

Challenges and Countermeasures in the Application of Criminal Law for Cyber financial Crimes in the Era of Artificial Intelligence

Qizhen Shangguan

Jiangxi University of Science and Technology, Ganzhou, Jiangxi, 341000, China

ABSTRACT

Artificial intelligence is widely used in the financial field, and online financial crimes are characterized by precision, diverse means, and deep forgery, which brings challenges to the application of criminal law such as difficult identification of criminal subjects, complex judgment of causal relationships, and legal lag. Therefore, it is necessary to break through the traditional legal application thinking, clarify the identification of subjects and responsibilities, establish the principle of criminal responsibility, refine the liability of accomplices, pay attention to the timeliness and adaptability of the law, strengthen cooperation and use technical means, improve the application of criminal law in this field, and maintain financial order and social stability.

KEYWORDS

Artificial intelligence; Cybercrime; Application of criminal law; International cooperation; Financial security

1 Overview of Internet Financial Crimes in the Era of Artificial Intelligence

1.1 Background, Purpose, and Significance

The rapid development of digitalization and the deep integration of artificial intelligence into the financial field have brought about innovative applications such as intelligent risk assessment models and automated trading systems, improving the efficiency and quality of financial services. But criminals use this to make online financial crimes more complex and diverse. They use intelligent algorithms to commit crimes with precision, interfere with the authenticity of transactions with deep forgery technology, manipulate the market with intelligent algorithms, and use machine learning to assist in money laundering. These new types of crimes are frequent, posing serious challenges to China's financial security and order, and increasing criminal legal risks. In this situation, traditional criminal law is difficult to effectively identify and sanction new types of online financial crimes, seriously threatening the financial market and investors' rights. It is urgent to solve the dilemma of criminal law application.

1.2 New Network Financial Crime Models Driven by Artificial Intelligence Technology

In the era of artificial intelligence, online financial crimes are constantly evolving and upgrading, giving rise to a series of new criminal methods that rely on artificial intelligence intelligence, automation, and efficiency.

1.2.1 AI face swapping and voice synthesis fraud

Scammers use AI face swapping to forge videos and photos, impersonate others to commit fraud; Falsifying the victim's voice through voice synthesis to gain trust.

1.2.2 Intelligent phishing attack

Using AI to analyze personal information and generate personalized phishing emails, developing automated phishing tools to deceive victims.

1.2.3 Ransomware and Malicious Software

Smart ransomware uses AI to identify system vulnerabilities, encrypt files, and demand ransom, while malicious software uses AI to generate variants to evade detection.

1.2.4 Social engineering fraud

Scammers use AI to analyze big data and develop precise strategies, using emotional manipulation to gain trust.

1.2.5 Virtual currency and blockchain crime

Using AI to analyze vulnerabilities in virtual currency to commit theft, and laundering money through blockchain technology.^[2]

2 Challenges faced by the application of criminal law in online financial crimes in the era of artificial intelligence

2.1 Difficulties in determining the criminal subject

2.1.1 Controversy over whether artificial intelligence systems can serve as criminal subjects

In the era of artificial intelligence, whether artificial intelligence systems can become criminal subjects has sparked heated discussions, and there is no consensus on this in the law. One side believes that artificial intelligence behavior is dominated by algorithms and programming, and lacks the ability to bear criminal responsibility; On the other hand, due to its increased autonomy and even the possibility of losing control, it is believed that it should be regarded as a criminal subject.

From a legal practice perspective, it is difficult to treat artificial intelligence systems as criminal subjects. It lacks emotional and moral judgment, cannot understand the legal consequences of its actions, and its punishment is difficult to implement. So, currently most legal systems tend to attribute responsibility to the developers, users, or controllers behind it.

2.1.2 Issue of Responsibility Allocation when Multiple People Participate in Crime

In the era of artificial intelligence, online financial crimes often involve multiple people, such as developers, users, controllers, etc. According to the Criminal Law of the People's Republic of China, the responsibility for joint crimes is divided according to the roles and positions of the participants, with the principal offender having a heavier responsibility and the accomplices having a lighter responsibility.

However, in this context, the roles and positions of each participant are difficult to clarify. Developers may only provide technical support, and users may operate the program without realizing the harm. When assigning responsibility, it is necessary to comprehensively consider factors such as subjective intention, nature of behavior, and degree of harm.^[3]

2.2 Complexity of Defining Criminal Behavior

2.2.1 Legal difficulties in characterizing new criminal methods

The development of artificial intelligence has made online financial crimes more complex and diverse, with new methods such as deepfakes and fraud being covert, efficient, and difficult to trace. Traditional laws are unable to cope with this, and legal characterization is facing challenges.

To solve the problem, it is necessary to strengthen the research and monitoring of new criminal methods in the application of criminal law, grasp the characteristics and laws, provide a basis for qualitative analysis, and strengthen cooperation in multiple fields to combat crime.

2.2.2 The boundary between technological neutrality and criminal assistance behavior is blurred

In the era of artificial intelligence, the boundary between technological neutrality and criminal assistance behavior is blurred. Technological development provides convenience for crime, but also has a neutral and harmless attribute. To determine whether it constitutes criminal assistance, it is necessary to comprehensively consider the technical nature, purpose, and subjective intention of the perpetrator. Knowing that others are using artificial intelligence to commit crimes and providing technical support may constitute criminal assistance; Providing ordinary technical services without realizing that they are being used for criminal purposes should not be considered as criminal assistance.

2.3 Obstacles to Evidence Collection and Acceptance

In the era of artificial intelligence, evidence of online financial crimes is mostly in electronic form, which is easily tampered with and lost, making it difficult to collect and accept. Blockchain technology can be used to record the process of electronic evidence circulation, prevent tampering, strengthen identification and review, and ensure compliance with evidence standards. Meanwhile, although evidence analysis methods based on artificial intelligence are common, algorithms and models may have defects and biases, and the results may not be reliable enough. Therefore, regulatory

evaluation needs to be strengthened to meet legal requirements.^[4]

3 Strategies for Dealing with the Challenges of Criminal Law Application in Cyberfinancial Crimes in the Era of Artificial Intelligence

3.1 Clarify the criminal subject and the criteria for determining responsibility

3.1.1 Establish the principle of criminal responsibility for artificial intelligence related entities

Clarify under what circumstances artificial intelligence agents (such as AI systems, robots) can be considered as criminal responsibility subjects, or determine the responsibility attribution of the designers, developers, and users behind them. Develop specific legal provisions, distinguish the allocation of responsibilities in different situations, and ensure the fairness and effectiveness of accountability.

3.1.2 Refine the rules for sharing responsibility in joint crimes

In joint crimes involving artificial intelligence, it is necessary to clarify the responsibility ratio and sharing mechanism of each participant. The current criminal law does not grant artificial intelligence independent legal status, and its crimes need to be committed jointly with humans. Punish the manipulator in indirect offenders. In joint negligence crimes, the Criminal Law only recognizes joint intentional crimes as accomplices, but judicial interpretations have not completely denied joint negligence crimes. The provision of joint liability for hit and run traffic accidents can be compared to the negligence responsibility of artificial intelligence developers and users.^[5]

3.2 Improve the legal definition of criminal behavior

Timely revise and supplement relevant legal provisions to clarify the criminal nature of new forms of online financial crimes that have emerged in the era of artificial intelligence. Combining typical cases at home and abroad, analyze the characteristics and harm of new criminal methods, and provide empirical basis for legal interpretation. In March 2019, criminals used artificial intelligence speech synthesis software to synthesize the voice of the CEO of a certain energy company's German headquarters, in order to request the head of the UK branch to urgently transfer funds to foreign suppliers within one hour. Due to hearing the familiar German accent and the boss's language pattern, the person in charge had no doubts about the transfer instructions and was ultimately scammed 20000 euros. The following is an analysis of their criminal methods and characteristics.

3.2.1 Criminal Methods

AI speech synthesis: Criminals use AI speech synthesis technology to simulate high-level sounds, restore sound features, and enhance deception.

Social engineering attack: Establishing trust through simulated voice and language patterns, inducing transfers through psychological pressure and emergency time constraints.

Information theft: Illegally obtaining internal company information, simulating internal communication scenarios, and increasing the success rate of fraud.

Funds transfer: Quickly transfer funds to other accounts or regions after successful fraud to evade investigation.

3.2.2 Criminal Characteristics

Intelligence and concealment: AI technology makes criminal methods more intelligent, concealed, and difficult to identify. Accurate positioning and efficient execution: Big data and machine learning can accurately locate targets and quickly execute fraud. Cross border crimes and capital flows: It is difficult to investigate cross-border crimes and transfer funds without borders by using the Internet. Large economic losses: Victims often suffer huge economic losses due to large transfers in emergency situations.

3.3 Optimizing the Evidence System

3.3.1 Establish an electronic evidence collection and preservation mechanism

The importance of electronic evidence has increased in criminal justice. To ensure its authenticity, integrity, and recoverability, a dedicated collection and preservation mechanism should be established, using digital signatures,

timestamps, and other technical means to prevent tampering. At the same time, clarify the scope, methods, and procedures of collection to improve the efficiency and quality of investigation. For electronic data generated by artificial intelligence analysis results, specialized collection channels and storage methods need to be established.

3.3.2 Standardize AI evidence analysis methods and acceptance standards

With the widespread application of artificial intelligence, it is necessary to clarify its evidence analysis methods and processes, develop technical specifications, and ensure the scientific nature of the analysis process. Establish acceptance standards that comprehensively consider accuracy, reliability, and interpretability. Evaluate accuracy through comparison, peer review, and other methods, taking into account the legitimacy of data sources and the reliability of algorithm stability assessment. Provide technical explanations and clarifications to improve interpretability.^[6]

4 The role of international cooperation and exchange in addressing cybercrime

To explore the role of international cooperation in cyber financial crimes, it is necessary to analyze the characteristics of crimes, the status quo of international cooperation and strategies to strengthen cooperation, and focus on the challenges of Internet boundlessness and cross sectoral cooperation.^[7]

4.1 Characteristics and Trends of Cross border Cyberfinancial Crimes

The Internet has made financial crimes internationalized and cross-border crimes occur frequently. Criminals use the characteristics of the internet to commit transnational crimes, threatening global financial security, and their criminal methods are complex, spanning multiple fields, forming a complex criminal network.

4.2 Current Status and Shortcomings of International Cooperation

Although international cooperation mechanisms have been established, different countries have different laws, incomplete mechanisms for information sharing and judicial assistance, and difficulties in cross-border fugitive pursuit, which limit the depth and breadth of cooperation.

4.3 Strategies and Ways to Strengthen International Cooperation

To combat transnational cybercrime, countries need to jointly establish unified legal standards and enforcement frameworks. Information sharing and judicial assistance are key, and we need to strengthen platform construction, accelerate information exchange, and enhance monitoring and prevention capabilities; Improve judicial assistance, deepen cooperation in multiple aspects, and efficiently punish crimes.

Cyberfinancial crimes involve multiple fields and require cross departmental and international cooperation, resource integration, joint construction of cooperation mechanisms, and the development of standards and legal frameworks. Big data technology brings new methods to crime governance, which can accurately combat crime and facilitate cooperation, but the application needs to rely on legal frameworks to protect data and privacy.^[8]

5 Summarize

In the era of artificial intelligence, online financial crimes are characterized by technology driven, covert, and transnational features. Traditional criminal law faces challenges such as vague subject identification, difficulty in defining behavior, obstacles in evidence acceptance, and lagging charges. Research has found that the involvement of AI technology has led to disputes over the attribution of responsibility among criminal subjects, and new methods such as deepfakes and intelligent phishing are difficult to cover by existing charges. Moreover, cross-border crimes have intensified the complexity of governance. In response, the study proposes a collaborative governance framework of "law+ technology": it is necessary to clarify the division of responsibilities for AI crime subjects, improve the legal definition of new behaviors, establish a full process guarantee mechanism for electronic evidence, and promote the dynamic update of the criminal law criminal offense system (such as adding the crime of "deep forgery and abuse"). At the same time, drawing on international experience to strengthen corporate compliance supervision, establishing cross-border unified legal standards and law enforcement cooperation mechanisms, and utilizing big data technology to enhance cross-border tracking capabilities. The practical value of this study lies in providing a path to resolve the contradiction between technological abuse and legal backwardness, which has important reference significance for maintaining financial

security and promoting the reform of the global cybercrime governance system.

References

- [1] Li Lanying, Xue Chuja: "Theoretical Landscape and Implementation Path of Comprehensive Governance Effect Evaluation of Internet Financial Crimes", *Journal of Xiamen University*, Issue 1, 2023.
- [2] Yuan Jing: "Financial Security - AI Network Fraud and Prevention in the Intelligent Era", Information Technology Department of China Minsheng Bank.
- [3] Chen Si, Liu Yang: "Difficulties and Solutions in Determining the Criminal Responsibility Subject of Artificial Intelligence Participation in Financial Crimes", *Law Forum* (Issue 5, 2022).
- [4] Li Min, Wang Xue: "Research on Evidence Issues of Network Financial Crimes in the Era of Artificial Intelligence", *Modern Law*, (2023, Issue 4).
- [5] Wang Xiumei: "Criminal Responsibility and Punishment for Crimes Involving Artificial Intelligence", *People's Procuratorate* [Article No.] 1004-4043 (2023) 19-0011-06.
- [6] Yang Fei: Risk and Response: On the Application of Artificial Intelligence Evidence in Criminal Justice —— Taking "Facial Recognition Analysis Results" as an Example, *Journal of Shandong Police College*, March 2022, Issue 2.
- [7] Liu Kun: "Exploration of Issues and Countermeasures in the Governance of Cyberfinancial Crimes in the Era of Big Data", *Cyberspace Security*, 2024, 15 (01).
- [8] Pan Changhuan: "Analysis of International Criminal Judicial Assistance in Transnational Cybercrime", *Hebei Legal Vocational Education*, 2024 (03).