The Dilemma and Breakthrough of Data Identification in Electronic Lawsuits

Jie Jiang*

School of Law and Public Affairs, Nanjing University of Information Science & Technology, Nanjing, China

*Corresponding author, e-mail: nuistjj@163.com

DOI: 10.37420/j.mlr.2021.011

***Abstract**: The electronic lawsuit is an important engine driving the information age. The scientific and orderly identification of massive data involved in lawsuits has become a key factor for all participants and the public to trust the new adjudication form. It is urgent to actively reconstruct a compliant and reasonable data identification mechanism on the basis of understanding risks faced by current activities of data identification in complex environments. It will develop the digital economy, improve the quality of life in our communities, and promote technologies.*

***Key words**: electronic lawsuits; data identification; breakthrough of dilemma; reconstructing rules*

Introduction

With the rapid development of Internet technologies (such as big data, cloud computing, internet of things), the data transferred on the Internet is increasing. Data has become a key production factor that plays an irreplaceable position in economic and social resource structure.

Data evidence gradually highlights its unique position in the judicial process. "Electronic evidence has become the new king of evidence in the information age." (He & Liu, 2013) It continues to show a situation that the social relationship with the centralized regulation of substantive law is difficult to separate. In electronic lawsuits, a large number of materials and their derivatives that exist in digital form and can be used to prove the facts of specific cases are characterized by invisibility, infinity, dependence, fragility, traceability, etc. In the dynamic life cycle of collecting, storing, analyzing, applying, and circulating as the scientific basis for ascertaining facts, it is gradually exposed contradictions and conflicts between truth and efficiency, verifying facts and protecting privacy, and other public and private interests. It is urgent to actively reconstruct the data identification mechanism adapted to the digital strategies.

Analysis on the Characteristics of Data Evidence in Electronic Lawsuits

Compared with the traditional forms of evidence, the massive data evidence involved in electronic

lawsuits is invisible because it exists in the virtual space, infinite because it can be easily and accurately copied, dependent because it needs a physical carrier, fragile because it is placed in the environment of a strong technical system, traceable because each step of operation will have traces, and other important characteristics, corresponding collecting the processes of proof, crossing examination and certificating truths to be further strictly regulated.

Intangibility

For a long time, the academic and practical circles have generally recognized the existence in the material world as physical evidence, the existence in the spiritual world as verbal evidence, and the existence in the conceptual world as judicial cognition composed of principles and laws. In electronic lawsuits, data evidence takes the information resources of the virtual field as an important carrier, which is different from the intangible form of traditional evidence, making it difficult to apply the original qualification rule. There are problems in evidence collection, certificate storage, and authentication.

Infinity

Various types of massive data evidence involved in various electronic lawsuits belong to information resources, which can achieve the perfect replication in the computer environment, and there is almost no replication cost, resulting in an obvious infinite volume of data evidence, which can coexist with a large number of copies at the same time.

Dependencies

Although there is no entity of data evidence in electronic lawsuits, it must be carried by a certain physical medium. The interrelated hardware media and software system together form an overall architecture with some specific functions. Finally, the data evidence presented in the form of documents, images, video and audio is attached to the system, and various changes may have been generated through many instructions in the process of internal information processing, which affects the rapid determination of evidence admissibility to a certain extent.

Vulnerability

Generally speaking, the traditional forms of evidence such as physical evidence and documentary evidence have strong stability, high tampering cost, and are easy to be exposed. For example, the documentary evidence with paper as the carrier not only expresses the author's thoughts through the paper content but also includes a variety of relevant information elements such as paper material, pen and ink attributes, and the author's handwriting, which is relatively difficult to forge. In electronic lawsuits, the data evidence is relatively fragile, which may be damaged due to operational errors, or stolen or damaged due to malicious intrusion. It is difficult to identify authenticity.

Traceability

The characteristics of the traces left by everything on the Internet make every step of the whole process of the creation, modification, archiving, backup and circulation of data evidence in electronic lawsuits have clear traces in the information system, and even many deletion behaviors can be recovered through technical methods, making the data evidence different from the physical evidence in the real physical space.

The Dilemma of Data Identification in Electronic Lawsuits

Data identification in electronic lawsuits is a dynamic process involving many parties. Especially, the virtualization and distributed digital environment greatly increase the difficulty of data location and acquisition, the lower data control ability of all participants and the flexible storage mode adopted by information providers increase the risk of data loss, and the massive related information improves the difficulty of data identification. It is urgent to take a series of measures to improve the professionalism of forensic subjects, the compliance of forensic process, the scientific nature of forensic results, etc.

In the era of big data, the subject of judicial data identification has high professional requirements. It is often necessary to master not only enough judicial knowledge, but also a lot of data analyzing abilities, but also high character quality and good adaptability. The whole process of electronic lawsuits needs more rules and management, which will make all steps become regular. Keeping the results reasonable is an important judgemental criterion.

Virtualization and Distributed Digital Environment Aggravating the Difficulty of Data Acquisition

The data evidence involved in various electronic lawsuits is often scattered and stored randomly in data centers distributed in different countries and regions. Scattered and distributed virtualization platforms make data evidence often need to be obtained online, and it is difficult to directly obtain physical equipment carriers, especially the massive data located outside the domain is difficult to seize and seal. And a slight carelessness will affect the credibility of the evidence. Even if the difference between electronic evidence and traditional evidence is ignored, there will be a problem that the original storage medium is located abroad and it is inconvenient to detain and seal it by conventional means. Once the technical means such as network online extraction or remote inspection are improperly used, it will face the result of evidence loss. For example, when the public security organ of a certain place in China investigated an online MLM case, because the server was located in Hong Kong, the law enforcement officers obtained the electronic data of the business activities of the online mall by means of remote technical investigation and delivered the recorded CD to the judicial appraisal institution, but in the second instance, the defense argued that the MD5 value of the CD provided by the public security organ was different from that marked in the judicial expertise report, and the overseas server involved in the case had long been closed (Ye, 2020).

Participants' Controlling Ability and Flexible Storage of Providers Aggravating the

Risk of Data Loss

The mass data evidence involved in electronic litigation is often in the physical storage medium or network environment, especially the remote cloud environment, which is difficult for data owners to directly control. With the penetration of cloud services into all walks of life, cloud service providers often use virtual technology to recycle and redistribute data resources frequently. Continuous dynamic changes make the massive data on the platform easy to be released, which may lead to the old data being covered or polluted, and the relevant data evidence will be lost. Even if the part can be recovered by technical means, it may damage the integrity of original data, and then affect the validity of evidence.

Massive Related Information to Enhance the Difficulty of Data Identification

In the traditional sense, the objects of electronic data forensics are mostly stand-alone devices and electronic data storage media, mainly including personal computers, u disks, mobile hard disks, memory cards and other storage media, as well as mobile phones and other communication devices. Data related to the case is found through search and investigation. In recent years, with the unprecedented expansion of information networks and the rapid development of communication technology, the data evidence related to electronic litigation is widely stored in the cloud environment, with huge data volume, numerous nodes, and complex formats, including data sets of target users and non-target users and different data sets of the same user. A large number of virtual host data are mapped and stored on the same physical device, virtual machines rented by different users are mixed and stored in the same server, and a certain data set uploaded by users may be stored in different data centers in a scattered way, involving multiple physical storage media. Lots of related information adds the difficulty of mining accurate data and seriously threatens the data identification activities. It is difficult to mine key digital evidence from scattered and massive data. For example, in the case of E-rent Treasure of Anhui Yucheng group, Ding Ning and Ding Dian brothers used E-rent Treasure (P2P platform) to release a large amount of false information by fictitious borrowers and financing projects, illegally absorbed a large number of public funds with the bait of ultra-high annual interest rate, and wantonly squandered, transferred and concealed them. The E-rent Treasure involved in the case was built on the cloud platform. In the investigation stage, law enforcement officers spent half a year, successively transferring more than 300 virtual servers and conducting investigation and evidence collection. Due to the identification, investigation, and analysis of massive data, the evidence extraction and processing process is difficult.

Reconstruction of Data Identification Rules in Electronic Lawsuits

At the moment when information changes into the basis of power, the interaction between state power and civil rights presents a tense and interdependent relationship. The process of data identification in electronic lawsuits may infringe personal data privacy, and may also pose a threat to economic security, social security, or national security. On the basis of implementing the general rules such as relevance rules, legality rules, proportionality rules, best evidence rules, confession arbitrary rules, and corroboration evidence rules. Practically improved specific rules such as professional rules, timeliness rules, truth presumption rules, certified search rules, and auxiliary proof rules, and then take the following measures:

Establishing a Standardized Data Identification Process of Electronic Lawsuits

With the rapid development of global economic integration and the rapid development of science and technology, more emphasis is placed on maintaining public order, harmony and stability in the forensic identification of case data related to interconnected products and services. Data identification in electronic lawsuits needs evidence-based development, and it is urgent to construct a standardized data identification process in electronic lawsuits. We must build an objective, stable and timely framework for balancing public and private interests. On the one hand, it is necessary to clarify the subject, target, and potential data evidence of data identification. Establishing a strict review mechanism for data identification, and comprehensively considering supporting data and its wide sources in combination with specific cases. In particular, we should strengthen the mining of related data at the network level and online platform, and adopt more efficient, orderly, and technical forensic tools and clear forensic processes. On the other hand, for the acquisition of data evidence in special scenarios such as cloud environment, we should focus on building service middle stations including diversion of identification requests, unified allocation of resources, information audit feedback, etc., fully invoking technical resources, adopting distributed extraction and analysis methods, not only avoiding resource waste caused by information confusion and repeated identification. It also reduces the probability of infringing on public privacy, trade secrets, and even national security.

Improving the Supporting Mechanism of Environmental Data Evidence

Data evidence in electronic lawsuits includes content data evidence, subsidiary data evidence, and environmental data evidence. Taking the e-mail evidence stored in the cloud as an example, the e-mail content itself is content data evidence, while the record information generated in a series of processes such as e-mail creation, editing, sending, receiving, and deleting is subsidiary data evidence. It is urgent to further improve the supporting mechanism of auxiliary environmental data evidence in electronic lawsuits, not only strictly supervise the data recording system of service providers but also establish their assistance mechanism for evidence collection, so as to form a complete evidence chain that is more conducive to proving the authenticity, relevance, and legitimacy of data evidence.

Improving the Cross-border Data Forensics Collaboration Mechanism

Perfecting the cross-border data forensics coordination mechanism under the principle of respecting network sovereignty is the key link to strengthen international judicial cooperation without infringing on the interests of domestic cyberspace. Collaborative work should be carried out at least from the following aspects:

(1) Strengthening the collaboration of criminal data forensics. There is a strong consensus among countries on cross-border data forensics on issues such as international money laundering and terrorism-related crimes. However, there are often some differences in the program steps, process preparation and details in the specific case practice. It is urgent to further strengthen the cooperation in forensics of serious crime-related data and establish a simpler, more accurate and faster cross-border cooperation.

(2) Improving the rules of mutual accommodation of evidence collection means. There is no obvious conflict

between online extraction and online inspection in cross-border unilateral data forensics and the principle of a country's network sovereignty. Online extraction mainly refers to browsing, collecting and fixing foreign public data, and online inquest refers to logging in and obtaining evidence through the platform accounting number and password of suspects involved in the previous investigation. It is necessary for all countries to tolerate and give some assistance and support to these kinds of evidence collection.

(3) Establishment of special procedures for mutual legal assistance. The traditional ‘inverted U-shaped' process of judicial assistance often takes a long time and complicated process from the application of law enforcement agencies in the requesting country to the acceptance of feedback by law enforcement agencies in the respondent country, which obviously does not meet the actual needs of current data forensics. It is necessary to establish special procedures for mutual legal assistance to achieve effective and timely data forensics.

Accelerating the Improvement of the Technical System of Electronic Data Identification

It is necessary to make full use of various cutting-edge technologies to improve the data identification mechanism. It mainly includes digital signature technology, timestamp technology, disk mirroring technology, block-chain technology, parallel forensics technology, electronic evidence decryption analysis and recovery technology, etc. For example, digital signature refers to some data attached to the data unit or the cryptography transformation of the data unit. The data or transformation can enable the receiver of the data unit to confirm the source and integrity of the data unit, protect the data and prevent forgery. For another example, the key to the application of blockchain in the field of electronic evidence is to prove the authenticity of the evidence or how to obtain the recognition of the court, and the consensus mechanism, as one of the core contents of block-chain, can just solve this problem. The so-called consensus mechanism is simply understood as a way to reach a consensus. The blockchain can be regarded as a voting mechanism. As long as each node votes according to the preset consensus mechanism, the results will be effective for each node. For example, for a transaction, the consensus mechanism of a blockchain is that as long as more than half of the nodes agree, the transaction is effective as long as more than half of the nodes agree to the transaction. The purpose of obtaining evidence is to prove the facts of the case with evidence so that the evidence has the ability and power of evidence. The main body of the two reviews is the court, so as long as the court recognizes the evidence, the purpose will be achieved. Based on the same principle, take the court as the node and recognize the validity of the evidence if the conditions are met through a consensus mechanism. In other words, the blockchain's recognition of electronic evidence can produce a legal effect similar to notarization.

Conclusion

The innovation field built by the tide of digital intelligence has greatly improved social production efficiency, improved residents' quality of life, helped economic and social development, and fully demonstrated the incalculable value of data resources in the information age. With the development of evidence-based theory and the wide penetration of blockchain technology in the field of data identification, the security, accuracy, and usefulness of rapidly expanding data evidence have been greatly improved. If evidence rules cannot

keep up with the development of artificial intelligence, risks faced by citizens' basic rights and procedural justice will increase greatly. Public departments actively established a warning mechanism of data security and encouraged scientific and technological enterprises to concentrate on developing special tools for data identification. Many experts and scholars also put forward data identification schemes based on new technologies, and relevant enterprises actively improved the necessary information disclosure system and service information recording system. In particular, the digital signature technology, timestamp technology, disk mirroring technology, electronic evidence decryption analysis, and recovery technology are promoted at a high speed, so as to fully enhance the credibility of electronic litigation and promote the scientific construction of legal rules in the information age.

Funding

This study was supported by The Key Project of Philosophy and Social Science Research in Colleges and Universities in Jiangsu Province: "Research on Infringement Risks and Countermeasures of Data Identification in Electronic Lawsuits" [No. 2016ZDIXM021].

References

He, J. H., & Liu, P. X. (2013). *Evidence Law*. Beijing: Law Press.

Ye, Y. B. (2020). On the construction of diversified cross-border electronic forensics system. *Journal of people's Public Security University of China (Social Science Edition)*, 36(4), 11.