Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030725
ISSN 2616-2296 Vol. 3 Num. 7

Research on E-discovery of Cross-border Cybercrimes

Yuwei Chen[1,a,*]

[1]*School of Law, Shenyang University of Technology, Shenyang, Liaoning, China*
[a]*1310480732@qq.com*
[*]*Corresponding author*

Keywords: Cross-border cybercrime, Electronic evidence, International judicial assistance in criminal matters, Network service providers, Unilateral cross-border forensics

Abstract: With the advancement of science and technology in various countries, cybercrime is gradually becoming globalized, and the number of cross-border cybercrimes is increasing year by year. In the era of rapid development of the Internet, electronic evidence of cross-border cybercrime is extremely important in the process of governance of cross-border cybercrime. Based on three cases, this paper analyzes and studies the shortcomings of the three electronic evidence collection methods in the international community: international criminal justice assistance, network service provider provision, and unilateral cross-border evidence collection, so as to put forward an effective response to the problem of electronic evidence, which will help to better combat cross-border cybercrime and reduce the number of cross-border cybercrime.

At present, due to the characteristics of cross-border cybercrime that are more harmful, have a wide range of impact, and the time and risk cost of the crime are lower than those of ordinary crimes, coupled with the differences in the level of development of various countries and the differences in their own laws, resulting in conflicts in the jurisdiction of cross-border cybercrimes, governments around the world pay more attention to the investigation and handling of cross-border cybercrimes. [1] In cross-border cybercrime, electronic evidence is an important evidence to combat cybercrime, so the issue of electronic evidence for cross-border cybercrime has become particularly important.

1. Overview of Electronic Evidence of Cross-border Cybercrime

In the period of rapid development of informatization, electronic data based on computers and networks has played an irreplaceable role in the process of investigating and prosecuting cybercrimes. This evidentiary information in digital form is defined as electronic evidence. At present, there is no clear definition of the meaning of electronic evidence for cross-border cybercrime in the international community.

The Queensland Courts and Electronic Evidence Record defines electronic evidence as "reading text, symbols, pictures and other data stored in electronic media such as tapes and optical discs through network-based files"; [2] Electronic evidence is defined in the Electronic Evidence Rules as "electronic documents, electronic signatures, commercial records produced by electronic, optical or even other similar means, audio recordings, video recordings, video recordings, and instantaneous evidence, electronic testimony that can prove the facts of a case".[3] To sum up, electronic evidence

of cross-border cybercrime can be defined as electronic data generated on the basis of the network to prove the facts of a criminal case in the process of the perpetrator committing a criminal act against the data stored in the network in different regions or using the network as a means of committing a crime. [4]

2. Cases and Deficiencies of Cross-border Electronic Evidence Collection Methods

2.1 International Judicial Assistance in Criminal Matters

Between 2015 and 2016, defendant Kaimin Zhang and 52 others participated in criminal groups in the Republic of Indonesia and the Republic of Kenya that carried out telecommunications network fraud against residents of Chinese mainland. At the time of the case, Kaimin Zhang and other defendants defrauded 75 victims of a total of more than 2,300 yuan through the above-mentioned fraudulent means. Since the victims in this case were all residents of Chinese mainland, in accordance with the principle of priority of territorial jurisdiction, in April 2016, Kenya repatriated 76 suspects of telecommunications network fraud to Chinese mainland. In view of the fact that Kenya had already handed over the seized physical evidence involved in the case, such as laptops, voice gateways, and mobile phones, to the Chinese public security organs before the repatriation of the criminal suspects, in order to ensure the objectivity, relevance, and legitimacy of the evidence, the procuratorial organs communicated with the public security organs on issues such as the standard of proof that the case evidence needed to meet and the extraction of foreign-related electronic data, and proposed to extract and restore the electronic data involved in the case, such as Skype chat records, Excel and Word documents, and Internet phone dial records. According to this clue, all 52 suspects in the Kaimin Zhang case were brought into the case.①

In this case, even though Indonesia and Kenya responded positively to China's request for access to electronic evidence and submitted all the relevant evidence in the case to the Chinese police, through the method of collecting evidence through international criminal justice assistance, the Chinese police could only obtain electronic data storage media from foreign police, but could not directly obtain relevant electronic evidence. Under such conditions, the time of obtaining electronic data will be much later than the time of transfer of evidence and criminal suspects, and it is easy to be deleted or changed in the process of waiting for electronic evidence to be extracted and identified, and the probative power of electronic evidence obtained will be reduced, affecting the police investigation and handling of cases. The evidence collection method of international criminal justice assistance has an "inverted U-shape" structure, which involves more institutions than other evidence collection methods, and the procedures are more complex, and the evidence extraction procedure cannot be completed in a short time. [5]

In addition to the shortcomings of the complicated procedures and excessive time required in the cases, international criminal justice assistance is also prone to the problem that there are no relevant international treaties concluded between two or even more countries. At present, China has signed relevant bilateral international treaties with 86 countries, but the number of signatories in the international community is still insufficient. If the crime occurs in a country that has not signed a bilateral international treaty with China, it cannot be dealt with in a timely manner through international criminal justice assistance. In addition, the content of bilateral assistance treaties signed between China and some countries is not perfect, and if there are matters that have not been concluded in the treaty in the process of collecting evidence, the two countries will have no international treaty as a basis for handling, which will affect the investigation and handling of the case.

① Kaimin Zhang et al. 52 Telecom Network Fraud Case, "The 18th Batch of Guiding Cases Released by the Supreme People's Procuratorate".

2.2 Provision by Network Service Providers

In May 2017, when the suspect Gao was riding an ofo yellow shared bicycle at a bus stop on Shennan Avenue, Futian District, Shenzhen, he collided with a pedestrian Jia who came out of the platform and caused him to fall, causing Jia to suffer rib fractures and multiple soft tissue contusions. After the incident, Gao abandoned the car and fled the scene. Due to the lack of on-site video, the company to which the vehicle belonged did not actively cooperate with the investigation and evidence collection, and it was difficult to solve the case. After a large-scale investigation, the traffic police department arrested the suspect Gao in June.[②]

On the one hand, network service providers bear the responsibility of assisting the police in obtaining electronic evidence in the process of investigating and handling cases, and on the other hand, as data storage parties, they also bear the obligation to protect personal data from leakage. Requiring a network service provider to provide relevant electronic data without the data owner's permission may result in the network service provider taking time to consider whether the electronic data should be provided. In addition, there is currently no law on the conduct of assistance by network service providers, resulting in the reluctance of network service providers to actively cooperate with the police in the process of providing assistance to complete evidence collection, resulting in low efficiency in case investigation and even irreparable losses to society.

2.3 Unilateral Cross-border Evidence Collection

In 2016, criminal suspect Zijia Hu used his electronic device to help add new members to a gambling website created on the Internet, defrauding more than 1,000 victims. Because the gambling website's operating server is a foreign server, the Chinese police are unable to log in to the website to extract the victim's information, the investigation cannot continue, and the case cannot be continued due to the inability to obtain favorable relevant evidence information from the website.[③]

Although unilateral cross-border evidence collection is more efficient, less time-consuming and costly than other methods of evidence collection, and does not require too many complicated application procedures, there are also many drawbacks. In the period of rapid information development, cyberspace sovereignty is as important as national sovereignty. Unilateral cross-border evidence collection does not require an application from the national government, and unauthorized collection of electronic evidence is very likely to infringe on the cyberspace sovereignty of other countries. Not only that, electronic data also stores a lot of other personal data information that is not related to the case, and while extracting evidence through unilateral cross-border evidence collection, it may also extract personal data other than the criminal suspect, including personal information and property. While unilateral cross-border evidence collection is efficient, it also increases the risk, and it is very easy to infringe on the legitimate rights and interests of entities other than criminal suspects.

3. Responding to Cross-border Electronic Discovery Issues

3.1 International Judicial Assistance in Criminal Matters

In view of the problems of international criminal justice assistance, which is a method of collecting evidence, the procedures are complicated, and the scope of international assistance treaties is insufficient, [6] the following solutions can be found.

② Transferred from the Internet "Hit and run on a shared bicycle, the bicycle was not locked".
③ Hu Zijia's case of opening a casino, the first-instance criminal verdict of the People's Court of Renqiu City, Hebei Province.s

3.1.1 Simplify the Forensic Process

The procedures for traditional international judicial assistance in criminal matters are very complicated, and there are many procedures that can be simplified after the two sides have agreed upon them, especially the procedures for the application and review of evidence collection can be directly specified in the treaties signed by the two countries, which can not only simplify the procedures for collecting evidence, greatly shorten the time spent on evidence collection, [7] but also will not infringe on the country's sovereignty over data space.

The "inverted U-shaped" evidence collection mode has complex procedures and involves too many organs, which can easily lead to the problems of high cost and untimely evidence collection. In the era of rapid development of information and the increasing importance of electronic evidence, this traditional forensic mode can no longer meet the needs of cross-border forensics collection of various countries, and countries can sign a bilateral assistance treaty to build a "one-word" forensic collection model after discussion, that is, the investigation department directly carries out forensic collection with the law enforcement department or network service provider of another country. Article 32 (b) of the *Convention on Cybercrime* also provides that law enforcement authorities may obtain electronic evidence directly from individuals if it is reasonable and lawful and with the consent of the person concerned. In addition, the application and review procedures for evidence collection can also be carried out through the Internet, and evidence can also be obtained directly from the requested country through the Internet, so as to improve the efficiency of cross-border evidence collection.

3.1.2 Increase the Number of Treaty Parties

With the rapid development of science and technology in the information age, existing laws cannot fully meet all needs, and in order to keep up with the progress of the times and meet the needs of keeping pace with the times, it is necessary for countries to negotiate and sign new international bilateral treaties in the process of collecting evidence. So far, China has signed international criminal justice assistance treaties with 86 countries, and through the increasing number of signed treaties, we can effectively avoid the problem of lack of clear legal support in the process of evidence collection caused by insufficient legislation. At the same time, the addition of States Parties can improve the efficiency of evidence collection by the international community and have a positive impact on the realization of cross-border evidence collection by all countries.

3.2 Provided by Network Service Providers

Network service providers' negligence in assisting in the collection of evidence should also be effectively regulated. Since network service providers not only bear the obligation to assist in the collection of evidence, but also bear the responsibility of preserving personal data from being arbitrarily extracted, while requiring network service providers to assist in evidence collection, they should also take compensatory measures and strengthen the screening of the extracted data to prevent the leakage of personal information of persons unrelated to the case, so as to ensure that they can actively cooperate with the police in extracting electronic evidence, effectively improving the efficiency of cross-border evidence collection.

3.3 Unilateral Cross-border Forensics

In the era of big data, more and more countries in international practice are using unilateral cross-border forensics as an efficient way to collect evidence in order to improve the efficiency of forensics. However, due to the unilateral cross-border evidence collection model, it is easy to raise the issue of national sovereignty in cyberspace, so it is necessary for governments to actively regulate it.

3.3.1 Stipulate the Scope of Application of Unilateral Cross-border Evidence Collection

Until a more efficient and secure method of evidence collection is developed, governments can apply unilateral cross-border evidence collection to a certain extent. Due to the high risk of unilateral cross-border evidence collection, this method of evidence collection should only be applied when other methods are insufficient to meet the demand for evidence collection and are faced with major cases that endanger the national or collective public interests. In addition, based on the principle of reciprocity, on the premise that a country takes the initiative to apply the unilateral cross-border evidence collection method, and on the basis of not undermining the cyberspace sovereignty of the two countries, the requested country can also apply this method to extract electronic evidence from that country.

3.3.2 Strengthen Supervision of the Evidence Collection Process

In order to reduce the risk of harming the cyberspace sovereignty of other countries that is easily brought about by unilateral cross-border evidence collection, it is necessary to strengthen supervision over such evidence collection methods, and strictly stipulate the approval system and enforcement organs. At the same time, the electronic data extracted in the process of supervision and inspection shall be supervised and recorded, so as to prevent infringement of the national sovereignty of other countries and the legitimate rights and interests of individuals. Strict supervision of the process of applying unilateral cross-border evidence collection can effectively avoid the unreasonable extraction and use of electronic evidence, reduce the legal and diplomatic problems caused by it, and reduce the risks caused while improving the efficiency of evidence collection.

4. Conclusion

Cross-border cybercrime has a significant impact on the era of big data, and it is inevitable to crack down on cross-border cybercrime, and in order to effectively combat cross-border cybercrime, it is inseparable from the acquisition of cross-border electronic evidence. At present, the traditional method of international judicial assistance in criminal matters is still the most widely applicable, but there are still many problems that need to be solved in this method. Countries should further explore research to find more efficient and reliable ways to obtain cross-border electronic data forensics.

References

[1] Lan Y, Qiyan C, Sixin L. Study on International Cooperation to Address Cross-border Telecommunication Network Fraud Offence[J].Journal of Politics and Law, 2024, 17(2):51.
[2] United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime[J]. Department of Justice (DOJ) Documents / FIND, 2022
[3] Filippo S. International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime [J]. ERA Forum, 2022, 23(1):101-108.
[4] Künnapu M. Challenges Related to Fight Against Cybercrime. A Need to Strengthen International Cooperation[J]. International Journal of Criminal Justice, 2021, 3(2)
[5] Butunbaev N T. Features of International Legal Cooperation In Combating Cyber Crime[J]. International Journal of Advanced Research, 2020, 8(5):100-107.
[6] Cassim F. Formulating specialised Legislation to address the Growing Spectre of Cybercrime: A Comparative Study[J]. Potchefstroom Electronic Law Journal, 2009, 12(4):35-79.
[7] Wan C. International Cooperation for the Prevention of Cybercrime[J].Korean Criminological Review, 2007, 113-140.