Advances in Computer Science Research, volume 65

3rd International Conference on Communications, Information Management and Network Security (CIMNS 2018)

Confusion and Relief of Criminal Jurisdiction of Cybercrimes

Jun Li[1, 2, *] and Jidong Jia[1]

[1]School of Law, Huazhong University of Science and Technology, Wuhan, Hubei, China, 430074
[2]Criminal Justice School, Zhongnan University of Economics and Law, Wuhan, Hubei, China, 430073
[*]Corresponding author

***Abstract*—Nowadays cybercrime occurs more and more frequently. However, the traditional criminal jurisdiction system has certain difficulties in investigating it due to the particularity of cybercrime, especially in the criminal jurisdiction of transnational cybercrime. It has seriously restricted the effective punishment of cybercrime by the international community. The key to effectively resolve the conflict of jurisdictions is keep the premise of adhering to the concept of national sovereignty in cyberspace.**

Keywords—cybercrime; criminal jurisdiction; district jurisdiction; international cooperation

I. DETERMINING THE PREDICAMENT OF CRIMINAL JURISDICTION

Cybercrimes are increasing with the development of computer information technology and the popularity of the Internet. The particularity of cybercrime makes it more difficult to investigate and the situation is getting more severe [1]. As pointed out in August 2017 by the Chief Prosecutor of the Supreme People's Procuratorate, Jianming Cao at the BRICS Attorney General's Meeting: due to the particularity of the network, it is difficult to identify the subject for cybercrime, and hard to detect or collect evidence such as electronic evidence. The cost of fighting crime is high, and the jurisdiction is conflicted. Among them, the issue of jurisdiction may be the biggest problem in dealing with transnational cybercrime in addition to evidence [2]. At present, there is no specific legislative provision for the criminal jurisdiction of cybercrime in China [3]. Therefore, the research on this issue is not only of theoretical significance, but also a realistic problem that needs to be solved urgently in China's judicial practice.

Cybercrime has the characteristics of strong concealment, low crime cost, wide coverage, large number of victims, and great social harm. Compared with traditional crimes, the virtuality and borderlessness of cybercrime make it difficult to confirm criminal jurisdiction [4].

A. The Challenge on Criminal Jurisdiction Brought by Virtuality

The essence of cyber-criminal jurisdiction is that the cybercrime space is completely different from the traditional criminal space. The traditional criminal space refers to the physical space in which the perpetrator carries out the criminal act. The traditional criminal act is realistic and is three dimensional. Therefore, the traditional criminal law's jurisdiction over crime is based on the physical space of reality. In the criminal jurisdiction, the traditional criminal law adopts the jurisdictional theory mainly based on the territorial jurisdiction, while assisted by the principle of personality, the principle of protection and the principle of universal jurisdiction. The so-called territorial jurisdiction is also the "four-space theory" of the traditional criminal jurisdiction theory that is territorial waters, airspace and proposed territories. Therefore, cyberspace does not belong to the "four spaces" of traditional criminal jurisdiction theory. Some scholars refer to this space as the "fifth space." [5] Therefore, the crime of the fifth space, which occurs outside the country and not directly against the citizens of the country, so traditional criminal jurisdiction supplemented by the principle of human or protection is obviously difficult to cover. In addition, the virtual nature of cybercrime is also manifested as the concealment of criminal tools, criminal acts, and criminal consequences. The objectively visible material tools in the real world are often achieved by tapping the keyboard and mouse in cybercrime; after the cybercrime, there will be no physical traces such as fingerprints, footprints and bloodstains. These will undoubtedly increase the difficulty of investigating cybercrime.

B. The Challenge on Criminal Jurisdiction Brought by Borderlessness

The jurisdiction of the law is based on a relatively stable connection. One of the theoretical foundations of traditional territorial jurisdiction is that one or both of the acts or results of the crimes should be in a certain jurisdiction, that is, it has a relatively stable relationship with a physical space. The cyberspace is a digital virtual space that uses the network to exchange information. The online address is not necessarily related to the real space. For the space of traditional crime, the territorial land, territorial waters, airspace and mobile territories all have certain boundaries and fixed scopes. Naturally, it is easy to distinguish whether a certain cybercriminal act occurs in or outside China. The cyberspace is different. The entire network world is like a vast interstellar space. The boundaries between physical features such as sea, land and air are blurred. The region is no longer meaningful in cyberspace. Anyone can use their computer to connect to the Internet to attack the computer systems of citizens of other countries in the world without leaving home. For example, the WannaCry ransomware incident that ravaged the world in May 2017, The breadth of its coverage is the most cybersecurity incident in recent years. According to information released by well-known cyber security agencies, as of May 17, 2017, more than 150

countries and regions in the world, more than 300,000 computers were blackmailed, and the ransom has reached 72,000 US dollars [6]. The scope of its influence and the number of countries involved are far from comparable to traditional crimes. On the one hand, the globality and uncertainty of cyberspace make a network behavior unable to point to a certain jurisdictional factor, thus making the relationship between network behavior and traditional jurisdictional basis uncertain. On the other hand, cyberspace, as a global whole, has the characteristics of virtual and intangible, and it is impossible to divide it into jurisdictions as physical space. Then, the traditional criminal law regional jurisdiction theory which is applicable to the "four-space theory" is difficult to cover the "fifth space" of computer networks. Because the boundaries of criminal jurisdiction are vague and cybercrime may cross the globe, it may lead to multiple countries claiming jurisdiction over the same criminal case, resulting in conflict of jurisdiction.

Therefore, the challenge to the space and scope of traditional criminal law brought by cyberspace is omnidirectional and multi-leveled. Due to the borderlessness, decentralization of cyberspace, and the virtual nature of crime scenes and space, inter-regional conflicts are intertwined with international conflicts at the time determining the jurisdiction, thus make the determination very difficult [7].

II. The Debate On Theory Of The Criminal Jurisdiction Of Cybercrime And Corresponding Response

On the issue of how to get rid of the dilemma of criminal jurisdiction of cybercrime, scholars in the criminal law community proposed the theory of jurisdiction different from traditional criminal jurisdiction. At the same time, national legislation also responded to this issue.

A. Virtual World Sovereign Independence Theory

The theory holds that virtual space sovereignty does not belong to any country, nor is it possible for any country to violate it. It is not appropriate for countries to enact domestic laws to regulate them. In addition, the legal jurisdiction of the real world does not go beyond the boundaries demarcated by national borders. The virtual world has no national borders at all or the national border of a country does not include virtual space at all. This situation also makes it difficult for countries to formulate laws for virtual space. This doctrine fundamentally denies the state's criminal jurisdiction over cybercrime, and its substantive academic support is the theory of cyber liberalism. However, in recent years, cybercrime has begun to seriously endanger public safety and public life and property security. The security problems brought by the Internet have increasingly attracted the attention of governments around the world. Judging from the responses of countries around the world, the international community has generally accepted the concept of "cyberspace sovereignty" and believes that the state's involvement in cyberspace is justified. Most countries are trying to solve the criminal jurisdiction of cybercrime through legislation. For example, in the Computer Crimes Act of 1990, the United Kingdom provides that if the victim or offender in the case is in the United Kingdom, the English courts have jurisdiction over the offences covered by this Act [8]. In addition, the long-arm jurisdiction rule applicable to US cybercrime is also a typical example [9].

B. Network Autonomy Theory

The main content of the theory is that cyberspace is a special region and should exist as a new jurisdiction outside the sovereignty of the state, just as the high seas, the international seabed region and Antarctica. Any country can govern and apply its laws to any activity of anyone within cyberspace. Cyberspace needs to create its own legal institutions and laws. In the cyberspace disputes, actors can appear in specific courts through network contacts, and court decisions can also be enforced through the Internet. Many scholars have criticized the theory, saying that the doctrine subverts the basic position that the cyber world should be exercised by sovereign states, and construct new jurisdictional rules away from national sovereignty. Are all sovereign states willing to renounce or transfer their jurisdiction of cyberspace? In the absence of national coercive protection, can cyberspace function as a criminal jurisdiction? These are the problems faced by the network autonomy theory. Obviously, this theory lacks a legal basis and is not operational in practice [10].

C. Expanding the Theory of Territorial Jurisdiction

The theory holds that the "domain" of traditional criminal law can be extended to the fifth space with restrictions. Some scholars have argued that: first, the terminal equipment and the server establishment site for online crimes are within the first, second, third and fourth space of the country. 2. The intruded system LAN or terminal equipment is within the first, second, third and fourth space of the country. 3. The terminal that the actor obtains and displays the information of the online crime result is located in the space of the first, second, third and fourth space. That is, by interpreting the principle of territorial jurisdiction in the existing criminal law theory, the standards of criminal behavior and the place of crime are appropriately expanded to achieve jurisdiction over a cybercrime. But the theory still cannot solve the conflict of jurisdiction fundamentally. Because of the over-expanded territorial jurisdiction, all crimes in a networked environment become global crimes in which all countries have universal jurisdiction, leading to a positive conflict of jurisdiction.

D. Limited Jurisdiction Theory

This theory is the most representative theory put forward by the criminal law scholars in China, and has won the support of many scholars. The theory holds that, on the basis of personal jurisdiction, the existence of criminal jurisdiction should be determined by the fact that whether the criminal act violates or affects the relevance of the country or its citizens. If there is an relevance, then it has criminal jurisdiction; if there is no relevance, it does not has criminal jurisdiction. The specific meaning of relevance is that the criminal action has already formed a practical infringement or influence on the country or citizen, that is, it already had direct contact with the country or citizen.

E. Principle of Physical Contact Theory

The theory is modified based on the aforementioned limited jurisdiction theory. The theory holds that the mere connection

is not enough for jurisdiction. The actual damage caused by the cyber behavior to the legal interests should be used as the criterion for judgment in determining whether a field of law has criminal jurisdiction over a cybercrime. The "relevance" criteria of the principle of limited jurisdiction are very vague and often rely on the discretion of judges. The principle of physical contact theory is more applicable to the types of crimes that can be specifically judged by facts, specific dangerous criminals, etc., and can also solve the jurisdictional problem of network signal "abstract crossing" [11]. However, in practice, "practical harm" itself is a very abstract concept, so this theory will still lead to positive and negative conflicts of criminal jurisdiction.

F. The Source Country Theory

The theory holds that the jurisdiction of cybercrime should be determined based on website. Compared to the range of activities on the web, the URL is a relatively stable factor. The generation and change of the URL requires the network service provider to carry out certain procedures, so the URL is relatively stable. This theory has some truth, but in practice, the actor can completely use technology to hide and transform his own website. That is to say, the physical space represented by the website is not unique, and the physical space associated with the website is spread throughout the network. If this problem is not properly resolved, there will still be conflicts of international jurisdiction [12].

III. THE BASIC THOUGHTS ON CONSTRUCTING CRIMINAL JURISDICTION IN CHINA

China has no specific legislative provisions on the criminal jurisdiction of cybercrime. The relative legislative provisions are scattered in the sixth chapter of the Criminal Law and the "Decision on Safeguarding Computer Network Security", which greatly restricts the exercise of jurisdiction. Therefore, it is necessary to improve the cybercrime legislation in China through the gradual legislation, and to treat the domestic jurisdiction and international jurisdiction differently. On this basis, construct the criminal jurisdiction of cybercrime that suits China's national conditions.

A. Domestic Jurisdiction of Cybercrime

For the jurisdiction of domestic cybercrime, the author believes that the current theory of regional jurisdiction of the Criminal Law can be applied, and the jurisdictional rules of civil network cases can be used as reference. The location of the server according to the IP address when the cybercrime is committed can be used as the connection point of cybercrime jurisdiction. Every computer connected to the network will be assigned an IP address, which is unique and deterministic. The IP address assigned to the computer accessing the network through broadband remains fixed for a certain period of time; Although the address assigned to computer through the telephone line is temporary, but its network accessing records including the time of accessing, the number of the telephone line, etc., will be kept for a long time by the network service provider according to the laws and regulations. Therefore, it is more reasonable to determine the jurisdiction of cybercrime through the server where the IP address is located. In addition, the determination of the jurisdiction of cybercrime by IP address is conducive to the realization of coordination with the civil jurisdiction system. According to the provisions of Article 1 of the Interpretation of Several Issues Concerning the Application of Laws Concerning the Trial of Computer Network Copyright Disputes Promulgated by the Supreme People's Court of China on the 19th, 2000, the network copyright dispute case is under the jurisdiction of the court where the infringement is committed or the defendant's domicile. The place of infringement includes the location of the network server, computer terminal, etc., where the alleged infringement is committed. For the case where it is difficult to determine the location of the infringement or the location of the defendant, the location where the plaintiff finds the infringing content of the computer terminal device can be regarded as the place of infringement. This regulation has important reference significance for China's current cybercrime. Use the location of the server to which the IP address belongs at the time of the crime as the connection point of the cybercrime jurisdiction, can not only solve the jurisdiction problem of cybercrime perfectly, but also realize the coordination and unification of the jurisdiction in criminal trial and civil trial.

B. International Criminal Jurisdiction of Cybercrime

The conflict of domestic criminal jurisdiction of cybercrime is relatively easy to solve. Due to the particularity of cyberspace, the conflict of criminal jurisdiction of cybercrime between different countries and regions, has confused many countries. For the time being, it is difficult for scholars to explore the so-called "feasible" jurisdictional rules on this issue. No matter what rules are applied, the conflict of jurisdiction cannot be avoided. The author believes that the fundamental way to solve this problem lies in respecting the sovereign jurisdiction of countries over cyberspace and strengthening international cooperation, and solving the positive and negative conflicts of jurisdiction on the basis of international cooperation.

1). Based on the principle of territorial jurisdiction in the current Criminal Law

In the issue of criminal jurisdiction of transnational cybercrime, the principle of traditional criminal jurisdiction should be established first. As a basic law of the country, the Criminal Law needs to maintain a certain degree of stability. If the provisions of the Criminal Law are adjusted according to the changes in the form of cybercrime from time to time, it will have a serious impact on the stability of the Criminal Law, and at the same time it will bring trouble to the judicial practice, and thus affect the punishment of cybercrime.

2). Participate or conclude of an international convention on criminal jurisdiction of cybercrime

In November 2001, the Council of Europe adopted the world's first international convention on cybercrime: the Cybercrime Convention. The Convention has not only played a positive role in promoting the cooperation of the international community in combating cybercrime, but also played an important guiding role in the cybercrime legislation of many post-development countries. Due to various considerations, China has not yet joined the Convention. The author believes that in order to jointly combat transnational cybercrime, China should strengthen its research on the Convention and consider joining the Convention when conditions are ripe.

3). Strengthen international cooperation among countries in the world

The key of solving the negative conflicts of jurisdiction is to actively seek international cooperation on the premise of respecting the sovereign jurisdiction of each country. Promote the active exercise of jurisdiction by concluding international conventions, multilateral or bilateral agreements, and avoid criminals using the differences in national laws to escape punishment.

REFERENCES

[1] Bingzhi Zhao, Zhigang Yu. The Response of Computer Crime and Its Legislation and Theory[J]. Chinese Law, 2001, (1): 148-163

[2] Wenzhi Jian. Working together to form a joint effort to combat cybercrime. Build a peaceful, secure and open network cooperation space [N]. Procuratorate Daily, 2017-08-25

[3] Liping Zheng. Transnational cybercrime and its legislation[J]. Contemporary Law, 2005(2): 101-106

[4] Zhigang Yu.The Evolution of Network Thinking and Sanctions of Cyber Crime[J]. Chinese and Foreign Law,2014(4):1045-1058

[5] Xiuzhong Xu. Network and cybercrime [M]. Beijing: CITIC Publishing House, 2003: 152

[6] Juan Wen. The ransomware incident is the epitome of global cybersecurity [N]. People's Post and Telecommunications, 2017-5-22

[7] Zhigang Yu. Intergenerational Evolution of Cybercrime and Criminal Legislation and Theoretical Response[J]. Qinghai Social Sciences,2014(2):1-12

[8] Zhigang Yu. Thoughts on Criminal Jurisdiction in Cyberspace [J] Chinese Law, 2003 (6): 102-107

[9] Peng Er. On the determination of the jurisdiction of cybercrime [J]. Journal of Yunnan University, Law Journal, 2004 (10): 23-27

[10] Hong Wei, Xu Chao. On the criminal jurisdiction of cybercrime[J] Guizhou Social Sciences (In Chinese), 2006(6): 83-86

[11] Huarong Wu. On the Construction of Criminal Jurisdiction of Cybercrime [J] Crime Research, 2006(4): 69-75

[12] Yuhua Tan.Study on Criminal Jurisdiction of Cyber Crime[J]. Administration and Law,2007(8):114-116