ISSN: 2688-8653

The Construction of Authentication Rules for Criminal Electronic Data

Wenye Ye

Jiangsu Normal University, Xuzhou, Jiangsu 221100, China

Abstract

The virtuality and fragility of electronic data make the legal positioning of electronic data more controversial, and also affect the authenticity of criminal electronic data in practical trials. The United States proves the authenticity of evidence through authentication rules, and electronic data, as one of physical evidence, can also be regulated by it. Therefore, learn from the U.S. authentication rules to build Chinese criminal electronic data authentication rules, and improve the judicial system of criminal electronic data. Identification rules to solve the authenticity proof dilemma of criminal electronic data in the application process.

Keywords

Criminal Electronic Data; Authentication Rules; Evidentiary Capacity; Forensic Identification.

1. Introduction

In 2012, in line with the voice of the times and the process of judicial reform, electronic data officially became one of the types of statutory evidence in criminal proceedings. At present, with the popularization of the Internet and the iterative update of electronic devices, the explosive growth of cyber crimes, the use of Internet technology for traditional crimes, and the entry of electronic data into criminal courts more and more frequently. In this new criminal situation, electronic data evidence has also become the new "king of evidence" in the information age.

2. Legal Positioning and Characteristics of Criminal Electronic Data

As emerging evidence, the academic community has conducted intense discussions on the evidentiary status of electronic data, and the legal position has also undergone a transition from "audio-visual material theory" to "independent evidence theory". In fact, electronic data is derived from traditional physical evidence, and is quite different from it. Any or all of the other types of evidence cannot completely cover electronic data, so the emergence of the "independent evidence theory" is not accidental. Electronic data is mostly presented in written form in the stage of evidence presentation, but its essence is virtual data, which cannot be directly perceived. With the development of science and technology, the forms of expression will become more diverse, while documentary evidence uses paper as the medium, which is mostly expressed in general. Text, which actually exists in physical space, is fundamentally different. The easily tampered nature of electronic data is in stark contrast to the reliability and strong stability of physical evidence, so electronic data is also not physical evidence. When it is difficult to distinguish the authenticity of electronic data, appraisal is an important means and way to assist the prosecution, defense, and trial to identify, but not all electronic data needs to be authenticated, so the "appraisal opinion" is unreasonable. Therefore, at a time when audio-visual materials are gradually fading out of people's vision and being eliminated by the times, "Independent Evidence Theory" complies with the needs of the development of the times and meets the objective needs of the current surge in criminal cases involving electronic data. "The

ISSN: 2688-8653

future electronic data will inevitably become one of the most frequently used evidence" development trend.

As a product of technological development, what distinguishes electronic data from other evidence is its virtuality and fragility. On the one hand, the data information contained in electronic data is not attached to human expression, and is separated from objective things. It is stored in the virtual space in the form of binary code, and cannot directly reflect the facts of the case in a form visible to the naked eye. Therefore, electronic data cannot exist independently of the electronic medium. It must be converted into language perceptible by a specific program and output through electronic equipment. On the other hand, electronic data is extremely fragile. Through certain electronic equipment, the deletion and modification of electronic data can be realized. It is stored in the electronic medium in the form of binary code, and anyone can delete, modify, or even destroy or destroy the electronic data through its storage device, which makes the electronic data unable to reflect the facts related to the case, and thus loses the qualification of evidence. With the development of science and technology, it is no longer difficult for the network to remotely operate computer equipment, implant Trojan programs or directly invade the computer to delete, modify and destroy electronic data. A censored electronic data may not only fail to correctly reflect the facts of the case, but may even subvert the entire case and construct a completely opposite "truth". However, "the wild goose leaves traces, the wind leaves the sound", through professional technical means, the deletion and modification of electronic data is still traceable. Unlike other physical evidence that is difficult to restore or even permanently lost after damage, the modification and restoration of electronic data is a reversible process. Data deletion is not the same as data loss. Professional technical means can find clues of deletion and modification in the background database. According to these traces, data recovery can be achieved to a certain extent. However, whether the recovered data is true and complete cannot be judged by human senses alone, and it still needs to be identified through professional technical means. .

3. The Legitimacy of Electronic Data Authentication

In common law countries, the rule of authenticity is generally used to prove the authenticity of evidence and to preliminarily screen whether the evidence is admissible. "Jianzhen" comes from "authentication", which is an evidence system in which the evidence proposer proves the admissibility of the physical evidence he cites through the formal relevance of the evidence and the legality of the process. It solves the authenticity and reliability of the evidence form by proving the objective connection between the physical evidence and the facts of the case. However, not all evidence applies to the authenticity rule. According to its manifestation, evidence can be divided into verbal evidence and physical evidence. Verbal evidence can solve the problem of proving the relevance of his testimony and the facts of the case through the declarant's elaboration and refutation in court. Therefore, this rule only applies to the field of physical evidence. So what type of evidence does electronic data belong to in our country? The "Electronic Data Regulations" clearly exclude the digital form of oral evidence from the scope of electronic data , therefore, the authentication rules must be applied to the electronic data as the category of physical evidence. At the same time, due to the fragile nature of electronic data, anyone can tamper and change electronic data with the help of electronic equipment, and compared with traditional evidence, the operation method is more convenient. This determines that electronic data, compared with other physical evidence, need authenticity rules more urgently. It can even be said that authentication is the premise of the admissibility of all electronic data.

ISSN: 2688-8653

4. Problems Existing in Electronic Data Authentication

At present, there are only similar provisions on "evidence should be verified to be true" in my country's criminal proceedings, as well as the requirements for reviewing the three natures of evidence, but these provisions are not equivalent to the rules of authenticity, but are under the substantive reality of my country's criminal procedure law. Substantial requirements for the authenticity of evidence. For the first time in my country, the word "jianzhen" is used in the law in the "People's Courts Unified Evidence Regulations (Judicial Opinion Draft)", which makes it clear that for objectionable physical evidence (including electronic evidence and its indicative evidence), relevant personnel can testify in court. Identify, or determine the authenticity of evidence through authentication. At the same time, the regulations mainly adopt the mechanism of electronic data authentication from three aspects: legal sources, collection procedures, and custody chains. However, this provision is only a judicial opinion draft, which is still in the pilot stage and has not been universally applied nationwide. Therefore, in a strict sense, my country has not yet established the rules of authenticity, only the concept of authenticity is implied in individual legal norms.

On the other hand, with the improvement of scientific and technological level, the diversified development trend of criminal forms has put forward higher requirements for the scientific and technological level of my country's judiciary. Unfortunately, due to the differences in economic levels between regions, the intellectualization and technological level of judicial practice in many regions cannot fully meet the needs of case investigation. In this context, forensic identification is undoubtedly one of the main ways to ensure the authenticity of electronic data. However, in the practical process, judges lack the necessary ability to review and judge highly professional electronic data, which makes it difficult for electronic data to be substantively verified. Effective scrutiny, i.e. identification, has little effect on the adoption of electronic data. The root cause is that the authentication authority of electronic data in our country is insufficient at present. In judicial practice, the identification part of electronic data is undertaken by for-profit social identification agencies, which makes the impartiality of identification results not guaranteed and lacks sufficient social credibility. In addition, the identification process is not open and the standards are not uniform, which makes the authority of the electronic data identification results questioned.

Therefore, it is not only necessary to establish the authentication rules from the level of legal norms, but also to improve the guarantee mechanism for the operation of authentication rules from the practical level.

5. Reference and Construction of Electronic Data Authentication Rules

(1) Extraterritorial reference for electronic data authentication

U.S. authentication rules focus primarily on the Federal Rules of Evidence, in which Section 901(a) states that when the evidence is sufficient to establish that the matter at issue is the fact it is asserted, then the evidence meets the authentication and identification requirements, and the authentication The prerequisites and pre-procedures for the admissibility of genuine evidence. This article clearly stipulates that the authentication standard only needs to be The "sufficient to support" standard is not required to meet the "beyond all reasonable doubt" standard of conviction. Specifically, there are three types of authentication methods in the United States, including case authentication of evidence, self-authentication of evidence, and testimony of signed witnesses. Case verification is mainly to prove the authenticity of electronic data through circumstantial evidence; self-verification refers to the exemption from verification of evidence under certain conditions, mainly for electronic data such as public and

ISSN: 2688-8653

private documents; the testimony of signed witnesses only occurs in "When required by the law of the jurisdiction of the applicable law to which the validity of the instrument requires".

(2) China-based construction of electronic data authentication

In my country, the basis for constructing and perfecting electronic data authentication rules is to explicitly incorporate authentication rules into the evidence rule system.

First, clarify the principles of electronic data authentication. The purpose of authenticity verification is to ensure the reliability of the electronic data in form, to avoid the influence of the deletion of the data content on its evidence qualification, to prevent the tampered electronic data from subverting the facts of the case, falsifying the "truth" of the case, and adversely affecting the trial of the case . At the same time, through authentication, the identity of electronic data in the whole process of case investigation and trial can be ensured. Therefore, the authentication of electronic data must adhere to the principles of formal authenticity and identity.

Second, clarify the standards for authenticating electronic data. In the field of criminal procedure, the party presenting the evidence is obliged to prove the authenticity of the evidence presented, otherwise the evidence will not be admissible. Therefore, the party presenting the electronic data should be responsible for verifying the authenticity of the electronic data. Since our country is in the initial stage of the construction of authentication rules, the proof standard of "beyond reasonable doubt" is too strict, which is not conducive to the construction and development of authentication rules in our country. At the same time, electronic data has certain requirements for professional technical capabilities. Therefore, It is more appropriate to adopt the "preponderance of evidence standard" for electronic data authentication.

Furthermore, clarify the way of authenticating electronic data. The generation of electronic data records the process of the case and is not affected by the forensic process. The process of case investigation mainly involves the extraction and storage of electronic data, so that the authenticity of electronic data can be realized by proving the legitimacy of the data source and the integrity of the chain of custody of evidence. This requires investigators to collect evidence in accordance with laws and regulations during the process of collecting evidence, and make electronic data extraction records, indicating the time, location, evidence storage medium, personnel, tools and equipment of the evidence collection for verification; at the same time, in the evidence collection In the process of presenting to the court, make a record of the corresponding circulation to avoid loopholes in the handover record and affect the authenticity of the electronic data.

(3) Improvement of the electronic data forensic identification system

In addition to electronic documents endorsed by the state's credit and electronic data notarized by a notary public in accordance with the law, judicial authentication is also one of the most important ways to confirm the authenticity of evidence in my country. However, the complexity of forensic identification agencies has a certain impact on the fairness and credibility of electronic data identification. In this regard, we should scientifically set up identification agencies, and build an electronic data identification system with public security organs as the main and social identification agencies as a supplement. Starting from the initiation and supervision of forensic identification procedures, strengthen the neutrality and reliability of forensic identification.

In my country, the security protection work of computer information systems is under the overall management of the Ministry of Public Security, and the investigation of most criminal cases is also in charge of the public security organs. Therefore, the public security organs have the ability to undertake the identification of electronic data and reduce the time for the circulation of identification materials. , to improve the identification efficiency. However, in

ISSN: 2688-8653

view of the current situation of "there are few cases" in criminal cases in my country, only the departments above the provincial level are responsible for the appraisal work, and the workload of the provincial departments is too heavy; and electronic data appraisal requires a lot of investment in equipment and instruments, and appraisal agencies are set up in all local-level cities. It is inevitable that it is unrealistic. Therefore, when setting up an appraisal unit, you should consider the different needs of different regions and different cases in terms of level of secrets, appraisal difficulty, appraisal needs, and human resources. The establishment of each identification agency can meet the identification needs of itself and surrounding cities. At the same time, there are restrictions on the level selection of appraisal units. For example, the appraisal of electronic data must be inspected by public security organs at or above the municipal level, and only the same level or superior public security organs of the court of first instance can be entrusted to conduct forensic appraisal; For confidential cases, the public security organs at or above the provincial level shall be responsible for relevant appraisal matters. In addition, the Ministry of Public Security or the Provincial Public Security Department will select social appraisal institutions with high credibility nationwide to ease the pressure on the public security organs for appraisal.

At the same time, improve the accountability and punishment mechanism and establish a multi-faceted supervision model. Forensic appraisal in my country adopts the appraiser responsibility system, and the appraiser conducts appraisal independently according to the law, but the appraisal institution is the work unit of the appraiser, which provides the necessary testing instruments for the appraisal work, and identifies the appraisal opinion in the form of stamping the official seal. Behaviors should also be held accountable to the appraisal unit, so as to urge it to establish a dynamic supervision mechanism and strengthen the supervision and assessment of internal appraisal personnel. At the same time, industry associations and administrative supervision departments should establish a third-party supervision mechanism and an appraiser's integrity evaluation system, regularly publicize the evaluation results, and disclose their dishonest behavior. On this basis, establish an elimination and withdrawal mechanism, and cancel the qualifications of appraisers and institutions with particularly serious dishonesty. At the same time, according to the natural law of "survival of the fittest", orderly competition and healthy development of the industry are promoted. The Ministry of Justice should also, on the basis of improving the mechanism for handling judicial appraisal complaints, refine the circumstances of illegal punishment, clarify the "restricted areas" and "red lines" of practice activities, increase the penalties for violations, and "zero tolerance" for violations of laws and regulations, and step up the formulation of Relevant laws and regulations on penalties for illegal and illegal judicial appraisal acts.

Of course, with the development of science and technology, my country is actively exploring the application of emerging technologies such as blockchain in the judicial field, in order to realize the technical self-certification of electronic data and promote the intelligent development of the evidence system. However, at present, these emerging technologies have great limitations and security risks at the technical level, and cannot meet the evidentiary standards for criminal trials in my country. However, it is foreseeable that in the future judicial reform process, with the development of technology and the Perfect, new technologies such as blockchain will gradually enter the field of criminal litigation from the civil field, and greatly improve judicial efficiency and enhance judicial credibility.

Acknowledgments

Fund Project: The 2021 Postgraduate Research and Practice Innovation Plan Project of Jiangsu Province "Research on Criminal Electronic Data Cross-examination Rules" (SJCX21-1073).

ISSN: 2688-8653

References

[1] Zhang Qifei, Yu Chunchun. The construction of an electronic data authentication mechanism for public security organs [J]. Journal of Guangxi Police College, 2020,33(06):52.

[2] Fu Yilong, Zhou Guoping, Li Liang. The Value and Realization of Electronic Evidence Rules [J]. Journal of Hubei Police Academy, 2012,25(10):151-154.

[3] He Jiahong, Liu Pinxin. Research on Electronic Evidence Law [M]. Beijing: Law Press, 2002: 535.

[4] Liu Zhenyu. The reform and development of forensic identification work in the new era [J]. China Forensic Identification, 2018, (01): 3.