

The Dilemma of Original Storage Media Rules in the View of Electronic Data and the Path of Improvement

Yao Zhang, Xinying Yang

School of Law, Southwest Minzu University, Chengdu 610200, China

Abstract

The continuous development of electronic science and technology to the traditional evidence model has brought impact, the original storage media rules in China has a pivotal position, but with the continuous development of science and technology, in the field of electronic data, this rule on the one hand, the lack of concern for the rights of the rights, on the other hand, it seems that its guarantee of the authenticity of the evidence is also being challenged, this paper from the current legal provisions of China's original media rules for electronic data and the existence of problems, analysis of the causes of the problem, and put forward the improvement path.

Keywords

Electronic Data; Original Storage Media Rules; Principle of Proportionality.

1. Introduction

According to the "on the collection and extraction of criminal cases and review and judgment of electronic data on a number of issues," the first provision: "electronic data is the case formed in the process of occurrence, stored in digital form, processing, transmission, to prove the facts of the case data." This provision indicates that the distinction between electronic data evidence and other evidence lies in the difference of its carrier. The carrier of electronic data consists of signal codes, which are stored in information devices and exists along with modern information technology and information systems. Combined with the prevailing evidence materials in China, as well as the characteristics of electronic data evidence, its concept can be summarized as follows: electronic data evidence refers to all materials and their derivatives that exist in electronic form and can be used to prove the facts of the case. In essence, it refers to all kinds of electronic data generated, sent, received or stored by electronic, optical, magnetic or similar means.

China is one of the few countries to typify evidence. 2012 electronic data into the law, formally become a member of the types of evidence, but the theory and practice of the authenticity of electronic data has never stopped. A scientific electronic data evidence needs the support of two links, the first is to ensure its originality, authenticity, integrity, legality and relevance in terms of source, forensics, content and preservation; the second is the need for reasonable and reliable interpretation of the facts reflected by electronic data by people with professional knowledge. The former can be described as formally true, and the latter can be described as substantively true. The form of electronic data authenticity is an electronic evidence to reflect the objective facts of the case of the antecedent elements, if the electronic data itself does not have objective authenticity, then the facts reflected will also produce bias, and thus lose the evidence qualification. On the current judicial practice, in the forensic level, the original storage media rules become an important element of electronic data authenticity judgment, but whether the rule itself is reasonable, and what is worth improving, still need to be further discussed.

2. The Original Storage Medium: The Best Rules of Evidence in the Field of Electronic Data

The best evidence rule, also known as the original document rule, is an important rule of evidence in the common law system, and the best evidence rule holds that “a party who relies on the content of a document, rather than the document itself, as evidence must present original evidence of the document's content.”

The best evidence rule is to determine the best evidence status of the original textual material and to confirm that it is the main object of consideration for the judge to restore the facts of the case, with the principle that the original textual material is the best evidence and the exception that non-original textual material is the best evidence under other circumstances (such as legal regulations). [1]

In 2016, “on the collection and extraction of criminal cases and review and judgment of electronic data” Article 5, Articles 8 to 10, 2019 Ministry of Public Security “public security organs for electronic data forensics rules for criminal cases” Chapter II, Section 1, 2, 3, 2021 “Supreme People's Court on the application of the <PRC Criminal Procedure Law> interpretation” Article 110, 111 and other provisions clarify the status of the original storage media: whether the seizure and sealing of the original storage media is an important criterion for judging the authenticity of electronic evidence, the original storage media seizure and sealing state is an important step in reviewing the integrity of electronic data. At the same time, the original data storage media rules apply to the process: the investigative authorities in electronic data forensics, in principle, should seize the original electronic data storage media for seizure, and for sealing. Here “seizure” processing is not only the physical sense of the seizure, including the wireless communication function of the storage media to take signal shielding, signal blocking and other technical sealing. Seizure, the relevant personnel to understand the situation of the original storage media and take appropriate protective measures, if the original storage media are not collected, it should be noted in the deposition transcript, including the reasons for not seizing the original storage media transfer, the original storage media storage location, the collection and extraction process, electronic data sources and other information.

The jurisprudence of the original storage medium rule for electronic data as seen in the above provisions lies in the spirit of the best evidence rule. The best evidence rule is often applied to documentary evidence, and the field of electronic evidence is analogous in theory to the spirit inherent in this rule.

From the practical level, the application of the original storage media rules also appears to be particularly important: First, throughout the world, although many countries require electronic communication data for written or other easily identifiable form, but after doing so, usually only reflect the content of the electronic document information, and the document related to the subsidiary information, associated traces, system environment information, etc. usually cannot be reflected. And these information for the investigation of the facts of the case is of great significance, so countries generally also on the original storage medium provisions [2]; at the same time, the original storage medium is required because if the electronic data extraction or copying to other storage media, the process may damage and destroy the electronic data and weaken the authenticity of the data; finally must also have to the original storage medium sealing provisions, which is in order to Protect the dynamic security of electronic data, electronic equipment, electronic data stored in electronic equipment is easy to be deleted, with the leap forward in information technology, and even data information and traces of remote erasure, and the process is difficult to be found, even if the development of detection technology, but in order to meet the economic and efficiency requirements, sealing the original storage media is still a common practice in many countries.

2. Challenges to the original storage media rules caused by technological developments

(1) The original storage rules of electronic data are not conducive to the protection of rights holders' rights

In the era of big data there are both physical detective acts that unfold in physical space with material as the medium and data detective acts that unfold in data space with data as the medium. [3]

In physical space, search is often preceded by seizure, because the forensics officer needs to search before he can find the items that should be seized in the case of unknown evidence location. And in the virtual space, electronic data storage media can be analogous to the aforementioned physical space that needs to be searched, it becomes a crime site in the data space, "isolated electronic files such as a document, a picture is a small 'field' that can tell a small story; if it is kept in the electronic media, the electronic media is a big 'field' can tell a big story" [4] so the first seizure of electronic data or electronic data storage media to conduct a comprehensive search of electronic data has become the norm of electronic data forensics. [5]

This generalized method of evidence collection, in emphasizing the authenticity of electronic evidence, while ignoring the protection of the rights of the rights holder. The provisions on the collection, extraction and review of electronic data in criminal cases adopt two approaches to electronic data collection: scholars summarize them as "one collection" and "separate extraction". The former refers to the seizure of the original storage media for electronic data, and the latter refers to the separate extraction of electronic data itself (divided into on-site extraction and online extraction). Although the former has search approval procedures (approval of the person in charge of public security organs above the county level), but this mode" will not only interfere with the basic rights carried by the electronic data of the case, but also violate the property rights of the original storage media and the basic rights carried by the electronic data stored therein and unrelated to the case. "The latter does not provide for the corresponding approval process. [6] The generalization of data collection has become a common phenomenon in judicial practice, and the weakness of the protection of rights holders will lead to adverse social effects.

Thus, in the era of big data development, even though a complete set of restrictions on seizure procedures has been developed in the past, with the change of technology, the practice of placing a search before seizure still needs more regulation and improvement.

(2) The use of original storage media is also difficult to guarantee the authenticity

The necessity of sealing the original storage media was discussed in the previous section, but the authenticity of the electronic data cannot be guaranteed by sealing the original data storage media.

Evidence rules require relevance, in terms of traditional documentary evidence, its content and storage media are inextricably linked, even to a considerable extent with homogeneity, if the storage medium does not change, its content often does not change. And electronic data is different from the documentary evidence, its content and its carrier is not so closely linked between the two is often one-to-many, many-to-one, many-to-many relationship, and as evidence of the use of the content rather than the carrier. [8] the authentication of the storage medium is also difficult to achieve for the authentication of the content of the electronic data therein, with the continuous development of technology, in the context of cloud computing, the use of data fragments distributed and shared, the cloud computing environment is rapidly changing, the data coverage process is rapid [7], even if the original storage medium is mastered it is difficult to ensure that the data changes, at the same time, the device encryption technology will hinder the recovery of data, at this time the original storage medium even if existence is also difficult to play a useful role.

3. The Optimization and Improvement of the Original Storage Media Rules

(1) Application of the principle of proportionality

The connotation of the principle of proportionality includes: constitutionality, validity, necessity, and the principle of proportionality in a narrow sense, while the combination of the above four points forms the principle of proportionality in a broad sense. [9] The principle of proportionality was born to reconcile the national interest and the public interest in case of conflict, in order to seek a relatively reasonable result without excessive imbalance.

As mentioned above, the current judicial practice pays too much attention to the authenticity of electronic data, while ignoring the personal interests of citizens, in this case, the forensics of electronic data when the introduction of the principle of proportionality to regulate.

Thinking in the positive direction, the problem to be solved is how to regulate the forensics of electronic data. Combined with the content of the principle of proportionality, first of all, in line with the level at which the Constitution, to clarify what rights are absolute areas of protection, and what rights have room for concessions, such as human dignity as the most basic human rights deserve to be the strictest protection, while freedom of communication, communication secrets and other rights can be compromised when in conflict with the national interest.

And validity means that the means can effectively achieve the purpose, which can also be called the fitness for purpose of the means. The validity requirement itself is an empirical judgment, and although there is a certain tolerance for error, in practice, there should still be a reasonable division of responsibilities between engineering and technical staff and reviewers, and continuous accumulation of review experience of the case-handling authorities, for example, when the prosecutors browse electronic data, they should pay attention to the use of statistics and markers, so that the review personnel have an overall understanding for the follow-up work to plan, and when conducting business operations, they can start from the composition of the crime and dig around the needs of the charges and proof. [10]

Necessity is reflected in the field of electronic data is actually the relevance of the forensic judgment. As mentioned above, China adopts a generalized forensic evidence, in terms of the premise of electronic data search, what degree of search and seizure can be carried out, China currently has no clear provisions, as long as the search can be carried out based on the purpose justified. The practice of ignoring the relevance of the search object and the search target will expand the scope of the search indefinitely, so the content of the search should be made specific, and the case officer should not start a direct search when he or she only has the tendency of mere suspicion, but needs relevant facts or reasons to show the existence of relevance in order to conduct a search, especially in the field of the privacy of the relator should improve the standard of search and seizure, so as to maximize the protection of the interests of the opponent. The principle of proportionality, in a narrow sense, is really a generalization of the application of the principle of proportionality, i.e., a step-by-step review of constitutionality, consideration of the effectiveness of the means, and necessity, followed by an overall weighing of interests, comparing the value of the goals achievable by the means at the two ends of the scale and the harm to civil rights.

(2) Giving investigators more autonomy on a macro level

The rigid requirement for the original storage media will affect the investigation activities, because when the investigating authority explicitly does not follow the original storage media rule for evidence, then the evidence may be found by the court as lacking authenticity or integrity, and its investigation activities will certainly be limited.

If the original storage media rules must exist as the best evidence rules, then the scope of application of the original storage media rules can be expanded to seek a balance with reality, such as expanding the circumstances without collecting the original storage media. In fact, in

the current judicial practice, although theoretically has been formed in the process to protect the authenticity of the original storage media rules. However, the referee documents show that the existence of electronic data storage media only about 10% of the cases, the public prosecution of electronic data is still mainly in the form of printouts, photocopies, screenshots of pages and other text images [11], because the original storage media itself there are also operational difficulties, a requirement of the original storage media is not realistic.

In the future, in the existing provisions of the original storage media “cannot be sealed” or “inconvenient to move” in addition to other circumstances, in the protection of the collection of electronic data authenticity and integrity of the basis, by giving investigators the choice and discretion whether to extract, copy electronic data without seizing the original storage media forensic model, at the same time, to actively explore alternatives to the original storage media, and actively call for the use of new technologies to protect the rights of the rights holders while increasing the objectivity and reliability of electronic data.

4. Summary

In the present day, the original storage media rules still enjoy an important position in the field of electronic data in terms of forensics, and the original storage media rules are now negligent in protecting the rights of rights holders. At the same time, the development of technology also brings impact on its authenticity guarantee, on the one hand, the rules should be regulated in the process of seizure priority over search and set the threshold. On the other hand, to highlight the use of the principle of proportionality in the process of forensics, to reduce the damage to the rights of the rights holder, should also give investigators the right to choose the original storage media, in order to be more flexible with the practice, to help the operation of intelligent justice.

References

- [1] Cui Xueli: “Best Evidence Rules in Electronic Evidence Based on the Internet,” in Journal of Shanghai Law School (Rule of Law Series), No. 3, 2019.
- [2] Chen Yongsheng: “On the Institutional Framework of Electronic Data Search and Seizure,” in Global Law Review, No. 1, 2019.
- [3] He Jun: “Research on the Legal Nature and Regulatory Path of Data Investigation Acts”, in Journal of the Chinese People's Public Security University (Social Science Edition), Vol. 1, 2021.
- [4] Liu Pinxin: “The Basic Theory of Electronic Evidence,” in Journal of State Prosecutors, No. 1, 2017.
- [5] Wu Tong: “Research on the Relevance of Electronic Data Search and Seizure Acts”, in Journal of the People's Public Security University of China (Social Science Edition), Vol. 5, 2021.
- [6] Xie Dengke: “On the Protection of Rights in Electronic Data Collection”, in Journal of Lanzhou Studies, No. 12, 2020.
- [7] Pei Wei: “On Carrier Seizure in Criminal E-Discovery,” in Journal of Chinese Criminal Law, Vol. 4, 2020.
- [8] Xu Lanchuan, Lu Jianming, Wang Xinyu and Xu Tao: “E-discovery in the cloud computing environment: challenges and countermeasures,” in Criminal Technology, Vol. 42, No. 2, 2017, pp. 151-156.
- [9] Fan Jianhong: “The principle of proportionality in the EU and Germany - connotation, origin, application and reference in China”, in Journal of Zhejiang University (Humanities and Social Sciences Edition), Vol. 30, No. 5, 2000.
- [10] Zhao Xianwei, Liu Zheng, and Xu Yan: “The Realization Path of Massive Electronic Data Review”, in China Judicial Identification, Vol. 1, 2022.

- [11] Hu Ming: "The Positioning of Electronic Data in the Criminal Evidence System and the Rules of Review and Judgment - Analysis Based on the Judgment Document of the Online Counterfeit Crime Case", in Jurisprudence Research, 2019, No. 2, p. 177.