes in the form of technology. Introduce a dynamic adjustment mechanism, regularly assess technology trends and judicial feedback, and revise the provisions in a timely manner [20]. Specific access and regulatory standards for highly hazardous technology applications could be set by drawing on the classification of high-risk systems under the EU's Artificial Intelligence Act. Establish a "regulatory sandbox" mechanism that allows technology to be piloted in specific areas, with limited exemptions from legal liability, and encourages enterprises to explore compliance paths, reducing innovation costs while accumulating experience for legislation. Strengthen multi-party collaborative governance and encourage the joint participation of governments, enterprises, industry associations, etc. in rule making to form a "co-governance" regulatory system to provide a stable legal environment for the healthy development of artificial intelligence.

4.2 The Judiciary Clarifies the Allocation of Responsibilities and the Rules of Evidence

4.2.1 Legal guidance on the allocation of liability

In AI fraud cases, clarifying the judicial guidelines and criteria for determining the

responsible party is a core issue that urgently needs to be addressed in criminal justice practice. AI technology is complex and involves multiple parties. Traditional liability determination models are difficult to apply directly. It is necessary to construct targeted judgment standards in combination with technical features and legal norms.

The construction of standards should start with the technical chain and clarify the legal status and obligations of the subjects in each link. Developers, as the source of technology, are responsible for algorithmic compliance and application predictability. If an AI system is flawed or used for illegal purposes, the developer may be held responsible for not exercising reasonable care, such as when an AI speech synthesis system is used for fraud without an identity verification mechanism, the developer should be held responsible. The responsibility of the platform operator should be determined in combination with its regulatory and control capabilities. Failure to effectively review or remove fraudulent information may constitute a crime. The user, as the direct operator, has subjective intent and relevance to the consequences of the act as the key to determining liability, and it is necessary to determine whether it constitutes a principal offender or an accomplice based on the way of use, purpose and result. It is necessary to define the boundaries of responsibility for indirect participants such as technical intermediaries and data providers to avoid generalization of responsibility. It is suggested that specific judicial interpretations or guiding cases be introduced to clarify the rules of responsibility allocation, standardize evidence review and fact-finding, and ensure that judicial decisions take into account both technical logic and the requirements of criminal law doctrine.

4.2.2 Suggestions for optimizing the rules of evidence

The frequent occurrence of AI fraud crimes poses a severe challenge to traditional criminal evidence rules. Ai-generated content is highly realistic, dissemination is automated, and data storage is decentralized, making it difficult to collect, review and determine evidence. To this end, an evidence rule system tailored to the characteristics of AI fraud needs to be established to enhance the accuracy and efficiency of judicial determination. In terms of evidence collection, it is necessary to strengthen the norms for the fixation and extraction of electronic data, clarify the requirements for the simultaneous collection of technical evidence such as AI model parameters and training data to ensure the integrity of the chain, and introduce blockchain evidence storage technology to enhance the tamper-proof ability of electronic evidence. When reviewing evidence, establish the principle of algorithmic transparency, require technology providers to explain the operating mechanism of the AI system, and those who cannot explain or conceal it can be presumed to have illegal intent. At the same time, strengthen technical analysis and enhance the probative force of evidence through methods such as data traceability. In the determination of evidence, presumption rules can be introduced to comprehensively judge subjective intent through indirect evidence such as the way the perpetrator uses AI technology, and explore cross-border electronic evidence retrieval mechanisms to solve the problem of obtaining evidence for cross-border AI fraud. To effectively address the judicial challenges of AI fraud, systematic optimization of evidence rules is necessary.

4.3 Social Co-Governance Promotes Public-Private Collaboration and Public Participation

4.3.1 Co-governance between the government and enterprises

Collaboration between the government and enterprises in the fight against AI fraud is key to effective governance. As a representative of the public interest, the government needs to set compliance boundaries for enterprises through legislation, regulation and policy guidance, and promote multi-party collaborative governance. Enterprises should take the initiative to assume the responsibility of risk prevention and control in technology development and application, and embed security mechanisms in all aspects of product design and operation. The government can establish uniform technical standards and compliance requirements to guide enterprises to implement security measures in algorithms, data usage and content generation, such as mandating deepfake content identifiers to ensure traceability and verification. Promote cross-departmental data sharing, provide technical support and intelligence sharing platforms for enterprises, and enhance risk early warning and response capabilities. Enterprises should establish internal compliance review and risk

assessment systems to filter out potential fraud content and prevent technology abuse. Both parties can also jointly carry out public education to raise public awareness of prevention. The government relies on regulation to push enterprises to fulfill their safety responsibilities, while enterprises embed safety design throughout the entire product cycle to form a closed-loop management. This collaborative model can enhance governance efficiency and precision and provide a feasible path for balancing technological development and legal regulation.

4.3.2 Raising public awareness and promoting education

The development of artificial intelligence technology has given rise to new types of fraud methods, which are concealed and complex, making it difficult for the public to identify and guard against them. Enhancing public awareness and ability to guard against them has become an important part of social governance. Education and publicity strategies should focus on systematicness and targeting to adapt to the characteristics of different groups. The basic knowledge of artificial intelligence should be popularized through a multi-level and multi-channel education system. For example, for the elderly, use community lectures and illustrated brochures to explain fraud techniques such as "AI face-swapping" and how to deal with them; for teenagers, incorporate them into the school education system to develop their rational cognition and critical thinking skills.

Innovation in publicity methods is of great significance for enhancing public acceptance and participation. New media tools such as short videos and interactive mini-programs can vividly convey anti-fraud knowledge. Public security departments and media platforms can jointly produce situational skits to recreate fraud scenarios. Invite victims to share their experiences to enhance awareness and immersion. Offline community lectures, public place warning signs, etc. should also be an important part of publicity, covering different groups.

To promote public education and publicity, governments, businesses and social organizations need to work together. The government plays a leading role in formulating plans and providing policy and financial support; enterprises, especially technology companies, take on social responsibility and use technology to enhance users' safety awareness; the media play a role in guiding public opinion and expanding publicity coverage. Integrate multiple parties to enhance publicity effectiveness and provide institutional guarantees for building an atmosphere of prevention.

4.4 Technological Countermeasures: Countering 'AI' with 'AI'

4.4.1 The defensive role of technological means

Artificial intelligence technology plays a significant role in identifying, tracking, and curbing AI fraud. With deep learning and big data analytics, AI can accurately identify scams and give real-time warnings, reducing the success rate of crimes. In the case of AI face-swapping and voice synthesis scams, biometr-based verification techniques can effectively distinguish between real and fake scams by analyzing parameters such as facial dynamics and voiceprint fluctuations. AI uses knowledge graphs to integrate multi-source data and build a full-chain tracking model to mine accounts, devices and IP associations involved in cases and improve the efficiency of solving cases. In the containment phase, AI-driven real-time interception systems can automatically identify and block suspicious operations in transactions, reducing financial losses. In the face of the complexity of fraud methods, AI anti-fraud technologies need to be continuously optimized, such as enhancing the comprehensiveness and accuracy of detection through multimodal fusion analysis, achieving cross-agency data sharing through federated learning, and providing support for building a national AI anti-fraud collaborative system. In the future, the development of AI anti-fraud technology will require algorithmic innovation, policy and regulation improvement, and industrial synergy to form a combined force of technology, law and social governance to enhance prevention and control capabilities.

4.4.2Technical ethics and legal constraints

Technical ethics and legal constraints are core issues in the application of AI countermeasures technology. Although the technical means are neutral, the application scenarios and effects are related to social order, individual rights and the public interest. Therefore, ethical guidelines and legal boundaries must be clearly defined during the development and use stages to prevent abuse or misuse.

Ethically, AI countermeasures should follow the

principles of fairness, transparency and accountability. Algorithmic design should avoid data bias or model flaws that lead to discrimination against specific groups, and ensure that the operation process is explainable and traceable to enhance public trust. Developers and users should take on social responsibility to ensure that technology serves public safety and social well-being, rather than manipulating the market or infringing on privacy.

At the legal level, the use of AI countermeasures must strictly comply with existing laws, covering data protection, privacy rights, intellectual property rights, and the application of criminal law. When dealing with deepfake fraud, content identification and interception must not infringe upon the legitimate rights of others to avoid misjudgment and liability. In response to the possibility that it could be maliciously used for new types of cybercrime, criminal law should promptly define the boundaries of criminal liability. Legislative bodies should, in light of technological trends, refine legal provisions and build a forward-looking and adaptive legal framework to regulate and guide AI countermeasures in a reasonable manner.

5. Conclusions

5.1 Research Summary

Artificial intelligence fraud crimes face multiple challenges in criminal law responses. The current law, which takes natural persons or legal persons as the responsible subjects, is prone to break the chain of accountability in the face of AI- involved crimes. AI, as a technical tool, has no independent criminal liability capacity. Its criminal acts are often manipulated by developers, operators or users, and it is difficult to define the proportion of liability under the collaboration of multiple subjects [21]. "Act" and "intention" are separated in time and space. The autonomy of AI makes it possible that the content or operation it generates is beyond the control of the designer, making it difficult to apply traditional criminal law standards for the unity of subjective intent and objective act, such as AI-generated false information fraud, where the determination of the subjective intent of the perpetrator becomes difficult. AI intervenes in multiple stages of the criminal process, making it difficult to define the causal relationship, affecting the allocation of criminal responsibility, and there are disputes over the admissibility and probative force of evidence generated by AI, making it difficult to construct the chain of evidence [22].

In terms of theoretical breakthroughs, the research has moved from opposition to integration. Some scholars advocate for a moderate expansion on the basis of adhering to traditional criminal law doctrine, introducing the concept of "technology- neutral but application requires regulation", emphasizing the substantive judgment of the subjective intent of AI fraud perpetrators, such as solving the problem of determining subjective intent through legal presumption and introducing the "risk increase theory" to assist in the judgment of causal relationship [23].

5.2 Prospects for the Future

The evolution of artificial intelligence technology poses challenges to the criminal law system, and the problem of determining criminal responsibility for AI- directed crimes remains unsolved. Discussions in the academic community on whether AI is a subject of criminal responsibility are still in theoretical debate and no consensus has been reached. Future research needs to combine technological trends to explore whether strong artificial intelligence can be given criminal responsibility status after it has autonomous consciousness and decision-making ability, which concerns both the traditional definition of responsibility subject in criminal law theory and the response of criminal policy to the risks of emerging technologies. Building a reasonable accountability mechanism within the framework of criminal law dogmatics for criminal acts caused by AI autonomous decision-making is a core challenge, especially when AI behavior is out of human control. Defining causal relationships, introducing new accountability principles or forms of liability all require in-depth research.

In the context of globalization, AI-related crimes are transnational, and issues of jurisdiction, application of law and international collaboration should be the focus of future research. There are differences among countries in the determination of criminal liability for AI, which may lead to conflicts of law application and obstacles to judicial collaboration [24]. Therefore, it is necessary to promote consensus among the international community and explore the establishment of unified international legal rules and collaboration mechanisms. The rapid

development of AI technology poses new challenges to criminal investigation, etc. How to reasonably introduce technological means to assist judicial practice while ensuring judicial justice is also an important issue.

References

[1] Fan Huxi. The generation logic, behavioral composition and determination of the new three characteristics of AI-intervened Telecommunications and Internet fr aud crimes [J]. Journal of Guizhou Police College, 25,37(04):110-116.

[2] Wang Chongyang. On Criminal Law Regulation of Artificial Intelligence in t he Economic Age. Rural Economy and Technology,2021

[3] Zhang Huanran. Research on New Types of Fraud Crimes Triggered by Gene rative Artificial Intelligence [J]. Legal Forum,2024,(03):143-157.

[4] Zhang Yi, Yang Chenlong. Research on the Investigation of Telecommunicati on and Internet Fraud crimes using Generative Artificial Intelligence [J]. Journal of Hunan Police College, 24,36(05):21-28.

[5] Zhang Xu, Yang Fengyi. Between Adherence and Reform: Artificial Intelligen ce Criminal Risks and Approaches to Criminal Law Responses [J]. Journal of So cial Sciences of Jilin University,2021,61(05).

[6] Liu Renwen, Cao Bo. Criminal risk and liability of artificial intelligence agent s [J]. Jiangxi Social Sciences,2021,41(08):

[7] Sun Hao. Research on Countermeasures of AI-related Crimes [D]. Supervisor: Hu Xiangyang. Zhongnan University of Economics and Law, 2020.

[8] Peng Shulin. Analysis of Criminal Law Issues Related to Artificial Intelligence. Legal Review (Master's Forum, Classic Essays),2021

[9] Liu Xianquan. Analysis of Attribution and Criteria of Liability in AI-related Crimes [J]. Oriental Law,2020,(03):66-75.

[10] Liu Xianquan. Determination of Subjective Fault of Developers in AI-related crimes [J]. Comparative Law Studies,2019,(04):101-110.

[11] Wu Yunfeng. The Dilemma and Solution of Criminal Law Application for Property Crimes in the Era of Artificial Intelligence [J]. Law,2018,(05):165-179.

[12] Chen Siyu. Research on Criminal Law Regulation of AI Crimes. Northeast Forestry University,2022-03-01

[13] Sun Hao. Research on Countermeasures for AI-related crimes. Zhongnan Uni versity of Economics and Law, June 1,2020

[14] Jin Yifeng, Ma Zhonghong. The application of artificial intelligence in criminal investigation: Practical forms, Risks and Challenges, and Development strategies. Science & Technology Review, April 13,2023

[15] Song Zebin. Research on Criminal Liability Capacity of Machine Learning-based Artificial Intelligence. North Minzu University,2022-12-01

[16] Xie Anping, Liu Yulong. Artificial Intelligence Subjectivity Theory and the judgment of Legal Normative Subjects in Criminal Law. Tianjin Law,2021-03-15

[17] Li Lifeng, Wang Junsong. Obstacles and Positioning of Artificial Intelligence Embedded in the Criminal Law System: Reflections on the Risk Society Theory within the Criminal Law Dogmatic System. Rule of Law Studies,2023-01-10

[18] Zhu Xiaoyan. Research on Criminal Law Responses to Telecom and Internet Fraud in the Context of the Digital Society. Jilin University,2022-03-01

[19] Wang Libin. The subject attributes of AI crimes and the reform of crimes and punishments. Journal of Fujian Police College,2020-06-20

[20] Guo Yifan. A Study on the Criminal Regulation of Web Crawlers from the Perspective of Data Crime. Huazhong University of Science and Technology, Ma y 1,2021

[21] Du Wenhui Research on Criminal Law Regulation of Cybercrime. Heilongjia ng University,2020-06-20

[22] Dai Siya. A Study on the Criminal regulation of the Use of Theft. East China University of Political Science and Law, May 12,2021

[23] Bai Bing. An Outline of Criminal Law Functions in the Age of Artificial Intelligence. Tianjin University, June 1,2021

[24] Liu Hongjie. Research on the Problems and Countermeasures of Judicial Ope nness from the Perspective of Artificial Intelligence. Wenzhou University, April 1,2020

[25] Chen Yijian, Qiu Jifeng. Dilemmas and solutions: Criminal Compliance Gov

ernance of Cyber Data Crimes. Rule of Law Forum,2023-10-31
[26] Chen Miaojuan. Research on Criminal Law Regulation of Data Crimes in th e Big Data Era. Taiyuan University of Science and Technology, May 1,2023
[27] Zou Xuan. Research on Criminal Law Regulation of Online Credit Manipula tion. Dalian Maritime University, May 29,2021
[28] Teng Jianwei Liu Wenqiang. Intelligent Investigation from the Perspective of Criminal Spatial Laws: Predicaments and Breakthrough approaches. Journal of S hanxi Police College,2023-11-15
[29] Zhang Jie. Research on Micro-crimes as a problem of Criminal Law regulation. Inner Mongolia University, May 22,2019
[30] Ma Zhiguo Tian Xiaochu. On the Possibility of Applying Artificial Intelligence to Criminal Law. Journal of Huazhong University of Science and Technology (Social Sciences Edition),2018-03-10
[31] Tang Mi. Research on Criminal Risks in the Age of Artificial Intelligence and Criminal Law Responses. Legal Review (Master's Forum, Classic Essays),2021
[32] Liu Xianquan Tang Jun. Criminal law regulation of data crimes in the Age of Artificial intelligence. People's Procuratorate,2019
[33] Wang Qianyun. Thoughts on criminal law regulation of Data Security crimes in the context of Artificial Intelligence. Law Forum,2019
[34] Yang Cheng. Research on the Subject and Criminal Responsibility of AI-ind uced Crimes. People of The Times 2022
[35] Liu Xianquan. The path of criminal law regulation of AI-related crimes. Modern Law,2019
[36] Di Ying, Wang Jichun. Risk Analysis and Criminal Law Regulation in the Age of Artificial Intelligence. Journal of Guangzhou Public Security Management C adre College,2019
[37] Wang Yanling Criminal Law issues and Responses in the Age of Artificial Intelligence. Politics and Law,2019
[38] Zhao Yanhong. Discussion on the Application of Artificial Intelligence in the Judgment of Criminal Proof Standards. Journal of Shanghai Jiao Tong University: Philosophy and Social Sciences Edition,2019

