Study on Rule of Exclusion of Electronic Evidence

Qi Zhang

College of Criminal Justice, East China University of Political Science and Law, Songjiang District, Shanghai, China 201620

zhangqi_in_ecupl@163.com

Keywords: electronic evidence; exclusionary rule of illegally obtained electronic evidence; exclusionary rule of illegally obtained evidence; criminal investigation; evidence collection

Abstract: Since the newly revised criminal procedure law of China has listed the "electronic data" as one of the legal forms of evidence, the problem of how to eliminate illegal electronic evidence in criminal proceedings arises. This article discusses the definition and characteristics of the electronic evidence. Then, study on the application of the rules of electronic evidence under the background of lacking of legal regulation in electronic evidence, and set an assumption to establishing the illegal electronic evidence exclusion rules, and slightly help the and legislation and the investigation.

1. Introduction

Since January 1st, 2013, China's newly revised criminal procedure law has listed "electronic data" as one of the legal forms of evidence, marking the establishment of legal status of electronic data evidence, responding to the problems encountered in practice in the past, which is a good legislative start. However, the existing rules for the exclusion of illegal evidence do not strictly restrict the electronic evidence in China's criminal procedure law, and the scope of the exclusion of illegal electronic evidence can be considered to be extremely limited. If the electronic evidence obtained illegally is not excluded, it will certainly violate the legal rights and interests of criminal suspects and even the public. This article will study on the application of the rules of electronic evidence under the background of lacking of legal regulation in collecting electronic evidence, and set an assumption to establishing the illegal electronic evidence exclusion rules, and slightly help the and legislation and the investigation.

2. The Concept of Electronic Evidence

For the discussion of the concept of electronic evidence in academia, generally, there are two theories: one is called "theory of computer evidence", which regards the electronic evidence as a kind of computer information. In this theory, computer data can be considered as the electromagnetic carrier which can confirm operation process of cases in the era of modern computer information technology. Electronic data is the information carrier of the output, input, operation and storage of the computer information obtained from the operation of the Internet system. Under this definition, electronic data contains the majority of computer carriers and peripheral products, such as optical disks, emails, network chats, electronic bills, electronic signatures and mobile storage drives and so on.

The other theory is the "theory of electronic materials". It is defined as the usage of transmission in the form of electronic information aiming at verifying the involved information. That is to say, the theory holds the view that electronic evidence is a kind of material evidence which relies on the advanced electronic technology and electronic products. In the theory of electronic materials, electronic material evidence contains not only the computer evidence, but also other evidence in electronic form, such as fax, telephone and database.

After comprehensive consideration, the author thinks that the second theory is more in line with social needs and adapts to the development of modern life. That is, in the theory of electronic

materials, electronic information, computers and their peripheral products are included in the catalogue of electronic evidence, which basically covers the types of evidence encountered in the information network. In the contrary, the first definition of computer evidence has two significant disadvantages: First, it makes the computer the only carrier of electronic evidence, ignoring the rest of the electronic tools used in the real life, such as mobile phones, printers, videotape machines and so on. Second, electronic evidence is not just in electromagnetic form. Throughout the progress of electronic and information technology in the world, there is no doubt that electromagnetic technology plays a very important role in it. However, many new electronic technologies have emerged in the recent development. For example, optics develops rapidly in the field of electronics, so that information carriers are not limited to electromagnetic recording. It can be seen from this that it is unreasonable to restrict electronic material evidence to computers, which will easily hinder its development, and at the same time, It will make some digitized materials cannot be used as the evidence. Therefore, the definition of electronic evidence should take into account the actual situation of modern development as much as possible, as well as the possibility of more forms of existence in the future.

3. Characteristics of Electronic Evidence

3.1. Spatial Virtuality and Environmental Dependence

It is well known that electronic data is a product of virtual space. People can store it in SSD, SM card, storage card, cloud disk, and so on. But no matter what carrier it is, no one has the possibility to enter it or touch it. Therefore, when people want to save or extract an electronic data in such a virtual space, they need to do so with the help of electronic tools. Electronic tools play the role of a technical agent in the process of saving and extracting. But the virtuality of electronic evidence does not negate its usefulness as court evidence. The Internet is invisible, connecting every corner and every individual together. Every seemingly independent behavior, on the Internet for all kinds of illegal activities or other legal activities, all occur in real life, even more likely in real life lead to serious consequences. Therefore, although electronic evidence exists in the virtual world, it still has a great impact on the actual cases. So, this is the spatial virtuality character of this kind of evidence.

Electronic material evidence cannot leave a certain operating environment, its existence certainly needs specific high-tech electronic equipment and software application to support. Just as the data in text format cannot be used in CD player, it can only work in a specific software environment for text editing. That is to say, certain forms of electronic evidence need to be transformed into a form that people can directly see. Therefore, no matter how much true and accurate electronic evidence is in the electronic carrier, it cannot be obtained and used by people and cannot be used as evidence in the legal trial if there is no equipment in the corresponding environment. Electronic evidence depends on the presentation environment, which has an important impact on its probative force. “Electronic evidence, which is beyond time and space, enables it to be transmitted rapidly in the global network space and every transmission is an exact copy of information. Even if electronic evidence were put in any coroner of the world, it would not affect its normal use.”[1] This also brings a lot of difficulties to the electronic evidence collection. Therefore, it also has environmental dependence.

3.2. Vulnerableness and Recoverableness

It is obviously very difficult to be recovered completely after the destruction of ordinary physical evidence, but it is relatively easy to restore the electronic evidence after the destruction of technology, unless the storage medium is destroyed. For example, if the computer is burned to pieces, It`s hard to restore the data in it. Some electronic evidence may be lost and unrecoverable, such as the separate text files and isolated photographs; most electronic data are stored in virtual spaces such as computers, so it is extremely unlikely to be counterfeited, which is also obviously discovered. Criminals may easily delete and change obvious data, but do they have the ability to completely delete the hidden information traces behind the data? There is only a little possibility that these traces and data will be completely removed. In addition, criminals will leave evidence and traces when they

manipulate and destroy electronic data in a technical way, but it is quite difficult to be unknown. Even if criminals are experts in the field of electronic technology, they may not be able to achieve such a situation. “When the data is written to the magnetic medium, the data on the original hard disk will leave a faint trace. The magnetic medium (including the hard disk) will leave a trace every time it is written, even after the media has been rewritten many times, every trace will still remain.”[2] While the judicial officers are still groping for the electronic evidence, they have to make effort to establish a high-quality team to examine and collect the electronic evidence.

3.3. Multiple-attributes

Electronic evidence also has a variety of properties, for example, it presents its content as evidence, which is the same as the property of documentary evidence; In the way of representation, electronic evidence exists in the computer in the way of information data, which is similar to physical evidence. In many cases, electronic evidence is a combination of words and audio-visual materials.

4. Exclusionary Rule of Illegally Obtained Electronic Evidence in Other Countries

4.1. American Exclusionary Rule of Illegally Obtained Electronic Evidence

The U.S. has a very strict requirement for evidence and electronic evidence is of no exception. In addition, the fruit of the poisonous tree, which means the evidence derived illegally, cannot be used. For example, if the police learned that the suspect's mobile phone was buried underground by torture in the absence of lawyers, all the electronic evidence in that device was invalid poisonous fruit owing to the torture is poisonous tree. According to relevant provisions of Foreign Intelligence Surveillance Act, the suspect under surveillance can make an application for exclusion of illegal wiretapping before the court. There are two kinds of reasons: one is the application procedure is incomplete and the other is that the actual behavior of surveillance is beyond the authorization. As long as the court approves the application, the electronic evidence obtained illegally will be subject to non-adoption. The exclusionary rule of illegally obtained evidence established in the United States, is mainly to regulate the investigation of the national police agency representing the public power as well as protect the legitimate civic rights. With the improvement of electronic evidence and the development of society, the exceptions such as "inevitable discovery", "neutral sources" and "good faith" are appearing in the Federal Rule of Evidence.

4.2. UK Exclusionary Rule of Illegally Obtained Electronic Evidence

In the 1990s, the British government stipulated the discretion of the judge to exclude evidence in the law of evidence of police agencies and criminal proceedings. Section 78 of the legal instrument states: "in any proceeding, the court may refuse to allow the prosecution to present the evidence if, in the view of the court, taking into account the circumstances, including the circumstances in which the evidence is obtained, the evidence on which the prosecution is based adversely affects the impartiality of the proceeding." Then we can find that the British exclusion is wider. It includes not only the illegally obtained evidence, but also the exclusion of electronic evidence which can affect the social justice after admission. What is worth noticing is that the judge cannot rule out physical electronic evidence arbitrarily. Because the exclusion of physical evidence actually depends on comprehensive considerations of many factors, among which the most essential standard is whether it impact the judicial fairness.

4.3. Exclusionary Rule of Illegally Obtained Electronic Evidence of Germany

In German legislation, the rules of adoption involving electronic evidence have been debated constantly. The key points of dispute are the objective of excluding electronic evidence and the definition of standards. Most German jurists do not agree with the practice of rejecting illegally obtained electronic evidence. They believe that the court can decide whether to adopt it on the basis of circumstances. The measure includes: one is that if the exclusion of electronic evidence complies

with the objective of rule of exclusion electronic evidence, it can be excluded. Assuming that the result is inconsistent with the objective, it can be seen whether adopt the electronic evidence involved in the case will not play a positive role, so the exclusion is rejected. Another is that there should not be serious conflict between the exclusion and the facts of the case. Assuming that the exclusion of illegally obtained electronic evidence would have a significant impact on the ascertainment of the facts, the court could adopt such electronic evidence in its proceedings. In addition, the illegally obtained electronic evidence cannot be adopted as the evidence in the court.

5. Assumption of Exclusionary Rule of Illegally Obtained Electronic Evidence of China

“There are certain differences in the specific contents of the legal evidence rules established in various countries in the world. Countries of Anglo-American law system is generally believed that electronic evidence should be used in the lawsuit activities, and not only prove its effect on the substantive issues of case, but also comply with the rules of evidence, such as hearsay rules, the best evidence rule and illegal evidence elimination rule and so on.”[3] According to these rules, the electronic evidence must have the evidence ability and probative force. The civil law countries have less limitation on the admissibility of electronic evidence. Generally, electronic evidence related to the facts of a case which collected under due process of law can be used as evidence.

Speaking of the legality of evidence, some scholars put forward: "There is no actual distinction between legal or illegal evidence itself. Therefore, in English, it is translated as' illegal evidence obtained’, so what the term 'illegal' actually refers to is illegal evidence collection procedures." [4] At present, in Chinese judicial practice, the most serious illegal evidence has the following two kinds: One is the evidence which violates our country constitution provides when the citizen enjoys the constitutional right, such as: illegal search or trespass citizen's residence without a warrant. It is mainly manifested as the infringement of individual's privacy and the infringement of property ownership. These rights are the most fundamental rights of the people according to the law. The other one is the actions of serious violations in judicial procedures and it may have a terrible impact on judicial practice.

The author believes that the electronic evidence should not be an exception to the exclusionary rule of illegally evidence, and should be included in it in some cases. If the authenticity of electronic data cannot be proved, it should be excluded. However, evidence of violations of constitutional rights and fundamental human rights should be completely excluded. In the case of a violation of procedural laws or procedural rules, a full consideration is expected to be taken on whether it eill affect judicial justice or the authenticity of evidence.

5.1. Illegal Electronic Evidence in the Category of Partial Words

Although electronic data has been listed as a new form of legal evidence, it has a wide variety of properties. On one hand, it has the form of "data"; on the other hand, it has the characteristics of "material evidence, documentary evidence and witness evidence". The electronic form of verbal evidence refers to all the electronic data including the content of the statement, such as audio and video recording, mobile phone messages, E-mails and so on.

Electronic data on verbal attributes obtained by means of torture, extortion, violence and threat should be excluded. For this is a serious violation of citizens' constitutional rights to obtain evidence act. If it is proved that the defendant's confession is the result of using torture to extract confession and other methods, while excluding the defendant's confession, other guilty confessions should also be excluded from recording their audio and video recordings of guilty confessions. For example, if the suspect was tortured to extract the confession in the first record, and he keeps making guilty confessions in the subsequent records although the video of the subsequent guilty confessions did not contain the content of torture. Then the subsequent guilty confessions should also be considered as illegal electronic evidence if they cannot be reasonably explained in the end.

5.2. Illegal Electronic Evidence of Partial Physical Kind

5.2.1. Electronic evidence obtained by serious human rights violations

According to the current law, electronic evidence obtained through technical investigation measures can be used as long as it is authentic. In addition, the court can choose to disclose the procedures and methods of the investigative measures. The current provisions of the criminal procedure law overlook the risk of human rights violations when electronic evidence is collected, which is much higher than the general evidence collection measures. If these evidences are not excluded, it will form a bad misdirection, and even lead to the abuse of technical investigation. For example, before the strict approval process is completed, the recording evidence obtained by illegal eavesdropping or video evidence obtained by illegal surveillance, or electronic data obtained through illegal Trojan programs should not be adopted .The rule of exclusion of evidence is a strong regulation, which can regulate the investigative behavior of the investigative authorities and protect the human rights of the accused. In order to implement the protection of the basic rights of the constitution and the baseline requirements of procedural justice ,and to prevent the abuse of technical investigation measures, the author advocates that illegal electronic data obtained by the investigation measures which do not conform to the legal procedures , or violate the constitutional rights and the basic human rights of citizens should be excluded.

5.2.2. Electronic evidence obtained by illegal search and seizure

"According to article 110 of the criminal procedure law, search in our country can be divided into two kinds of cases. Generally speaking, a search warrant must be presented to the person being searched during the investigation, but it can be carried out during the arrest and detention without a warrant in case of emergency. "[5] Should the electronic data obtained in an emergency situation, in which case investigators can also conduct unauthorized arrests, searches and detentions be excluded? In the author's opinion, as electronic evidence is stored in a very hidden place and transmitted quickly through the network, the suspect is likely to store the electronic data related to the case in multiple networks or in multiple computers. If investigators can only take evidence at a particular location, the useful information data that exists at that location in the process is likely to be transferred to another computer or network on the Internet. Critical electronic evidence may be damaged or lost if a search warrant is applied again in accordance with the procedure. In such cases that unauthorized searches are not illegal, the electronic evidence obtained should be adopted.

5.2.3. Electronic evidence obtained in violation of technical operation

From a technical standpoint, failure to follow a standard operation rules can lead to two consequences: first, the failure of evidence collection, that the original evidence is destroyed, or that the original copy is not obtained. The second is that although the results of forensics are successful, the possibility of error cannot be completely ruled out in theory because of the violation of the procedure. For example, if an investigator takes evidence on a computer's hard disk and he does not use read-only equipment. Instead, he uses a working computer connected the suspect's hard disk and mirrored it. Without the read-only device, investigators could not prove whether they had input some other data while output the suspect's hard drive. Technically, this method violates the basic requirements of electronic data forensics. However, investigators may not input any other data at all. From the perspective of evidence law, if the violation of the standard requirements for electronic data forensics makes it impossible to prove the authenticity of electronic data, it should be excluded.

5.2.4. Electronic evidence illegally obtained with procedural flaws

For those general defects in the process of obtaining evidence, the investigator can correct them. But if it cannot be explained properly, or cannot be corrected at all, it should be excluded. From the perspective of the rule of Electronic evidence illegally obtained in other countries, the evidence in violation of technical specifications should be ruled out. The criterion of discretion should be whether or not its authenticity can be determined as the bottom line. The trial of criminal cases

decide whether it is a crime or not. If the electronic evidence is the key evidence to the case, even with a little flaws, but which can be confirmed true, it cannot be ruled out. It mainly exists in the judicial practice in our country as the following situation: One is the investigators did not write the place, time, manufacturing processes, objects, and use of equipment clearly on legal documents. The other one it that a lack of the signatures of the investigator in the process. If the document has physical authenticity, the court can adopt it as long as reasonable explanations and corrections are made to the missing information and situations. Because these behaviors generally do not directly affect the authenticity of electronic data, so they can be included. However, punishment should be given to the forensic investigator through administrative sanctions to reduce negligence.

However, if the electronic evidence is defective and cannot be corrected or interpreted to establish its authenticity, it shall be excluded. Such defects of electronic evidence have already been allowed to be corrected or interpreted by investigators, but if they cannot be reasonably explained or explained in the end, the authenticity of electronic data cannot be proved then it should be excluded. Doing so is a balancing act between fighting crime and protecting human rights. In judicial practice, China's electronic data collection is just starting, and the collection level of investigative agencies is relatively low, and violations of technical standards are relatively common, so it is not necessary to set high exclusion standards. But at the same time, the baseline of authenticity should be maintained to ensure that the facts of the case are based on actual electronic data.

6. Conclusions

“In general criminal cases, the search process mainly involves the person, residence and property of social citizens, which can be easily perceived by people”. [6] When the criminal process is not only limited to the realization of the world, but also spans into the, the investigators also turn the sear from physical space to the virtual space. The danger is that the search for a citizen's virtual space can take place without the person being aware of it. With the advent of the information age, the network in virtual space has become a key area of people's privacy rights. The activities of investigators in searching electronic evidence not only affect the rights of the subject searched, but also negatively affect the rights of citizens and electronic service providers.

In modern criminal justice, the physical value of excluding illegal electronic evidence is to make the fact clearly, and its procedure value is to punish the illegal evidence collection behavior of investigators, so that it can limit the abuse of indictment. Fundamentally, it makes investigators cannot benefit from his illegal act, so that it can ban those acts from the source. The infringement of civil rights is particularly serious in electronic data forensics measures, especially in electronic evidence obtained by technical investigation measures that people do not aware. Therefore, establishing reasonable rule of exclusion of illegal electronic evidence is a necessary step guided by the goal of judicial justice. In a nutshell, this system should be the direction of our judicial practice.

References

[1] Zhang Fang, Zhang Yunquan. (2011) The characteristics of electronic evidence and influence on trials [J], Evidence BBS, NO.10, China Procuratorate Press, p73-p74

[2] Warren G·KruseII, Jay G·Heiser. "Computer Forensics: Essentials of Emergency Response", Duan Haixin, etc. translation, Posts and Telecom Press, 2003, pp. 52-53.

[3] Wei Rensi, Gu Xing. “On the admissibility rules of electronic evidence in China”, Criminal Research, No. 1, 2007.

[4] Wang Jiancheng. “What kind of illegal evidence exclusion rules China needs?”, Global Law Review, No. 5, 2006.

[5] Liu Guangsan, Xiang Dechao. “On the Search and Seizure of Electronic Evidence”, North Methodology, No. 2, 2007.

[6] Liu Fangquan compilation. "The search and seizure of computers and the acquisition of electronic evidence in criminal investigation", China Procuratorate Press, 2006.