

Analysis On the Criminal Jurisdiction Path of Foreign-Related Cybercrime from The Perspective of Transnational Telecom Fraud

Fei Wang^{1,*}, Tianqi Zheng²

¹Department of Law, Liaoning University, Shenyang, China

²China Law Department, Jinan University, Jinan, China

* Corresponding Author Email: 196092107@mail.sit.edu.cn

Abstract. In today's era of advanced science and technology and rapid development of big data Internet, China's online telecom fraud shows the characteristics of transnational behavior or result, collectivization of criminal organization structure, diversification of crime methods, ganging of people involved and internationalization of cybercrime connection points. When Internet telecom fraud crimes occur from abroad to China, the research on whether China has jurisdiction over other countries and how to determine jurisdiction is of great benefit to building an effective information framework to combat crimes, actively accelerating the pace of international cooperation, effectively coordinating jurisdiction conflicts, and continuously strengthening the ability of domestic judicial organs to perform their duties. Therefore, this paper will start with the criminal jurisdiction of foreign-related cyber crimes from the perspective of transnational telecom fraud, and actively explore the correct way to determine the criminal jurisdiction of foreign-related cyber crimes in China by using the methods of literature research and comparative research. This paper starts with an all-round overview of telecom fraud, and then studies its essence and characteristics in the dimension of transnational telecom fraud. The theoretical basis and existing difficulties of the exercise of criminal jurisdiction over transnational telecommunication network crimes are summarized in two parts. This paper expounds the dilemma of the exercise of criminal jurisdiction, and finally gives some suggestions on the exercise of criminal jurisdiction over foreign-related cybercrime in China according to the above problems.

Keywords: Criminal jurisdiction; Foreign-related cyber crimes; Principle of universal jurisdiction; Theory of real harm connection; Aiding the offender.

1. Introduction

At present, the means of telecom fraud are constantly improving, and fraud schemes are emerging one after another, which is hard to prevent. In our ears, there have been countless cases of paying a painful price for telecom fraud. As a new type of network crime different from traditional crime, telecommunication network fraud crime is the product of the combination of traditional fraud and computer network technology. This kind of crime has seriously hindered social development, endangered the safety of public and private property, personal information security and network order, and has a serious impact on people's production and life. The crime of telecommunication network fraud seriously infringes on citizens' legitimate rights and interests, so we should strengthen our awareness of learning, improve our ability to recognize and prevent fraud, and at the same time, we should get rid of the psychology of embezzlement, establish a correct consumption concept, strengthen self-prevention, protect our information security, and cherish our lives.

2. An Overview of Telecom Fraud

2.1. The Causes and Essence of Telecom Fraud

In today's era of advanced technology and the rapid development of big data Internet, while it brings us advanced technology and high-quality life, the high development of computers has also led to a new criminal model-telecom fraud network crime. The first step of preventive treatment is to

explore its causes and essence. In the view of big data, with the rapid development of science and technology, electronic products and smart devices have been popularized in the daily production and life of the broad masses of people, constantly optimizing people's lifestyles and production methods, and thus deriving more diversified and anonymous electronic information dissemination methods. Many criminals seized the transition period of this technology and started a series of new cyber crimes. Tracing back to the reasons for the high incidence of its cases, on the one hand, it lies in the low threshold of crime, easy implementation and strong concealment of crime; On the other hand, it is difficult to crack down on such crimes, and the relevant legal system is not perfect, which gives criminals an opportunity. There are three main points.

Low cost and high return. Telecom fraud is a crime with low cost and high return. The fraud method is very simple and easy to spread and imitate. Fraudsters get something for nothing, but live a life of debauchery.

(2) Crime concealment and fraud prevention awareness are not strong. The anonymity and mobility of criminals make it impossible for public security organs to effectively carry out investigation, investigation and evidence collection as in the objective real world, and the crime is quite hidden, which also plays a certain role in protecting criminals. The people's anti-fraud awareness is not strong, fraud is going on every day, and the deceived people want to cry without tears.

(3) The telecommunication network and financial system are not fully responsible. Only pay attention to efficiency, but fail to fulfill the responsibility of management. From telecommunication network On the network level, some telecom network operators and telecom network value-added service providers have not adopted an effective supervision mechanism after subcontracting their services layer by layer [1,2]. Fraud information is flooding the network, and it seems that no one manages and supervises it. From the financial point of view, some banks do not strictly check the batch card opening and entrusted card auditing. Criminals can easily obtain "nameless silver cards" through some channels and throw them away after committing crimes to avoid being pursued.

2.2. Overview of Transnational Telecommunication Network Fraud

The word "cross-border telecommunication network fraud" is widely used in judicial practice. Cross-border telecommunication network fraud evolved from ordinary fraud crime. Ordinary fraud, the criminal can only cheat in a specific area, is a "peer-to-peer" fraud model. With the development of telecommunications and Internet, fraud crime gradually presents new criminal patterns and behavior means, and finally breaks through the geographical restrictions, forming a "face-to-face" and "face-to-face" fraud mode. Generally speaking, the crime of cross-border telecommunication network fraud has gone through several stages, from telecommunications-oriented, to telecommunications-Internet parallel, and then to the Internet-oriented telecommunications supplemented. Cross-border telecommunication network fraud is skillful in design, combining the products of the two eras of telecommunications and the Internet, which breaks through the limitation of time and space and has serious social harm.

The concrete ways to implement transnational telecommunication network fraud include the following aspects: the first is to commit fraud by impersonating identity. Criminals get in touch with the victims by phone messages, pretending to be relatives, friends, colleagues, etc., and falsely claiming that they are in an emergency and then defrauding the victims of money; Or impersonate the personnel of public security organs, judicial organs, banks and other departments, and defraud the victim to transfer money on the grounds that the bank account is suspected of illegal income and needs to be verified. The second is to use mobile phone software to secretly steal the victim's account password. Using the mobile phone virus software developed overseas, falsely claiming that the online banking or U shield and electronic password have expired, defrauding the victim to log on to the phishing website, secretly stealing the password of the victim's bank account, and secretly transferring the funds in the victim's bank account to the criminal suspect's account. The third is to publish false information to defraud the victim's property. For example, send information about winning prizes, paying taxes and making false loans to the victims, and post intermediary information such as

recruitment, studying abroad, selling cars and selling houses on the website to defraud the victims of making money.

2.3. The Characteristics of Transnational Telecom Fraud

Telecommunication fraud is characterized by low crime cost, high illegal income, increasingly sophisticated criminal means, rapid development and growth of crime scale, collectivization, cross-regional and intelligence, which affects social stability and unity and brings great hidden dangers to China's social security. Among them, transnational telecom fraud is more dangerous. First, the collusion between criminal organizations at home and abroad is more prominent. Second, criminal groups are well organized and have a detailed division of labor; Third, the fraud means are diversified and the anti-investigation ability is stronger.

The specific characteristics of transnational telecommunication network fraud include the following aspects: First, the technical means are highly vertical: criminals of cross-border telecommunication fraud use advanced communication technology and network technology to commit crimes. They can modify the calling number through software and use VoIP to make the victim mistake it for a legitimate organ or company's phone. Technical means are highly vertical, making it difficult for victims to be alert. The second is cross-border crime: cross-border telecom fraud criminals often hide abroad and commit crimes across national borders through the Internet. This makes it difficult to trace and detect cases, and transnational cooperation is needed to effectively crack down on such criminal activities. The third is the diversification of money laundering methods: in cross-border telecom fraud cases, criminals usually use diversified money laundering methods to transfer illegal income to various places, which makes it more difficult to pursue the pursuit. They use virtual currency, online trading platform and other means to disperse the funds, making the pursuit more complicated.

3. Criminal Jurisdiction in Transnational Telecommunication Crimes

3.1. Overview of the Basis for Determining the Exercise of Criminal Jurisdiction by Transnational Telecommunications

In view of traditional crimes, even if the scope of criminal activities spans different countries, all parties concerned will stipulate territorial jurisdiction in their respective criminal law systems, so the conflicts caused by territorial jurisdiction are more focused on how to allocate the jurisdiction involved. The fundamental reason for the conflict of criminal jurisdiction in transnational telecommunication crimes lies in the infinity of the Internet and the limited sovereignty of the government. The author looks at the literature and draws several traditional viewpoints in academic circles.

The theory of universal jurisdiction. Universal jurisdiction means that every country has the right to exercise jurisdiction over a few specific international crimes that endanger the common interests of mankind in accordance with international law. There is only one relevant provision of universal jurisdiction in China, namely Article 9 of the Criminal Law. However, the universal jurisdiction stipulated in this article is a supplementary jurisdiction, with universal jurisdiction as a backup option. China can only exercise criminal jurisdiction over relevant crimes within the scope of its treaty obligations. After signing the relevant treaties, countries are given universal jurisdiction over cyber crimes. Universal jurisdiction is based on the conclusion of a convention, which dilutes the influence of the connection point. However, it is more difficult to expand universal jurisdiction rashly, which can even be called a legislative imagination [3].

(2) The theory of actual harm connection. The principle of actual harm connection is a revision of the theory of limited jurisdiction. Only the connection is not enough to determine that a court in a country can have jurisdiction over foreign-related criminals, but also requires that the behavior has actually infringed [4]. Whether a certain jurisdiction has criminal jurisdiction over an act should be judged whether actual harm has occurred. This theory makes the jurisdiction of cyber crime break

away from the virtual space, mainly considering the infringement of specific legal interests, determining the ownership of jurisdiction and eliminating disputes, which has strong rationality.

(3) Network autonomy theory. Cyberspace is forming a society divorced from the state and government, which has its own independent organizational form, value standard and code of conduct [5]. It advocates setting up its own rules system, clarifying the boundaries and scope of jurisdiction, and using the rules of the network to deal with the conflicts of cyber crimes [6]. We should apply equality rules to all actors who enter a certain domain and establish an independent jurisdiction system. However, the theory of network autonomy has great defects-it separates the connection between cyberspace and real national sovereignty and denies the power of real justice; The development of value standards and codes of conduct in cyberspace is unstable, and the codes of conduct and values in cyberspace are weak, so it is difficult to replace the law.

(4) The theory of network address jurisdiction. Advocate the division of jurisdiction according to the location of the website. Because the network address can't be changed at will, it should be done through the Internet service provider, so the website has stability and clarity in a certain period of time, so the location of the terminal server corresponding to the website can exercise relevant criminal jurisdiction.

3.2. The Existing Difficulties in the Exercise of Criminal Jurisdiction over Transnational Telecom Crimes

At present, the failure of the international community to establish a complete and effective prosecution procedure means that domestic legal provisions must be established to supplement and refine the international criminal law. The continuous development of technology has spawned a new type of crime, and international law is not conducive to cracking down on this crime in a timely and effective manner. It is helpful to explore the correct way to analyze the existing difficulties in the exercise of criminal jurisdiction over transnational telecommunications crimes.

First, the dilemma of jurisdiction exercise is the conflict of jurisdiction caused by different principles of determining connecting points. Nowadays, the form of crime is developing in the direction of organization, transnational and high-tech. The limitation of jurisdiction and the infinity of crime place are prominent in transnational telecommunication network fraud. Many places involved can easily lead to repeated investigations and waste judicial resources. Due to the principle of judicial sovereignty, when different countries claim to exercise jurisdiction over the same case based on the principle of personality or territoriality, there will be jurisdictional objections.

(1) Conflicts in territorial jurisdiction of different countries

Although the digital code that constitutes cyber crimes is virtual, the place where cyber crimes occur and the place where they result must be implemented in the physical space. Faced with the impact of new cyber crimes, territorial jurisdiction shows an expanding trend. The state gains the right to regulate network behavior by expanding territorial jurisdiction and strengthens its ability to fight crime. However, expanding the scope of territorial jurisdiction leads to the overlapping of territorial jurisdiction of transnational cybercrime, and the conflict of territorial jurisdiction is inevitable.

(2) The conflict between personal jurisdiction and territorial jurisdiction.

Personal jurisdiction exercises jurisdiction over people who have their own nationality. The conflict between territorial jurisdiction and personal jurisdiction in transnational cyber crime is caused by the actor crossing the border. The network behavior carried out by the actor abroad is related to the social order of the host country, and the host country has the right to exercise jurisdiction according to the principle of territoriality [7]. When a country exercises criminal jurisdiction over its citizens abroad, it often causes conflicts with foreign territorial jurisdiction.

Second, extradition cooperation needs to be further strengthened. Extradition refers to the transfer of criminals or criminal suspects to the requesting country for handling in accordance with extradition treaties concluded between countries or extradition treaties jointly participated. The arrest of criminal suspects must rely on the cooperation between the judicial organs of the two countries for extradition.

Extradition cooperation involves the balance of interests between countries, mutual recognition of the rule of law and mutual trust in sovereignty, so the negotiation process is often hindered. The most efficient way is to rely on bilateral extradition treaties. However, in practice, the legal procedures stipulated in extradition treaties are complicated. In order to crack down on transnational telecommunication network crimes quickly, it is necessary to simplify the legal process and further deepen the extradition cooperation between the two sides.

Finally, the application dilemma of the principle of universal jurisdiction in transnational cybercrime. Criminal jurisdiction can be exercised over the case only on the basis that the crime committed is a serious international crime [8]. The premise of universal jurisdiction lies in the provisions of international treaties. As far as cybercrime is concerned, the rise of the Internet is short, and the global code of conduct for regulating cybercrime has not yet been formed. Judging from the current legislation, the principle of universal jurisdiction has no strong operability in cyber crimes.

4. The Path to Determine the Criminal Jurisdiction of Foreign-related Cybercrime

4.1. Academic Disputes over the Criminal Jurisdiction of Foreign-related Cybercrime

The rapid development of modern network technology brings great challenges to regulators. Network activities are no longer limited by national boundaries and physical space, and the relatively clear boundaries of physical space cannot be copied to virtual cyberspace. Whether jurisdiction based on territorial sovereignty can regulate borderless cybercrime and how to regulate transnational cybercrime has aroused heated discussion in academic circles.

4.1.1 The conflict between the identification of the crime place and the ubiquity of the network

In the cross-regional and virtualized cyberspace, the jurisdiction rules based on the jurisdiction of the crime place are facing great challenges. With the imperfection of the rules of implicated jurisdiction, there are frequent disputes over the jurisdiction of cyber crimes, and designated jurisdiction has become a common practice to determine the jurisdiction of such crimes. However, the vague applicable standards of designated jurisdiction, the arbitrary determination of the case-handling organ and the lack of effective supervision have greatly impacted the statutory principle of jurisdiction, and the cumbersome examination and approval process, delayed the opportunity of investigation and poor connection of procedures can not effectively improve the quality and effectiveness of cyber crimes detection. At present, it is generally completed through loose division of labor and cooperation, and the investigation clues are fragmented and discrete, which determines that it is necessary to deal with the case in time to find out the facts of the crime. Implicated jurisdiction is regarded as the exception of hierarchical jurisdiction and regional jurisdiction, and it is a litigation system that the case-handling organ decides according to its functions and powers in order to realize the purpose of litigation economy.

4.1.2 The interpretation of "crime place" deviates from the principle of legality and lacks regularity and systematization

In response to the need to crack down on cyber crime, six representative judicial interpretations issued in China have expanded the interpretation of "crime place" from different aspects, among which the second paragraph of Article 2 of the Supreme People's Court's Interpretation on the Application of the Criminal Procedure Law of People's Republic of China (PRC); Article 17 of the Procedures for Handling Criminal Cases by Public Security Organs; Article 2 of the Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues Concerning the Application of Criminal Procedure in Handling Cybercrime Cases; Article 4 of the Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues Concerning the Application of Laws in Handling Online

Gambling Crimes; Article 5, paragraph 1, of Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues Concerning the Application of Laws in Handling Criminal Cases such as Telecommunication Network Fraud; The judicial interpretations such as Article 1 of Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues Concerning the Application of Laws in Handling Criminal Cases such as Telecommunication Network Fraud (II) are the most representative.

Although the above judicial interpretation provides an operational solution to the problem of cyber crime jurisdiction in practical departments, it cannot be ignored that this interpretation has gone far beyond the scope of the meaning of the word "crime place". With the increase of judicial interpretation related to cyber crime, there are more and more connection points related to "crime place". The number of existing connection points has increased blindly, and the number and content of connection points in crime sites are set inconsistently by different judicial interpretations, so the jurisdiction of cyber crime has not been systematized.

4.1.3 The traditional view can't adapt to the development of cyber crime

Based on various reasons, the academic circles explain the crime place in different directions, and the traditional view can't adapt to the development of cyber crime. The theory of network autonomy, also known as the new sovereignty theory, holds that the attribute of cyberspace is different from the real space. The borderless, interactive and anonymous nature of the network enables it to expand freely without being constrained by territorial power, and has its own unique organizational form, operating structure and value standards, so it should be given the autonomy of cyberspace. This view has certain desirability, but it can't enlarge the freedom of the network indefinitely. Therefore, this proposition is incompatible with the concept of network sovereignty. This view exaggerates the personality of cyber crime to a great extent. Cyber crime is actually the networking of traditional crimes, and traditional criminal rules are still applicable to cyberspace.

4.2. Practice and Suggestions on the Exercise of Criminal Jurisdiction over Foreign-related Cybercrime in China

4.2.1 Jurisdiction and judicial practice of cyber crime in China

Cybercrime, as a new high-tech crime, criminals often conceal their identity traces by forging domain names of other countries, and the place of crime contains multiple meanings. If it is not clearly defined, countries that are not closely related to crime will also enjoy criminal jurisdiction, thus aggravating conflicts. Taking the use of the Internet to open a casino as an example, according to the Opinions on Several Issues Concerning the Application of Laws in Handling Online Gambling Crime Cases dated August 31, 2010, the principle of taking the jurisdiction of the crime place as the main one and the jurisdiction of the defendant's residence as the auxiliary one should be adhered to. The crime places include the location of gambling sites server, network access, etc.

4.2.2 Suggestions on improving the criminal jurisdiction of foreign-related cyber crimes in China

(1) Improve relevant legislation. Among them, the crime place of foreign-related cyber crimes should be clearly defined, and the scope of jurisdiction should be properly explained in detail. To better provide a basis for establishing the jurisdiction of judicial organs over related cases and coordinate the positive or negative conflicts of jurisdiction.

(2) Combined with more scientific theory, comprehensively determine the criminal jurisdiction of cyber crime. Therefore, the author believes that the special legislation on cyber crimes should be strengthened in combination with the new sovereignty theory. Before the introduction of special legislation, the determination of criminal jurisdiction of such crimes should be comprehensively determined in combination with the specific nature of crimes and related basic principles [9-12].

(3) In the absence of current legislation, if we simply and mechanically adopt one of the specific principles or viewpoints, it will easily lead to dogmatism and improper accountability. Therefore,

joining the international conventions related to cyber crime may strengthen the legislation of cyber crime. In order to actively accelerate the pace of international cooperation and effectively coordinate conflicts of jurisdiction, China should actively participate in the drafting or signing of relevant international legal documents or conventions. Provide legal basis for extradition measures in case of conflict of jurisdiction.

5. Foreign-related Network to Help Criminals Convicted and Sentenced

5.1. The Identification of Aiding Criminals in Foreign-related Cyber Crimes

Telecommunication network fraud is committed by many gangs and groups, and the main organizational forms are fraud gangs and fraud groups. The principal offenders in fraud groups are divided into ringleaders and other principal offenders, and the accomplices are divided into accomplices and accomplices. The criminal subjects bear different responsibilities because of their different roles in the occurrence of criminal results. Knowing that others commit telecommunication network fraud and helping to withdraw money after conspiring in advance constitutes a crime of concealing and concealing, and conspiring in advance or helping to withdraw money occurs before the end of the act, which constitutes an accomplice to fraud and is usually recognized as an accessory to help.

5.2. Identification of Accessory and Coerced Accessory in Foreign-related Cyber Crimes

First, instigation can be oral or written. It can be expressed or implied, but the content of instigation must be specific and clear; Second, the behavior of aiding criminals can be either action or omission, but the behavior of abettors is only action. Third, the crime of assisting in organizing prostitution is not the crime of helping the offender to become a principal offender (conviction and sentencing are independent), but the crime of helping the offender to become a relative principal offender (whether the helping act is an act of execution depends on the infringement of the legal interests of the helping act itself); Fourth, the crime of helping information network criminal activities is not the principal offender, but the principal offender in sentencing (conviction series, sentencing independence); Fifth, those who instigate others to realize their existing criminal intentions and promote their existing crimes in advance are instigators; Sixth, anyone who instigates others to delay the realization of the existing criminal intention and reduce the existing charges is not guilty; Seventh, it is to help the offender to strengthen the existing intention of others.

5.3. Sentencing Rules for Aiding and Abetting Foreign-related Cyber Crimes

Knowing that others use the information network to commit crimes, providing technical support such as Internet access, server hosting, network storage, communication transmission, or providing assistance such as advertising promotion, payment and settlement, if the circumstances are serious, they shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall also or shall only be fined. It can be based on: Article 287 bis of the Criminal Law of People's Republic of China (PRC): [Crime of helping information network criminal activities] knowing that others use information network to commit crimes, providing technical support such as Internet access, server hosting, network storage and communication transmission for their crimes, or providing assistance such as advertising promotion, payment and settlement. If the circumstances are serious, they shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention, and shall also or shall only be fined. If a unit commits the crime mentioned in the preceding paragraph, it shall be fined, and the directly responsible person in charge and other directly responsible personnel shall be punished in accordance with the provisions of the first paragraph. Whoever commits the acts mentioned in the preceding two paragraphs and constitutes other crimes at the same time shall be convicted and punished in accordance with the provisions of heavier punishment.

The constitutive elements of helping the network information crime are: the subject of the crime-the subject of this crime is the general subject, the natural person with criminal responsibility ability, and the unit can also become the subject of this crime; The subjective aspect of this crime-knowingly helping others commit information network crimes, will cause damage to the country's information network management order, and still hope or let this harmful result happen. This crime also requires that the perpetrator must know that others are using the information network to commit crimes, and the perpetrator knows or should know; The object of crime-the object of this crime is the state's management order of the normal information network environment. The use of information networks to commit crimes destroys the stable, healthy and orderly information network environment. And the behavioral impact of helping these information network criminal activities is the same as above; The objective aspect of this crime-providing technical support such as Internet access, server hosting, network storage and communication transmission for information network crimes, or providing help such as advertising promotion and payment settlement, is a serious act.

6. Conclusion

How to legally and reasonably solve the national criminal jurisdiction disputes in foreign-related cybercrimes is a sufficient condition for effectively punishing transnational crimes and international crimes, which is related to the interests of the community of world destiny. From the definition and nature of telecom fraud. Starting with the characteristics, subjects and legal principles of foreign-related cybercrimes, this paper analyzes the origin of criminal jurisdiction conflicts. And with the complexity of the connecting factors such as the country of jurisdiction and the crime place of cybercrime, it is impossible to give priority to the principle of personal jurisdiction, territorial jurisdiction, protective jurisdiction or universal jurisdiction, which is the core legal issue of this paper. In order to solve the criminal jurisdiction disputes in foreign-related cybercrimes, we should not only apply the principles of territorial jurisdiction, personal jurisdiction, protective jurisdiction and universal jurisdiction mechanically, but also apply the more representative theories such as universal jurisdiction, actual harm connection principle, network autonomy principle and network address jurisdiction principle after in-depth analysis of the connecting factors such as the location of crime, transnational crime and cybercrime. They have no applicable priority, and the attribution of jurisdiction can be determined more accurately and reasonably in combination with specific circumstances. For emerging cybercrimes, it is necessary to make a comprehensive judgment based on territorial jurisdiction, supplemented by personal jurisdiction, real harm connection and network autonomy. Taking foreign-related telecom fraud as a breakthrough, we should actively solve the conflict of criminal jurisdiction of foreign-related cybercrimes, and explore the path of determining criminal jurisdiction of foreign-related cybercrimes in China from the aspects of perfecting relevant legislation, comprehensively determining criminal jurisdiction of cybercrimes, actively accelerating the pace of international cooperation, effectively coordinating jurisdiction conflicts, and continuously strengthening the ability of domestic judicial organs to perform their duties.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

- [1] Li Li. Research on Several Issues of Telecommunication Fraud Crime. Lanzhou University, 2018.
- [2] Yichao Gao. Countermeasures Research on Punishing and Preventing Telecommunication Fraud Crimes. Tianjin University, 2018.
- [3] Tianshui Zhao. Criminal Jurisdiction of Foreign Cybercrime. Journal of Jiangsu Police College, 2023, 38(03): 34-42.

- [4] Zhigang Yu. Reflections on Criminal Jurisdiction in Cyberspace. Chinese Jurisprudence, 2003,6.
- [5] Tianshi. Comparative study of criminal universal jurisdiction legislation. Journal of Chongqing Three Gorges College, 2023.
- [6] Zhang Ting, Chen Li. Application Dilemma and Solution of Criminal Jurisdiction in Transnational Cybercrime. Journal of Central South University for Nationalities (Humanities and Social Sciences Edition).
- [7] Yu Su. Conflict and Resolution of Transnational Cybercrime Jurisdiction. East China University of Politics and Law, 2021.
- [8] Dongjie Han. On National Criminal Jurisdiction Conflicts and Their Resolution. Shenyang University of Technology, 2018.
- [9] Ting Tan, Le Yue, Xianmin Li. Determination of Criminal Jurisdiction for Foreign-Related Cybercrime. People's Procuratorate, 2018(07): 62-65.
- [10] Qiang Meng. Study on the Conviction and Sentencing of Helping Offenders of Telecommunication Network Fraud Common Crimes. Journal of Wuhan Public Security Cadre College, 2018, 32(01): 60-62.
- [11] Olawale Surajudeen Adebayo, Joshua Bulus Micah, Ganiyu Shefiu Olusegun, et al. Development of Secure Electronic Cybercrime Cases Database System for the Judiciary.
- [12] Veena K., Meena K., Kuppusamy Ramya, Teekaraman Yuvaraja, et al. Cybercrime: Identification and Prediction Using Machine Learning Techniques.