The Dilemma of Telecommunication Fraud Crime——An Analysis of China's Governance Model as a Sample

Hanrui Gong*

Criminal Justice School, Zhongnan University of Economics and Law, Wu Han,430073, China

Abstract. In order to promote the international cooperative governance of telecommunication fraud crime and optimize China's legal issues on this crime, this paper takes China's governance model in telecommunication fraud crime as the analysis sample, and proposes the optimization path of governance of telecommunication fraud from both domestic and foreign aspects by analyzing the current shortcomings of China's domestic legislation, law enforcement, and judicature, as well as the problems in international cooperation such as off-site evidence collection and criminal judicial assistance.

1 INTRODUCTION

In the Internet era, traditional cybercrime is accelerating to new cyberspace crime transformation and spread. The emergence of "non-contact" crimes makes the cost of crime greatly reduced, and the most typical crime is the telecommunication fraud crime. Telecommunication fraud is a new expression of traditional fraud crimes in the telecommunication network space. From a jurisprudential perspective, the telecommunication fraud crime is defined as the criminal act of sending false messages to an unspecified majority of people through telecommunication communication technologies such as fixed telephones, cell phones, computer networks and their derivative technology products for the purpose of illegal possession, and the victim is thus duped and delivers the corresponding amount.

Telecommunication fraud crime has significant social harm because of the following reasons. First, the main body of telecommunication fraud crime often adopts the form of gang work, with a mature class of corporate management mechanism, forming a tightly organized chain. Second, the means of telecommunication fraud crime are usually non-contacted, and show a trend of diversification, technology and concealment. Third, a large number of cross-regional/border telecommunication fraud cases have emerged, making it much more difficult to govern for many countries. Based on this, it is of great practical significance to identify the key issues and study the mode of optimizing the governance of telecommunication fraud crimes.

Table 1. data on the progress of work to combat telecommunication fraud crimes

	Number of detected cases	**Number of suspects apprehended**	
2020	307,000	359,000	
2021	394,000	634,000	
		210,000 offshore (36,000 in Southeast Asia)	424,000 in the territory
Rise rate	28.5%	76.6%	

Source: China's State Council Information Office, 14/04/2022

As can be seen from Table 1, the number of telecommunication fraud crimes and the groups involved in China are extremely large. Currently, mainland China upholds a strict governance philosophy for telecommunication fraud crimes. Legislatively, the statutory maximum penalty for telecommunication fraud crimes under the mainland criminal law is life imprisonment with confiscation of property, which is far heavier than the statutory maximum penalty of only seven years for fraud crimes in Taiwan. In law enforcement, the public security authorities, financial institutions, telecom operators and other parties are cooperating closely, through the "Card-Blocked" action (i.e. an action that blocking criminals from illegally obtaining telephone and bank cards to prevent them from committing crimes such as telecommunication fraud) and other measures at the source, striving to achieve the elimination of telecommunications fraud crime. At present, this governance model has achieved good results. In 2021, China's public security organs, together with the Supreme People's court, the Supreme People's Procuratorate, the Ministry of industry and information technology, the

* Corresponding author: gonghanrui@stu.zuel.edu.cn

people's Bank of China and the three major telecom operators, continued to promote the " Card-Blocked " action, eliminating 42,000 illegal and criminal gangs who illegally selling telephone and bank cards, investigating and punishing 440,000 suspects, punishing 200,000 dishonest people, and punishing 41,000 business outlets and institutions. In addition, China has been issued the "Telecommunication Fraud Governance Research Report" every year since 2019 to study telecommunication fraud governance in depth.

In summary, it is of typical significance to take China's telecommunication fraud governance as a sample for analysis. The study of the governance dilemma of telecommunication fraud crime in China domestically and internationally can, on the one hand, help find an optimal path for China itself in legislation, law enforcement and judicial issues involving telecommunication fraud, and on the other hand, provide reference for other countries in order to promote the global collaborative governance of telecommunication fraud crime.

2 CHINA'S TELECOMMUNICATION FRAUD DOMESTIC GOVERNANCE DILEMMA

2.1 Legislation

At present, the telecommunication fraud crimes in China are mainly reflected in the part of the Criminal Law, as well as some judicial interpretations and other legal norms. Although the Chinese criminal law has established a large number of crimes involving telecommunication fraud, and the provisions are being supplemented and improved through the issuance of judicial interpretations in recent years, the boundary between telecommunication fraud crime and the other crimes is still not clear. Meanwhile, the principle of using one crime versus several crimes in the law has not yet established a perfect rule of application in telecommunication fraud crime.

Apart from fraud crime under Chinese criminal law, there are also crimes of facilitating criminal activities in information networks, concealing the proceeds of crime, infringing on citizens' personal information, obstructing credit card management, trading in official documents and seals of state organs, smuggling across the state border, and illegal use of information networks. In 2021, nearly 130,000 people were prosecuted for the crime of helping information network criminal activities, up more than 8 times year-on-year, ranking the 3rd in all types of criminal offenses and becoming the first major crime in the chain of telecommunication fraud crimes. In the judicial interpretation, Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues of Applicable Law in Handling Criminal Cases of Telecommunication Fraud have provided for specific circumstances of telecommunication fraud, especially stating that "by sending SMS, making telephone calls or using the Internet, radio and television, newspapers and magazines, etc. to publish false information, to commit fraud on an unspecified majority of people," the form of telecommunication fraud crime can be punished severely as appropriate. In addition, "sending more than 5,000 fraudulent messages" and "making more than 500 fraudulent phone calls" can also be considered as aggravating circumstances.

Because the charges involved are too miscellaneous, the judicial organs of the legal application of telecom network fraud will be different due to the different understanding of the legal provisions, will cause the charge is uncertain. Although Opinions of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Several Issues of Applicable Law in Handling Criminal Cases of Telecommunication Fraud (II) have been especially connected with some of the above crimes, the connections between the crimes have not yet been fully covered. And there is a greater difficulty in determining whether the crime of infringement of citizens' personal information is connected with the crime of fraud, judging whether there are legal articles competitive and imaginary application between fraud and other crimes [1]. As a result, there is a potential risk of different judgments in the same case for telecommunication fraud cases, which is not conducive to the maintenance of judicial authority and justice.

The reason for the above situation is that China's legislation lacks a unified approach to ranking the legal interests of such crimes [2], which makes it impossible for the judiciary to accurately identify and reasonably rank the legal interests when facing the crime of telecommunication fraud. In fact, special means for perpetrators to commit crimes such as sending SMS, making phone calls, using internet and other telecommunication technologies, which directly determines the diversity of legal interests infringed by telecommunication fraud crimes, and in turn leads to the accurate characterization of different perpetrators and the application of the crime in different criminal situations. If the rank of such crimes against legal interests can be ranked uniformly in legislation, the difficulties of such crimes in judicial practice would be overcome well.

2.2 Law Enforcement

In the management of telecommunication fraud, it is not only the law and the coercive power of the public security agencies and law authorities that are relied upon, but the cooperation of all sectors of society is also crucial. China's public security authorities are cooperating with financial institutions, communication service companies in the fight against telecommunication fraud, focusing on the implementation of the "Card-Blocked" action issued by the central government. In terms of financial institutions, banks and other key initiatives have adopted a real-name system for card issuance, big data networking for comprehensive information monitoring, limiting the number of cards issued, and paying attention to whether the details of fund transactions match the actual economic status of card issuers. In terms of communication services, the linkage and cooperation between the police and communication service companies is extremely close: for

the numbers involved in cases notified by the public security department, the communication service companies will complete the task of shutting down or inquiring related information in a timely manner, and provide timely feedback to the police. The above-mentioned cooperation mode has greatly enhanced the efficiency of the public security departments in investigating and combating telecommunication fraud.

But even though the Chinese government has now explored a model of law enforcement that links the police with third-party forces in society, with remarkable results, there are many new problems. In the process of the above-mentioned investigation, the from-case-to-person investigative path is very stable, not only forming a certain solid thinking, but also leading to the fact that it is not conducive to the flexibility of law enforcement for individual cases.

According to previous research results of the grassroots public security bureaus and the People's Procuratorate, it has found that in the process of promoting the "Card-Blocked" action has undoubtedly limited the number of bank cards, as a result, the action now leads to two new forms of crimes: 1. The staff of financial institutions use their positions to issue cards and resell them for profit by fraudulently stealing customers' ID cards in the course of their work. 2. There are people still lend their bank cards to others and usually charge them by hour. In summary, the investigation of the choice of the inherent ideas in the path can be explored again. The law enforcement agencies can start from the position of internal personnel, trying to adopt the from-person-to-case method of investigation.

At the same time, the difficulty in enforcing the law lies in the fact that although a governance chain has been formed with the participation of banks and telecommunication departments led by the public security authorities, the general participation of the society and the understanding of the "Card-Blocked" action are still not enough. According to the results of the questionnaire survey collected by author in 2021, more than half of the Chinese people (51.43%) do not know about the "Card-Blocked" action. The loss of the people's attention and response to the issue will directly lead to the lack of in-depth control of telecommunication fraud crimes and make it difficult to eliminate the root cause of the crime.

2.3 Judicature

The difficulty of China's domestic governance in judicature mainly lies in the examination of electronic evidence. Evidence examination refers to the judicial organ's examination and verification of evidence according to law. It is also a key link in the process of China's continuous promotion of the substantiation of court hearings. Its core content is to establish the central position of the trial, fully implement the cross-examination of evidence, find out the facts of the case on the basis of the full opinions of the prosecution and the defense, and form the reasons for the judgment in the court. To improve and perfect the admissibility rules of evidence, the judge needs to argue in the judgment whether and how various kinds of evidence are admissible to determine the facts of the case and the applicable laws. In Telecommunication fraud cases, the evidence is mostly in the form of electronic data, which is different from the traditional evidence. According to the three requirements of effective evidence (authenticity, relevance and legality), electronic evidence must always remain substantially identical and available throughout the whole process of evidence collection and review. Once the electronic evidence is contaminated, its authenticity will cause irresistible doubts, which will have a serious impact on the judges' review results.

In addition, due to the fact that electronic data forensics involves high-tech technology and professional skills, most of the investigators, prosecutors and judges lack knowledge in relevant aspects and judgment in the authenticity review of electronic data. In judicial practice, relevant professionals are generally employed for consultation, the appraisers are required to give identification on the electronic data, and the procuratorial technical department is entrusted to provide technical assistance. However, the officials are extremely passive in the process of electronic data handling. They are easy to be manipulated and deceived because lack of certain electronic knowledge. Take the case No. 67 of the Supreme People's Procuratorate of the people's Republic of China as an example. The structure, database and source code of the electronic data of such application programs involved in the online banking operation records need to be identified by a certain judicial identification institution. As a result, whether the public security organs are extracting electronic data in investigation, or procuratorial authorities and judges are identifying the authenticity of electronic data, they are all required to refer to or even rely on expert advice. In that case, the cases related to electronic data are now lack of "substantive review", and the supervision and control of the impartiality of expert opinions has become an urgent issue.

3 CHINA'S TELECOMMUNICATION FRAUD INTERNATIONAL COOPERATION DILEMMA

Due to the cross-border phenomenon of telecommunication fraud crimes, different countries and regions have different laws and law enforcement level. Although all countries involved have jurisdiction, no single country can deal with cross-border telecommunication fraud crimes alone. Existing international law enforcement suffers from difficulties in mutual recognition of evidence due to different procedures of investigation and evidence collection among police in different countries, insufficient extradition treaties in force, complicated extradition procedures, and so on [3].

3.1 Off-Site Evidence Collection In International Police Cooperation

The problem of off-site evidence collection in international police cooperation is quite prominent, mainly

lied in the following two aspects:

First, the collection procedures are not uniform due to the different laws of various countries. The rules for extracting and collecting evidence in the target country are different from those in China. Its forensics technology and case handling ideas will affect the quality of case evidence collection, bringing about problems such as collecting evidence untimely and having difficulty in transformation and certification. The time for cross-border crime fighting is relatively slow, and the police are often at a disadvantage in case evidence collection.[4] In order to avoid the exclusion of illegal evidence in international police cooperation, it is necessary to pay strict attention to the procedural requirements of evidence collection. As a result, the police can only freeze and seize the property involved in the case, such as computers, at a later stage, which greatly reduces the efficiency of case handling and is not conducive to the preservation of evidence. To sum up, it is difficult to meet the needs of combating such crimes. In addition to the time-lag problem of collection, getting approval for authority to search in a timely manner is also a major challenge. The places where telecommunication fraud is carried out, the residences and vehicles of the persons involved, etc. usually need to be investigated and searched for evidence. However, the provisions on search vary from country to country in terms of law: some require the authorization of judges, only in case of emergency like if the investigation organ does not immediately take search measures and may delay the investigation, can the police conduct the search, and some has no provision on searching without a license. Such evidence, collected in a manner inconsistent with Chinese law, will be an obstacle in the review process. It is rising a doubt about the legality of such evidences: whether the examination should be conducted in accordance with the laws and regulations of the target country or China. In summary, improving the development of international law enforcement cooperation and the refining specific regulations on the collection of evidence abroad are conducive to balancing the interests of both China and the countries.

Secondly, the fragile characteristic of electronic data inherently makes it quite difficult to collect remotely. There are two main types of collection: one is seizuring and freezing to obtain the case of physical evidence, documentary evidence, electronic data and audio-visual information through the conventional on-site investigation and inspection, another is conducting a remote electronic investigation by directly accessing the Internet to the computer used by the criminal gangs in the commission of the crime. The latter method is in principally equivalent to the rules of remote retrieval and collection of electronic data in China, mainly conducted by Chinese criminal technicians or commissioned institutions in accordance with China's laws and regulations. All that is required is for the subject country to assist the police in opening an international port to access the computer involved in the case so that the police can conduct remote investigations. However, due to the vulnerability brought about by electronic data itself, professional telecommunication fraud gangs usually install one-click destruction programs in electronic devices, leading to a steep

3.2 Criminal Legal Assistance

International criminal judicial assistance is essentially a rule of law cooperation, in order to achieve the purpose to make smooth convergence of the rules of operation between countries, rather than the reconstruction of the law itself. The legal rules of China and overseas or extra-territorial regions are significantly different, so that they have different legal systems respectively. To be specific, they differ greatly in terms of legal operation mechanism, crime system, criminal law norms and law enforcement procedures, which reduces the enthusiasm of participants to cooperate. Thus, to help smooth the channels of criminal judicial assistance and promote cross-border law enforcement cooperation with the system is the top priority in combating international telecommunication fraud crimes.

Take China and Southeast Asian countries as an example. In terms of the number of treaties on criminal judicial assistance, as of April 2021, according to the data of the treaty database of the Ministry of foreign affairs, among the 11 countries in Southeast Asia, China has signed treaties on both criminal judicial assistance and extradition with Thailand, the Philippines, Indonesia, Laos and Vietnam, treaties on single criminal judicial assistance with Malaysia, treaties on single extradition with Cambodia [5]. Therefore, from the perspective of the coverage of countries that have signed treaties on mutual legal assistance in criminal matters and extradition treaties, it only accounts for about half. In terms of the content of criminal judicial assistance, the content is still based on traditional investigation measures such as questioning witnesses and victims, interrogating suspect, conducting identification and judicial investigation. The online extraction and remote investigation of electronic data often involved in cross-border network crimes are still basically blank. At present, there is also a lack of specific provisions on the recovery and return of funds involved in cross-border cybercrime, which leads to the dilemma that even though the amount of funds involved is very large, the probability of recovery is contrarily low.

With ASEAN overtaking the EU as China's top trading partner by 2020, China is still in a situation where it has concluded treaties with Southeast Asia. There is a large gap in international judicial assistance between China and other countries at this stage.At present, according to the data provided by the treaty database of the Ministry of foreign affairs, there are only 20 countries in the field of judicial assistance [6]. Under the background of international trade, the channels of international law enforcement cooperation should be sufficient, but it still needs to expand its scope and depth by further promoting criminal law assistance with various countries. By doing so, an appropriate situation of international common governance can be eventually formed.

4 CONCLUSION

To sum up, we have to start the optimization path of governance against telecom fraud crime from both domestic and foreign aspects.

Nationally, China needs to first clarify the doctrinal and practical issues in the legal provisions involving telecommunication fraud, in order to improve the relevant judicial interpretations as soon as possible. For example, establish detailed rules applicable to telecommunications network fraud crimes when they compete with related crimes such as crime against personal information, fraudulent crimes etc. Only if China unifies the application of the law, can it provide strong judicial protection for grassroots rule of law personnel. At the same time, the law enforcement agencies still need to increase their efforts to carry out "Card-Blocked" action since the reduction of crime rate showcased that the action has already initial results. To deal with the emergence of new crime tactics, the officials should flexibly adjust the investigation strategy and achieve effective linkage between social agencies, gaining the support of the public to achieve full social coverage. Judicial decisions should also strive to promote the substantive review of electronic data and other non-traditional evidence by judges. Apart from that, at social level, all sectors of society should establish awareness of the rule of law to protect their legal rights, while adhering to the concept of governance at source, forming a benign atmosphere of mutual supervision. So that all forms of strengths can be focused on killing crime in the cradle.

Compared with other countries in the world, China has successfully achieved in the legislation and law enforcement of telecommunication fraud crimes. Its legislation fully reflects the criminal policy of strict control of telecommunication fraud cases, which sets high legal penalties to meet the original purpose of protecting the legal interests of criminal law and achieving the purpose of crime prevention by penalties. In terms of law enforcement, in addition to the establishment of internal investigation platforms and a five-level investigation mechanism of district, county, city, province and central government, the public security organs also establish a joint coordinating body with financial institutions and telecommunications sectors. It successfully carries out "Card-Blocked" action, effectively reducing the number of telecommunication fraud. China should make use of its own successful experience, and such measures and related technical means can also be exchanged with other countries with high incidence of telecommunication fraud. This would help strengthen international police cooperation as well as improve the efficiency of telecommunication fraud case prevention globally.

On the basis of promoting China's own experience and driving countries to link up to tackle telecommunication fraud crimes, it is also necessary to establish an efficient international police cooperation and criminal judicial assistance mechanism based on bilateral and multilateral agreements and respecting the national judicial sovereignty of participating countries, so as to jointly overcome the difficulties of police evidence collection in different places and broaden the breadth and depth of criminal judicial assistance. In addition, apart from improving the existing system, it is also necessary to innovate the "China-International cooperation mechanism against telecommunication fraud ", including information research, exchange and sharing, personnel training and team building between countries.

References

1. Liu Chunyan. Research on some issues of the number of crimes of telecommunication network fraud [J]. Journal of Guizhou Police Academy,2022,34(03):113-121.DOI:10.13310/j.cnki.gzjy.2022.03.015.
2. Zhang Hong. Research on the legal prevention of telecommunication network fraud crimes from the perspective of the criminal law system [J]. Journal of Southeast University (Philosophy and Social Science Edition), 2022,24(S1):82-88. doi:10.13916/j.cnki.issn1671-511x.2022.s1.014.
3. Wang Zhengyu,Zhu Xiaowei,Chen Saijun. Exploration of international police cooperation mechanism for non-contact crimes[J]. China Criminal Police,2020(05):55-59.
4. Liu Daoqian. Problems and countermeasures of international police cooperation in combating cross-border telecommunication fraud [J]. Crime Research,2019(06):50-57.
5. Zhuang Hua, Ma Zhonghong. Study on cross-border cybercrime and governance of Chinese citizens in Southeast Asia[J]. Nanyang Qishu, 2021(04):41-54. DOI:10.14073/j.cnki.nywtyj.2021.04.004.
6. Wu Zhaomei. An offshore examination of telecommunication network fraud crimes [J]. Journal of Wuhan Public Security Cadre College,2020,34(02):65-67.