Advances in Social Science, Education and Humanities Research (ASSEHR), volume 180
2018 International Conference on Education Science and Social Development (ESSD 2018)

Electronic-Date Evidence Regulation and Improvement of Public Security Cases

Jian Wei
Security Department
Chongqing Police Academy
Chongqing, China
Email: 413160184@qq.com

***Abstract*-With the advent of the era of Internet big data, electronic data has penetrated into all aspects of our lives and gradually became the legal evidence of the three major lawsuits in China. In the field of public security law enforcement, it has also become one of the important evidence of public security punishment. The evidence is of great significance to promote the Internet + economic and social development in the new era, to achieve justice and justice of law enforcement, and to protect the rights and interests of the people. Based on the intangible, vast, integrated-character of-electronic data evidence, this article probes into the problems of the "vacuum" of the existing security law concerning it, lack of evidence rules, and non-standard law enforcement practice, and proposes heavy-handed police electronic data in the field of legislation, perfecting the third party identification procedures, establishing the hearsay evidence and best evidence rule. As a result, the judicial administrative department will further improve the procedures of electronic data evidence regulation in light of this theory.**

Keywords: electronic data evidence; Procedural perfection; countermeasures

I. INTRODUCTION

As the escort to the social and economic development of the information age the law, the regulation of electronic data evidence in administrative law enforcement and judicial field plays a major role, especially in the field of public security penalties in electronic data evidence effect more obvious. However, the lack of existing legal provisions and the lack of practices in practice and the evidence of electronic data do not match the importance of law enforcement activities. This paper discusses the characteristics of electronic data and the existence of legal problems, and puts forward some improvement measures in theory and practice in order to attach great importance.

II. THE IMPORTANCE AND DEFINITION OF ELECTRONIC DATA EVIDENCE AND THE DEFINITION OF THE CHARACTERISTICS.

A. The Importance of Electronic Data Evidence in Judicial Administrative Law Enforcement.

In January 2016, Haidian district people's court heard the case of the spread of pornographic materials by Shenzhen Qiaosheng technology co., LTD. ("-the fast broadcasting case-"). In this case, the social attention is extremely high, and the two sides have gained a lot of support on the Internet, especially the application of electronic data evidence in the case to focus on the judicial field. Against the case exposed electronic data evidence applicable legal issues, projects and the ministry of public security issued on the extraction and examination for the criminal cases handled by collecting judgment provisions on some issues of electronic data. This is more typical of electronic data evidence used in the judiciary.

In the field of public security police law enforcement within the electronic data evidence used in the following categories cases: fraud, bawdy pornography, gambling remain the first three. The report of fake, illegal and adverse comments has increased. And these cases are typical and illegal activities, the use of the Internet means based on computer and its network of electronic data evidence collected and identified difficulties brought case penalties for no small difficulty.

B. Definition of Electronic Date Evidence.

Electronic data is the source of legal evidence. In 2012, the newly revised criminal procedure law, electronic data as legal evidence first appeared in the form of law. In 2014, the public security organ of the ministry of public security (hereinafter referred to as the "administrative procedures regulations") clarified the electronic data as one of the evidence types of public security administrative law enforcement. The administrative department of public security deals with the case program regulations system on the premise of no conflict with upper law, and sets forth it in this form of rules, but not in the form of "laws and administrative regulations" to confirm it. As for the concept of electronic data, it is not the same in theory and practice. It usually USES "electronic evidence" and "electronic data", but it has different definitions. The connotation of the two is consistent and the extension is slightly different. Generally speaking, the connotation of electronic evidence is broader, including analogue evidence and digital evidence. There is electronic evidence, such as electronic evidence, in the types of evidence provided in article 23 of the old administrative procedure rules. In 2005, the ministry of public security issued the "rules on the inspection and electronic evidence inspection of computer crime", which includes electronic data, storage media and electronic equipment. The electronic data evidence of public security case can be used for reference in criminal cases. Only index, and electronic data narrower meanings, word form of evidence, mainly exist in the computer, network and its accessory equipment, such as email, electronic data interchange, online chat, blog, microblog. This paper is consistent with the legal

evidence types in China, and it is consistent with the industry consensus, adopting the concept of electronic data, namely, electronic evidence in a narrow sense. Whether the evidence of the administrative case or the electronic data of criminal case, the essence of the content is the same, the stone of the other mountain can attack the jade, this article may as well learn from the criminal case concerning this kind of regulation.

C. Basic Characteristics of Electronic Data Evidence.

The characteristics of electronic data evidence directly influence the rule of evidence.

1) Intangible and virtual features. Intangible virtuality refers to the existence of electronic data evidence, which is not like physical evidence, which is directly exposed to us, and manifests and exists in the form of "field" in the form of information, text, message, knowledge and image. Physical evidence typically needs to occupy a certain physical space and can be directly touched by human beings. It is true that traditional evidence exists in a certain environment, but its existence is a "real reality", unlike electronic data evidence, which is a "virtual reality". From the point of view of evidence law, the influence of intangible virtuality on its evidence rule is mainly manifested in the problem of evidence collection and confirmation. Firstly, the interpretation of electronic data is inseparable from the computer and other electronic devices, which requires the relevant personnel to keep the corresponding hardware equipment when collecting evidence. Secondly, in the confirmation, we can't judge whether the electronic data really reflects the facts of the case with the naked eye, and we must rely on judicial expertise to help judge. Perhaps we are about to enter another era of forensic evidence, the age of electronic evidence.

2) Large amount of electronic data, rich contents and intuitive dynamics. The electronic devices in public security cases can store vast amounts of electronic data. The significance lies in that, with the exchange, integration and analysis of mass data, humans can predict their own behavior patterns and provide clues to the prediction of illegal crimes and investigation of cases. And the vast amount of electronic data has these characteristics to present the whole case in direct evidence. On the one hand, we can obtain direct evidence for the evidence of electronic data, but on the other hand, it makes it harder for us to obtain evidence. After all, there is a "needle in a haystack".

3) Integrity characteristics of electronic data. This is based on the extension of the second feature. Integrity requires that we gather evidence that should be comprehensive, to be able to prove that the facts of the case are not to be omitted from the fact that who has acted or not. If the evidence does not have full proof, it is necessary to combine other evidence to prove the case.

Electronic data, of course, not limited to the above characteristics, discussed include transnational, for example, the electronic data is essentially a kind of information, able to spread in cyberspace, thus easily across the jurisdiction of national boundaries, let the whole mankind living earth become a "global village".

III. THE ELECTRONIC DATA EVIDENCE FINDS THE CONFUSION AND THE REASON IN THE PUBLIC SECURITY CASE.

A. Absence of Law, Regulations, Local Law and Regulations.

First of all, we trace the evidence of electronic data in our country's entire legal system. In 2004, the electronic signature law and the provisions on the definition and content of electronic evidence of the provisions on the review and judgment of the examination and judgment of death penalty cases in 2010. In 2012, article 48 of the criminal appeals act stipulates electronic data as the statutory evidence. After the amendment of the civil procedure law and the administrative procedure law, it also clarified one of the legal types of electronic data evidence. In 2012, the supreme law issued the "interpretation of > of the criminal procedure law of the People's Republic of China" and further improved the evidence collection and examination of electronic data. In 2016, according to the exposure of electronic data evidence "quick" sowing case applicable law issues, projects and the ministry of public security issued concerning the collection for the criminal cases handled by extraction and review to determine provisions on some issues of electronic data. The regulation is the first time for China to regulate electronic data collection, extraction and review.

In 2014, the public security organ of the ministry of public security (hereinafter referred to as the "administrative case procedure regulation") clarified the electronic data as one of the evidence types of public security administrative law enforcement. This is regulated in the form of regulations, but it is not confirmed in the form of "laws and administrative regulations", and the validity level is open to discussion.

B. Practical Problems in Electronic Data.

1) Lack of expertise in forensic identification. In the practice of the public security investigation, security forces personnel and their own professional and technical personnel is basically a Sagittarius, professionalism and independence of its access to the electronic data is in doubt: first, the electronic evidence enough professionals. In the case of public security case investigation and forensics involved in electronic forensics, the personnel of the technical department only provide auxiliary work. The general public security police are prone to neglect, while the technical department has limited manpower. Second, the review of electronic data lacks technical guarantee. In general, the police will hand over relevant technical problems to the appraisal agency, and it is difficult for the appraisal agency to ensure that the appraisal results are realistic and objective. Thirdly, the evidence rule system of electronic data is not perfect.

2) The rules of the electronic data of public security cases are blank. Since the relative criminal cases of public security cases are relatively minor and the requirements of evidence are relatively low, the relevant evidence provisions are basically blank, or some of the relevant

provisions of criminal cases can be drawn directly. Relevant electronic data evidence rule system is not perfect criminal case: first, from the micro perspective, in the article 94 and 93 the Supreme Court has stressed the importance of electronic data integrity, authenticity, relevance and comprehensiveness, but how to carry out specific evaluation, only judicial interpretation stipulates very principles, such as "whether the case such as delete, modify, add" difficult to deal with complex judicial practice. Second, China's laws rely heavily on verification or inspection of electronic data in question, and the ministry of public security has published relevant technical rules. But there are still two big questions about electronic data: the authenticity of the electronic data itself and its expertise. For verification in our existing criminal law, administrative law rules, hearsay rule, the best evidence rule and the illegal evidence exclusion rule did not make clear a regulation, these are worthy of public security investigation electronic data forensics.

3) Incomplete evidence of electronic data evidence. Integrity is not only the absence of the evidence of the case, but also the "comprehensive extraction" of the evidence material. Public security cases by public security organs should be fully collecting evidence, but subject to large amount of electronic data, rich in content, intuitive dynamic and transnational characteristics as well as the subjective and objective factors, such as professional evidence collection comprehensive in reality will be discounted.

C. Objective reasons for the Characteristics of Electronic Data.

The characteristics of electronic data evidences make it more difficult to obtain evidence and prove it to some extent. Firstly, the electronic data is mainly concerned with its "authenticity" except for the examination of "legality" and "relevance". As to the real truth, it is impossible to verify directly, and the law can only be as close to the real truth as possible. Secondly, the development of science and technology has raised higher requirements for the law and the law has its own limitations. Traditional investigation and forensics measures have been developed to electronic forensics. The high technology of electronic data makes it difficult for public security police to directly form the "heart certificate" of the case through its examination. The application of electronic data is not ideal. Thirdly, electronic data, rich in content, intuitive dynamic performance make electronic data evidence directly, but on the other hand increased the difficulty we obtain evidence, after all, there are "looking for a needle in a haystack", "a drop in the bucket" meaning.

IV. THE ELECTRONIC DATA EVIDENCE USES THE RULE TO PERFECT THE PROPOSAL IN THE PUBLIC SECURITY CASE.

A. The Legislation Shall Improve the Relevant Provision.

There is a lack of legislation on electronic data in public order, only from the source. A review of its legislative process is a gradual process. In the field of public security and punishment law, only the ministry of public security's administrative procedures for handling administrative cases in 2014 clearly defined the electronic data as one of the evidence types of public security administrative law enforcement. This is regulated in the form of regulations, but it is not confirmed in the form of "laws and administrative regulations", and the validity level is open to discussion. And there is no other form a complete set of explanation and the relevant electronic data evidence system established, make security forces in the field of administrative law enforcement in such problems without access to relevant legal basis, only reference to criminal cases.

B. Review and Judgment of Electronic Data.

In view of the related characteristics of electronic data and problems in practice, it is suggested that relevant electronic data evidence rules should be established.

The three characteristics of authenticity, legality and relevance of electronic data are comprehensive requirements for its evidence ability and proof force. The current review of electronic data has many legal provisions, but there are still many areas that need to be clarified and combed:

1) Evidence capability of electronic data.

a) The application of hearsay rules of evidence. This is based on the electronic data evidence feature intangible virtuality and the special carrier extension. The hearsay rule is intended to exclude hearsay evidence in the trial, and in principle the witness testimony must be examined in court. We can draw lessons from the hearsay evidence rule in criminal cases in public security cases. Although the public security case evidence cross-examination and adopt right based on the security forces, but in the case of some important security electronic data stored in computers and other electronic equipment, and electronic equipment can't testify, so the electronic data in principle be regarded as anecdotal evidence. When applying the rule, the first step is to determine whether the electronic data is formed by artificial processing and production. After that, the person who requests the direct perception of the case, such as the electronic contract maker, input or modifier, etc should be required to testify.

b) Application of the best evidence rule. This rule is applicable to documentary evidence. Such evidence rules, the best evidence rules for electronic data, are also required in the security case investigation, requiring that the original or original storage medium of electronic data be submitted. Copies of electronic data, as long as those through computers and other electronic equipment to print on paper or storage, recording, reproduction optics medium or magnetic medium material, can accurately reflect the information expressed by the electronic data, electronic data reliability guarantee conditions, and is complete, it has evidence ability. This rule can be used in the collection and examination of electronic data evidence in the security case investigation.

2) Proof of electronic data.

Public security police are both collectors and examiners of electronic data in public security cases. Electronic data that censorship is not only a legal problem,

or a logical problem, draw lessons from the criminal case, from the point of the Supreme Court interpretation, is the key to the electronic data integrity, and dependability (authenticity). In terms of integrity identification, this is a special review that takes into account that electronic-data are intangible, recoverable evidence. The integrity of electronic data includes the following-:_(1) whether the electronic data itself is complete. Usually, electronic equipment used in the generation, transmission and preservation of the electronic data with no trouble, no change of hardware and software, and no safety accident, is regarded as the complete equipment system. In terms of reliability, judges are either based on their own cognitive reasoning or judged by their opinions. In particular, the reliability guarantee condition of the foreword provides a judgment path for the judge. (2) whether the equipment dependent on the electronic data is complete.

C. Improvement of the Practical Work of Electronic Data Evidence.

1) Establishing rules for expert or third party assistant handling. Strengthening the professional degree of electronic data forensics and corroboration can be carried out in both internal and external ways. (1) To improve the cognition and professional level of public security police on electronic data. If the public security organ has a special agency, it engages in electronic forensics work; the technical department is engaged in identification and other work. In addition, public security may employ professionals from the public to provide technical assistance for the collection and analysis of electronic data.

For security case electronic data in the process of collection, extraction and analysis of the investigators technology level the demand is higher, on the basis of the traditional law, criminal investigation, public security of the public security police personnel and rarely have to adapt to the technical level, caused a public security organ "help", although has the legitimacy and necessity, but lack of legitimacy, and the defense question, therefore, should take legal ways to refine and implement technical assistance qualification of the expert and the third party, the meaning of the expert auxiliary people responsibilities, rights, obligations, selection and working rules, etc to make institutional arrangements; to strict experts or third-party auxiliary case the certification of expert evaluation and authentication institutions, appraiser set professional study and practice of electronic evidence standards, qualification is maintained by the specialized agencies, not only to investigate the professional technical ability, also includes the legal knowledge and the ability to appear in court, ensure its professionalism, neutrality and authority; to perfect the system of expert or the third party auxiliary investigators 'questions to testify, public security and summoned the parties may apply for people with specialized knowledge, after qualification examination in auxiliary, improve the use of electronic data evidence ability and the legal effect, find out the case facts.

2) Integrity protection of electronic data evidence extraction. In the case of public security, the public security police should take full evidence, and the burden of proof should be on the police, which require that the electronic data collection should be comprehensive. It is necessary to extract the electronic data evidence which is illegal, aggravated and heavy. It is also necessary to provide evidence of electronic data that is not illegal, mitigated, lenient, exempt from punishment, and where appropriate. Great importance should be attached to the extracts of electronic data. Besides accessories, the intactness of information extracted, electronic data, processing, storage, transmission and operation environment of information data relevant and applicable condition should be ensured, and the integrity of electronic data evidence should be ensured.

Limitations. The existing law regulations of electronic data security class are absent or insufficient. The existing electronic data evidence forensics and the corroboration rule refer to criminal law. The evidence is different from the traditional electronic data characteristics, which requires the public security law enforcement has the special provisions on the legislation and practice. The article puts forward the rules strengthening electronic data legislation, perfecting the third-party identification procedure, establishing hearsay evidence and the best evidence in the field of public security, which is helpful to the legislation and law enforcement in the future.

ACKNOWLEDGMENT

Fund project: this paper is one of the achievements of the research on the construction of electronic data evidence rule system under the big data perspective (project no.: r2018-02) of Chongqing Public Security Bureau.

REFERENCES

[1] Long Zongzhi. Evidence classification system and its reform [J]. Legal research, 2005 (5)

[2] Pei Yinling. The type of argument [J]. Chinese criminal law, 2009 (11).

[3] He Jiahong. Evidence learning BBS (volume 3) [M].China procuratorial publishing house, 2001(321).

[4] He Jiahong, liupinxin. Evidence law [M]. Law press, 2012 (162).