8th International Congress of Information and Communication Technology (ICICT2018)

Research on Criminal Jurisdiction of Computer cybercrime

Abstract

This article mainly discusses the jurisdiction of computer cybercrime. This article introduces the new theory of cybercrime jurisdiction and puts forward the system of establishing cybercrime jurisdiction: the principle of priority of power, the principle of territorial superior rights, criminal jurisdiction dispute negotiation system and drawing on the civil jurisdiction of computer cybercrime system.

1. Introduction

With the rapid development of Internet technology, the use of the Internet has penetrated into all fields of social life. The number of Internet users and the time spent on the Internet have been continuously increasing. According to the 40th Statistical Report on Internet Development in China (hereinafter referred to as the Report) released by China Internet Network Information Center (CNNIC) on August 4, 2017. As of June 2017, the number of netizens in China reached 751 million with an Internet penetration rate of 54.3%. At the same time, with the development of the Internet, especially the rise of mobile phone networks in recent years, computer cybercrime has been constantly spreading. Crimes against cybersystems, internet defamation crime,internet illegal business crime, internet extortion crimes and computer cybergambling continue to emerge, posing a serious threat to personal property, information and security, disrupting the overall social order. According to the U.S. think tank Strategic and International Studies Center, computer cybercrime is estimated to cost the world 445 billion U.S. dollars a year,

including over 45 billion U.S. dollars in economic losses in china. Therefore, it is a problem that the world needs to deal with to eliminate the computer cyber environment, crack down on computer cybercrime, safeguard citizens legitimate rights and interests, and safeguard the order of the Internet. Among them, the jurisdiction of computer cybercrime is issues that need to be solved first.

2. Overview of criminal jurisdiction

The jurisdiction of computer cybercrime includes two kinds of situations: First, which country is responsible for the crime. Second, which court in the country is under the jurisdiction of the crime? The former is the jurisdiction of criminal substantive law, that is, the issue of the space effectiveness of criminal law, which is a kind of static criminal jurisdiction. The latter is the jurisdiction of the trial in criminal proceedings, is a dynamic criminal jurisdiction.

Computer cybercrime occurring in China mainly involves the issue of geographic jurisdiction in criminal proceedings, which is generally governed by the criminal court, If the jurisdiction of the peoples court where the defendant is domiciled is more appropriate, it may be under the jurisdiction of the peoples court where the defendant resides. Transnational computer cybercrime jurisdiction is the issue of criminal jurisdiction in substantive law, mainly related to the conflicts of international jurisdiction. Due to its own virtual and transnational characteristics, computer cybercrime has an impact on the basic principle of the traditional space effect of criminal law. The basic principle of the space effectiveness of Chinese criminal law is based on the principle of territorial jurisdiction and adopts the principle of personal jurisdiction, protection of jurisdiction and universal jurisdiction. This principle can effectively protect the legitimate rights and interests of our country and citizens, but, how to apply the jurisdiction of transnational computer cybercrime needs further study.

In general, the criminal jurisdiction of computer cybercrime should be applied in accordance with the relevant provisions on the space effectiveness of the general principles of criminal law. Article 6 of the Chinese Criminal Law stipulates that, Any person who commits a crime in the territory of the Peoples Republic of China shall apply this law unless otherwise specifically provided by law. Chinese criminal law has jurisdiction as long as one of the criminal acts or criminal consequences occurs in China, including ships, aircraft and other aircraft outside the territory as well as Chinese embassies and consulates abroad. Article 7, 8 and 9 of Chinese Criminal Law respectively stipulate personal jurisdiction, protection of jurisdiction and universal jurisdiction. According to personal jurisdiction, China has criminal jurisdiction of computer cybercrime committed by Chinese citizens outside Chinasterritory. According to the principle of protection, China has criminal jurisdiction over foreigners in the field of computer cybercrime committed against Chinese countries or citizens outside China. In addition, for the international treaties that China participates in, if the treaty provides for computer cybercrime, China can apply Chinese criminal law within the scope of its treaty obligations and exercise its criminal jurisdiction.

3. New issues of criminal jurisdiction of computer cybercrime

Traditional criminal crimes do not have the characteristics of virtuality and unlimited expansibility. Even transnational crimes, since the crimes themselves are noncovert, the targets of the crimes are tangible and the objects constituted by the real threedimensional space , Each country may determine the criminal jurisdiction of the crime according to its own criminal law or the provisions of the relevant international (or bilateral) treaty. The criminal jurisdiction of computer cybercrime is different from the traditional crime. The typical one is abstract crossborder behavior. Since the criminal act involves many countries, it is difficult for this illegal computer cybercrime to point to a certain area of criminal jurisdiction. For example, several former Federal German students invaded the U.S. Department of Defense over the Internet for the purpose of stealing military secrets for the KGB, the students first log in to servers in Japan through the former Federal Republic of Germany network while using Japans network data and signaling system to transfer to a university in the United States and finally invade the U.S. Department of Defenses computer through this U.S. university network system and steal important U.S. military secrets. In this case, several students criminal behaviors spanned the Federal Republic of Germany, Japan and the United States in three countries. Whether all countries should have criminal jurisdiction over this case and whether

Japan has jurisdiction as a trans boundary state became the hot topics discussed by criminal law scholars. The issue of abstract crossborder has formed a great challenge to the traditional theory of criminal jurisdiction.

The nature of the network itself changes some of the content and form of traditional crime, and perpetrators can commit crimes through virtual spaces that span several or dozens of countries without close contact with specific or nonspecific subjects and its result is far greater than natural crime. However, computer cybercrime requires terminal devices such as computers or mobile phones to implement crime through a web server, to access web pages of a target country, and also to output and input relevant data instructions, these new behaviors have greatly impacted the traditional criminal jurisdiction, and the two are hard to come into agreement. For example, it is a legal act for Jackie to establish a pornographic website in country A and a criminal act in country B, C and D, so the perpetrator set up a pornographic website in country A through the web server of country C , A country court does not exercise its jurisdiction. However, many citizens of country B visited the site. The citizens of the country, Mike, interacted with Jacks website and continuously uploaded pictures or videos. In this case, Court A does not exercise criminal jurisdiction; State B considers that the commission of a crime in connection with its own computer is criminalized in its own country and therefore claims jurisdiction in the case. Because perpetrator Jack is an pornographic website registered on the server of country C and the criminal act of establishing pornographic websites in country C, country C considers himself having criminal jurisdiction. The court of State D believed that the act of its own citizens, Mike, was an active and purposeful visit. It violated its criminal law provisions on the dissemination of obscene articles and violated its own good customs. Therefore, the court of State D should have full jurisdiction over the case. Based on the above new issues concerning the jurisdiction of computer cybercrime, all countries will inevitably compete for the criminal jurisdiction, resulting in conflicts of jurisdiction, detrimental to the trial of the facts of the case and the protection of the legitimate rights and interests of the victims.

4. New Theories of Cybercrime Jurisdiction and Analysis

Therefore, how to solve the conflict between new computer cybercrime and traditional criminal jurisdiction has become a hot topic in the field of criminal law. Conservative scholars believe that we should still uphold the traditional criminal jurisdiction and should not change this tradition because of the appearance of special phenomena. Open scholars have proposed some new theories of jurisdiction. Mainly include:

4.1 Theory of new sovereignty

The theory of new sovereignty can be called the theory of network autonomy, or called radical independent jurisdiction theory and the sovereignty of the virtual world is independent. The doctrine holds that computer cyberspace is creating a global civil society that has its own form of organization, values, and rules that are completely independent of the government and have the right to selfgovernment[1].According to this theory, since the network itself has the characteristics of being different from those of other objects, the current legal norms should no longer be applied to the issue of jurisdiction over computer cybercrime. A separate system of laws applicable to computer cyberspace should be developed separately so that the jurisdiction of computer cybercrime is independent from the traditional criminal jurisdiction.

4.2  Theory of jurisdictional relativity

In order to solve the problem of criminal jurisdiction of computer cybercrime, Professor Darrel Menthe of Stanford University in the United States put forward another theory the theory of jurisdictional relativity. The theory has become the fourth international space theory after Antarctica, outer space and the high seas. The theory holds that computer cyberspace should exist as a new jurisdiction, as in the high seas, Antarctica and outer space, establishing new rules of jurisdiction that are different from the traditional ones[2].If a citizen illegally enters the computer cyberspace and commits a crime in space, any country may exercise jurisdiction over the perpetrator according to the laws of its own country. At the same time, they also believe that the parties do not need to go to a court to respond, they only need to go to court in a court through computer cyberspace, and the court can execute the verdict they have made online. This theory is obviously the principle of nationality needed to establish

jurisdiction in the analogous application of the high seas, however, it is difficult for the virtual characteristics of the Internet to determine where a persons nationality is. Moreover, based solely on nationality as the basis for legislative jurisdiction, it is bound to make radical changes to the current principle of territorial jurisdiction, which is unacceptable to all countries [3].