Scientific Research Publishing

Chinese Studies, 2023, 12, 80-90
https://www.scirp.org/journal/chnstd
ISSN Online: 2168-541X
ISSN Print: 2168-5428

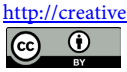
Similar Cases Retrieval for Illegal Electronic Data in Criminal Proceedings and Suggestions for Improving

Shuxi Zhou[1], Luying Dai[2]

[1]School of Law and Humanities, China University of Mining and Technology, Beijing, China
[2]School of Social Sciences, Lingnan University, Hong Kong, China
Email: na.jiang@bnu.edu.cn

How to cite this paper: Zhou, S. X., & Dai, L. Y. (2023). Similar Cases Retrieval for Illegal Electronic Data in Criminal Proceedings and Suggestions for Improving. *Chinese Studies, 12,* 80-90.
https://doi.org/10.4236/chnstd.2023.121008

Received: October 28, 2022
Accepted: February 10, 2023
Published: February 13, 2023



Abstract

In China's current system of rules for the exclusion of illegal evidence, the focus of adjustment is on the exclusion of illegal verbal evidence and illegal physical and documentary evidence. Based on the analysis of similar case search, this paper distills the following rules and legislative proposals: whether electronic data collected by illegal methods should be excluded, the evidence can be differentiated into defective evidence and illegal evidence according to the severity of the illegal methods, and the decision of whether to exclude it can be made on a case-by-case basis. Defective evidence can be corrected and adopted through legal procedures, but illegal evidence that cannot be examined to determine its authenticity, or the time, place and manner of its production or acquisition are in doubt and cannot provide the necessary proof or reasonable explanation should be excluded.

Keywords

Electronic Data, Technical Investigation, Illegal Evidence Exclusion, Similar Cases Retrieval

1. Introduction

With the advancement of technology and the development of social informatization, modern criminal activities show a clear trend towards digitization, and the form of electronic data is increasingly varied. For example, emails, instant messages, websites, electronic transaction records, files stored in electronic devices, IP addresses, etc. In judicial practice, the defense parties raised more and more requests for reviewing the legality of electronic data (Li et al., 2015). In 2016, the

Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Justice promulgated the "*Provisions on Several Issues Concerning the Collection, Extraction, Examination and Judgment of Electronic Data in Criminal Cases*" (hereinafter referred to as the "*Electronic Data Provisions*"), which addresses the types of electronic data, preservation methods, evidence collection procedures, and other contents, providing specific guidance for the collection, extraction, examination and judgment of electronic data. Illegal electronic data is evidence that violates the law and seriously affects the justice. In 2021, the Supreme People's Court amended the Article 113 of the "*Interpretation of Criminal Procedure Law*" to clarify the principle that the electronic data is "defective + cannot be corrected or reasonably explained = shall not to be used as the basis for the verdict". However, what is defective, how to define and judge illegal electronic data, there is still a lack of more detailed and clear standards and rules in China.

According to the "*Implementation Measures for the Uniform Application of Law by the Supreme People's Court*" which came into effect in 2021, nine types of cases should be subject to similar cases retrieval, including cases in which the public prosecution, the parties and their defenders or litigants submit guiding cases or similar cases in which the Supreme People's Court's effective decisions support their claims[1]. In the cases where the exclusion rules are unclear, a precise similar cases retrieval can help judges to accurately determine the difficult issues in the exclusion of illegal electronic data, and can effectively avoid some conflicts between the "prosecution, defense and trial parties". Since the outbreak of COVID-19 raged in China, online litigation rules have been applied to many cases in the prevention and control of infectious diseases. However, the specific rules for the exclusion of illegal electronic data are still being explored. As the review of the legality of electronic data has gradually become a long-term controversy in judicial practice, the core of improve the exclusion of illegal evidence rules for electronic data should be to curb the abuse of public power and to ensure the procedural justice in the collection process as well as the legality of the evidential material itself (Chen, 2022). This paper proposes adjudication rules for electronic data exclusion in similar cases by searching individual cases in the national court system, as a supplement to the loopholes in the ambiguous areas of legislation.

2. Discovery Based on Similar Cases Retrieval

Cases studied in this paper are drawn from the Alpha case library. The search was conducted on July 20, 2022, using "illegal evidence" and "electronic data" as specific keywords, and 166 samples in total were collected. The samples basically cover various court levels of the Higher People's Court, the Intermediate People's

[1]The samples in this paper are guiding cases, typical cases and cases with effective judgments by the Supreme People's Cour of P.R.C., reference cases and effective judgments by the High people's courts, and effective judgments issued by local intermediate people's courts and grassroots people's courts.

Court and the Basic-level People's Court, including different proceedings of the first trial, second trial and retrial. The range of cases covers crimes related to obstructing social management order, crimes against socialist market economic order, crimes against property, crimes against citizens' personal rights and democratic rights, crimes of corruption and bribery, and other related crimes. From the search results, it is basically able to achieve an objective, comprehensive and accurate reflection of the current application of the rules on the exclusion of illegal evidence in electronic data and the difficulties of the adjudication process in the Chinese court system.

The distribution of cases by year in **Figure 1** shows the trend of the number of cases under current situation: a general increase in the number of cases between 2014 to 2019, and a "precipitous" decline after 2020. In this regard, the possible reason is the strict application of the rules on the exclusion of illegal electronic data, or even exclude the application. However, based on the analysis of a large number of cases and interviews with judges from the Supreme People's Court, the implementation of normative documents and special enforcement reforms played an important role. Around 2019, the introduction of relevant laws and judicial interpretations further regulated the evidence collection process during inspection and investigation. The 2018 "*Supervision Law*" emphasizes that evidence collected by illegal methods should be excluded in accordance with the law and shall not be used as the basis for case judgement. In 2019, the Ministry of Public Security further regulated for the evidence collection process for electronic data regarding collection, extraction, prosecution, investigation experiments, testing and identification[2]. At the same time, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of Justice, etc. also issued a series of procedural provisions to further clarify that the three authorities have obligations to exclude illegal evidence in their respective stages of handling cases, so as to improve the investigation supervision and cooperation mechanism. Since then, in conjunction with the criminal proceedings, many disputes over the exclusion of illegal electronic data have been resolved prior to the court trial. It's means that before the court investigation, the public security authorities and the procuratorial authorities have already launched the review on electronic data and excluded some illegal evidence. In addition, in 2018, the Central Committee of the Communist Party of China (CPC) and the State Council issued the "*Notice on Carrying out Special Campaign against Gangs and Mafia*", the special campaign was escalated from earlier fights against Mafia-like crimes on a case-by-case basis to a new stage of declaring a war aiming to wipe out the gangs and Mafia, and under the overall deployment by the CPC Central Committee and the State Council, various departments have co-ordinated various means of governance, such as legal, economic and administrative measures, showing a high pressure and severe punishment in cracking down on the forces of gangs and mafia. And the leniency system in

[2]See Rules on Electronic Data Collection for Criminal Cases by Public Security Authorities.

pleading guilty and accepting punishment has been fully promoted in the criminal justice system. According to the interviews with defense attorneys, in the case of crimes that are punished strictly, the application for the exclusion of illegal evidence will be reduced when the accused pleaded guilty.

What is the exclusion rate of applications for illegal electronic data exclusion? From the results of case decisions, 98% of the cases were not excluded and only 2% of the cases were excluded (Figure 2). Why there are so few cases of electronic data illegal exclusion is the core in this paper. Penetrating the appearance of these data and dissecting the key areas where judges weigh in, case by case analysis is an important research method. Judicial cases show that the focus of the dispute lies in the fact that electronic data in violation of the law and seriously affecting justice. There are a number of differences of judges and comments among courts, procurators and defense parties. The following analyzes the controversy situation with specific similar cases.

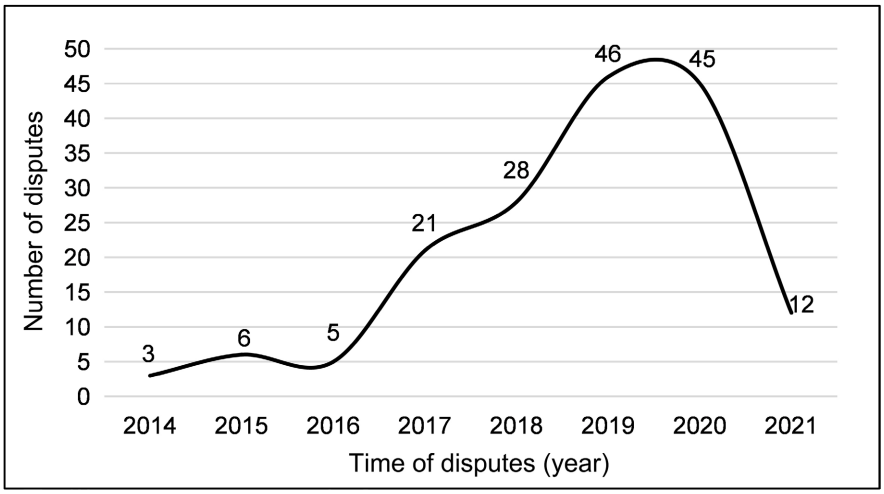


Figure 1. Distribution of disputed cases by years.

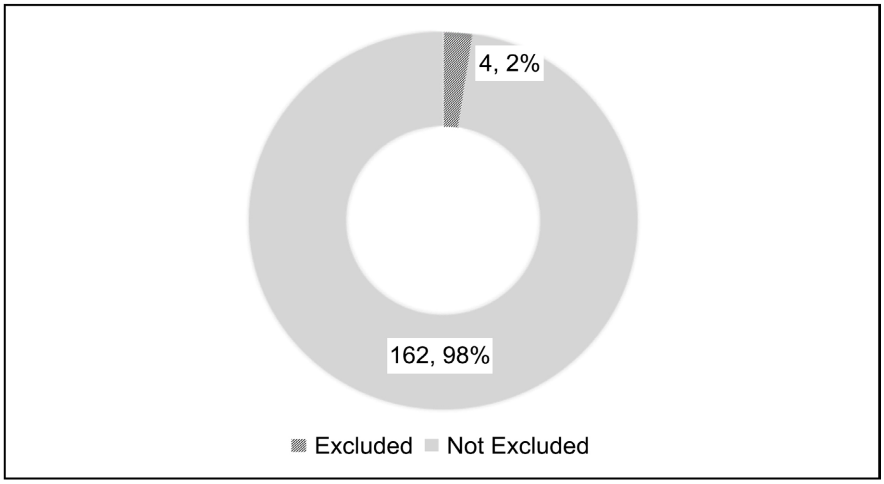


Figure 2. Application of illegal evidence exclusion to electronic data in similar cases retrieval.

3. Prominent Issues and Controversies of Illegal Electronic Data

In the causal reasoning where the rate of illegal electronic data exclusion is low, there are also some cases consensus and common acceptances between the prosecution and the defense are reached. For example, although the defense party suggested that the electronic data is defective, and there was no disagreement between the prosecution and defense parties on the nature of the defect; however, the investigative authorities provided the necessary proof or a reasonable explanation, which eventually accepted by the prosecution, defense and trial parties. In general, according to similar cases where defective electronic data is not excluded by judicial interpretations and the courts, discretionary standards can be summarized as follows: Firstly, the investigative and other authorities issued a statement or investigators to appear in court to explain the situation, correction or reasonable explanations to the process of evidence collection are made. Secondly, it does not belong to the situation that may seriously affect the judicial justice and needs to be excluded. Thirdly, impacted by the theory of substantive truth, the situation of evidence defective does not affect the determination of the evidence authenticity.

Based on the result of similar cases retrieval, the critical controversy between the prosecution and the defense as following. The outstanding divergences are mainly in how to judge the procedural defects in the collection and extraction of electronic data in the storage media? What standards to determine the defects of electronic data can be corrected? How to judge the degree of illegality of taking technical investigation and detective measures to collect electronic data before initiation of a case, and the degree of impact on justice and whether to set exceptions?

3.1. Procedural Issues in the Collection and Extraction of Electronic Data from Storage Media

According to Article 10 of the *Electronic Data Provisions*, only for objective reasons or inappropriate to fix electronic data by more appropriate methods, it can be done by printing or photographing, and the reasons should be indicated in the transcript, otherwise, the collection and extraction of electronic data by way of screenshots and printouts can easily face the question of legality. In the Alpha case library, the author chose the case of Lai's illegal possession of drugs as a typical case for analysis (**Table 1**)[3]. The WeChat records in this case belong to electronic data, and their collection and extraction should comply with the specific requirements of the *Electronic Data Provisions* for electronic data. The representativeness of the case is that the electronic data is not in compliance with the specifications in the process of evidence extraction and collection, and there are contradictions between the electronic data and other evidence. According to the provisions of the *Criminal Procedure Law*, the original storage

[3]See The Third Intermediate People's Court of Chongqing Municipality (2018) Criminal Retrial No. 5.

Table 1. Opinions of the prosecution, defense and trial parties in a typical case.

Case Number	Opinions of the Defense Party	Opinions of the Prosecution Party	Opinions of the Court
(2018) Yu03 Criminal Retrial No. 5	The screenshots of the defendant's mobile phone were of unknown origin.	The defendant acknowledged the content of the relevant WeChat records.	The public security authority did not comply with legal procedures and failed to provide a reasonable explanation for the source of the screenshots.
(2018) Yu1628 Criminal First Trial No. 374	The computer mainframe was not identical to the one seized by the investigator.	Because the law enforcement recorder was damaged, the audio and video recordings were not handed over with the case.	The investigators did not transfer the defendant's computer mainframe in a sealed state, and did not produce electronic data extraction transcripts.
(2017) Gan1224 Criminal First Trial No. 33	The investigators took technical investigative measures against the defendant a week before the case was initiated.	This case was a tip-off from other cases before the defendant was wiretapped.	This evidence was taken from technical investigative measures against the defendant before the case was initiated and should be excluded.

media (Lai Mouming's and Dong Mouhan's mobile phones) should have been seized in accordance with the law, but they were not seized and sealed in accordance with the law. Instead, "screenshots of WeChat content and other images" were submitted, which did not indicate the source of legality, and were ultimately not used as conclusive evidence. It is easy to see that the judge's discretion to exclude includes: if the collection and extraction of the relevant electronic data does not comply with the relevant technical standards, the original storage media and the backup of the electronic data were not transferred with the case, the video recording of the relevant activities resulted in the collection and extraction of electronic data cannot be reproduced, then the extracted electronic data cannot be used as the basis for the case determination. And for cases where there are conflicting evidence, the handling authorities should explain the defects of the electronic data, and if the reasonable explanations cannot be made to the source of the originally lost evidence that suddenly appear, the authenticity and legality of the electronic data cannot be identified.

Of course, from the perspective of general rules, in refining the rules of electronic data storage media, following issues should be considered simultaneously when determining whether to constitute a "violation of legal provisions": Firstly,

the investigative authorities did not make a sealed transcripts. In relevant cases regarding electronic data, the original storage media, such as computers and mobile phones, are seized without being sealed, without a transcript being made, without the sealing status being recorded or being sealed in a delayed manner. Secondly, the sealing of the original storage media is incomplete. From the perspective of evidence preservation, it should be ensured that the electronic data cannot be added, deleted or modified without unsealing the original storage media. Therefore, legality review on the procedure for electronic data storage media should focus on the seizure transcript, sealing state, source, uniqueness, dynamic flow of evidence, the presence of defacement and destruction and other aspects. The existence of incomplete, damaged and unknown sources of the original storage media can seriously affect the determination of the authenticity and integrity of the electronic data (Xie, 2022).

3.2. Issues regarding the Identification, Correction and Reasonable Interpretation of Electronic Data Defects

According to the provisions of Article 27 of the *Electronic Data Provisions*, for the investigative authorities, a statement of circumstances may only be used if it can reasonably explain the issue of defective electronic data. In the Alpha case library, the issue of defective identification and non-remediation of electronic data in the case of Huang's infringement of citizens' personal information is representative (**Table 1**)[4]. The controversial focus in terms of the electronic data in this case is that the investigating authorities did not transfer the seized computer host of Huang in a sealed state, and the investigating authorities did not make the electronic data extraction transcript, nor did they make the synchronous audio and video recording. For the defective electronic data that were "not transferred a sealed state", they may be used if the authenticity and integrity of the electronic data could be proved by any video and audio materials or reasonably interpreted by combining with special emergency and other objective reasons. However, in this case, once the electronic data was tampered with, it had a significant impact on the defendant's conviction and sentence. The defects associated with it, in the absence of correction or reasonable explanation, the corresponding harm of procedural violations will gradually "worsen" to a degree that seriously affects the administration of justice (Liang, 2020). The lesson for the investigating authorities in this case of illegal electronic data exclusion is that timely and effective correction or reasonable explanation of defective evidence is also an important step to dilute the "illegality" and avoid escalation of negative consequences.

3.3. The Exclusion of Electronic Data Collected by Technical Investigative and Detective Measures Taken prior to the Initiation of a Case

In China, the scope of application of technical investigative measures are strictly

[4]See The Primary People's Court of Luyi County of Henan Province (2018) Criminal Initial No. 374.

limited to cases of crimes against national security, crimes of terrorist activities, crimes of organizations of the triad nature, major drug crimes or other crimes that seriously endanger society. Supervisory authorities to investigate suspected major corruption and bribery and other crimes in office, according to the need, after strict approval procedures, can take technical investigative measures. In Alpha case library, the controversy between the prosecution and the defense over the smuggling, trafficking, transportation and manufacturing of drugs by Zhang and Liang was whether the electronic data collected by the public security authorities should be excluded if the time of taking technical investigation measures occurred before the criminal case was initiated[5]. As demonstrated in Table 1, the relevant authorities in this case bugged citizen Liang before seizing the drug suspicion and thus obtained electronic data such as cell phone call records and text messages. The point of view advocating exclusion is that the authorities in charge of the case approved to take technical investigation and detection later than the formation of the materials obtained by technical investigation and detection, meaning that technical investigation and detection measures were taken to collect materials before the case was filed, which is a manifestation of a serious violation of legal procedures, as well as a serious interference with citizens' right to privacy, and should be considered as a situation that seriously affects judicial justice (Zhang, 2021). However, from the prosecution's point of view, exceptions should be allowed for special crimes and when evidential materials with authenticity have been collected.

The result of the court's decision shows that it was more resolute in excluding illegal electronic data obtained prior to the filing of the case. In effect, it reiterated the position of the *Criminal Procedure Law* that "strict approval procedures" are required. Specifically, the prerequisite for strict approval is that the case has been filed as a criminal case, and that the electronic data collected through technical investigation measures should be carried out in accordance with the scope of the applicable case, the object of application and the period of application. This is also an integral part of implementing the principle of legal procedures and the principle of proportionality as described in *Criminal Procedure Law* in the application of technical investigative measures. If the authorities taking technical investigation and detective measures are allowed to make exceptions to this on a discretional basis, it would indeed contain a systemic danger of possible serious violations of human rights.

4. Suggestions for Improving the Rules of Adjudication of Similar Cases

In order to make up for the deficiencies of legislation and justice, and to improve the exclusion rules of illegal electronic data, the rules of adjudication in judicial practice of similar cases can be refined to guide the processing of individual cases. By summarizing the gist of the decisions in the above cases, the following

[5]See The Primary People's Court of Kang County of Gansu Province (2017) Criminal Initial No. 33.

provisions of the exclusion rules of illegal electronic data can be further clarified in the future judicial interpretation (Chipperius, 2009).

Firstly, the types of illegal electronic data should be specifically distinguished as defective evidence and illegal evidence, on which the corresponding adjudication rules are constructed. It's means that the exclusion of electronic data cannot be generalized. Whether the electronic data collected by illegal methods should be excluded, can be based on the severity of the illegal methods, on which the evidence will be distinguished as defective evidence and illegal evidence. The decision whether to exclude will be dependent on the specific circumstances: defective evidence can be corrected through legal procedures and then adopted; while the illegal evidence for which the authenticity cannot be proved, or the production, acquisition of time, place, manner, etc. are in doubt and cannot be proved with necessary evidence or reasonably explained shall be excluded.

Secondly, to focus on the review of the electronic data storage media, and actively realized the evidential function of the relevant audio and video recordings and other materials. Compared with other types of evidence, electronic data has a strong dependence on the storage medium. The basis and beginning of the review of electronic data is to review the storage medium. In the review of the legitimacy and authenticity of electronic data, the following measures can be conduct: checking the source of the storage media to determine whether the storage media from the crime scene and whether there is a unique identification; conducting analysis of the search, seizure and custody chain, the flow of transfer and the corresponding transcripts; reviewing whether the witnesses are qualified; confirming whether there is synchronized audio and video recording to corroborate the relevant data; and then conducting a comprehensive assessment.

The third is the special application of the exclusion rules for illegal electronic data obtained through technical investigation and detective measures. Because of the potential interference of technical investigation and detective measures on the basic rights of citizens, improving the exclusion rules for obtaining illegal electronic data through technical investigation and detective measures is in line with the constitutional goal of "respecting and safeguarding human rights". It is important to strictly examine the "legality" of the electronic data obtained through technical investigation and detective measures. First of all, the focus should be on whether the collection time is after the filing of the case and whether it is for the legal scope of the case. This is the most common procedural violations in practice. Secondly, in compliance with the requirements of "investigative needs" and "after strict approval procedures", from the principle of legal procedures and the principle of proportionality, to conduct a comprehensive review of the relevant materials including the legal documents, relevant information, the case officer's signature and seal, etc. transferred with the case to determine whether there is any violation of the provisions of the law. Thirdly, the materials collected through technical investigation and detective measures need to be verified by presentation, identification, cross-examination and other investigation proce-

dures in the court or can be even investigated and verified outside the court if necessary. The correction and reasonable interpretation for defective electronic data should also be strictly reviewed, so as to avoid the power abused again.

After court investigation or out-of-court verification, if there is contradictions between the electronic data collected through technical investigation and detective measures and other evidence in the case, the officer should correct the material or make a reasonable explanation, analyze whether the relevant material is true and whether it can form a complete chain of evidence with other evidence in the case. The electronic data for which the contradictions between the relevant data and other evidence in the case cannot be reasonably explained shall be excluded.

5. Conclusion

In the process of moving towards an information society and a privacy society, a stricter rule of law position should be adhered to in relation to illegal electronic data in criminal proceedings, based on the principle of adjudication of evidence. The way of collecting and extracting electronic data should be implemented legally. It should be carried out by more than two investigators and take the way of obtaining evidence with relevant technical standards. For the original storage medium of electronic data, it is generally necessary to take the way of seizure and storage, and make records to ensure that the content of electronic data cannot be added, deleted and modified without lifting the storage. After a series of identification, collection, preservation, analysis and identification, electronic data can be used to impeach the defendant to defend, reinforce verbal evidence and corroborate indirect evidence, affecting the judgment of the case (Riekkinen, 2019). In the process of specific adjudication, it is important to not only strictly follow the requirements of the principle of procedural legality and proportionality, but also be consistent with logic and rules of thumb. In practice, many judges are still overly cautious about the exclusion of illegal electronic data. As a result, in many individual cases, the police and prosecutors are successively given too much opportunity to make corrections, reasonable explanations, or to overemphasize the examination of authenticity. Even for some illegal electronic data, judges still carefully assess whether there are unexplained contradictions between them and other evidence on file, and whether it can form a complete chain of evidence before excluding them. In criminal defense, the application for exclusion of illegal electronic data through the retrieval of similar cases is expected to bridge some long-standing differences in understanding between the prosecution and defense, promote the consistency of judgment in similar cases, and improve the chances of such applications being accepted. For the judges, strengthening of the rules for the adjudication of illegal electronic data cases and implementing "zero tolerance" on the relevant investigation and detective measures that constitute serious violation of the law or seriously affect the justice, is conducive to reduce the influence of the supervision-centrism or investigation-centrism on the im-

plementation of the trial-centered litigation system reform.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

Project Source

The Supreme People's Court on "*Study on the Difficult Issues in the Application of the Leniency System of Confession and Punishment by the People's Courts*". The Procuratorial Theory Research project of the Supreme People's Procuratorate in 2022 "*Study on Legal Procedures and Evidence of Criminal Cases Involving Patients with Major Infectious Diseases*" (GJ2022D41).

References

Chen, R. (2022). Paradigm Reshaping of Electronic Evidence Review Judgment from Hybrid Review to Detached Review. *Hebei Jurisprudence, 7,* 46-72.

Chipperius (2009). *Methodology of Jurisprudence* (Translated by J. B. Jin). Law Press.

Li, H. et al. (2015). The Perfection of the Rule of excluding Evidence of Illegal Technical Investigation. *People's Procuratorate, 3,* 67-69.

Liang, K. (2020). On the Legal Regulation of Electronic Data Collection in Preliminary Investigation and Discussion with Long Zongzhi and Xie Dengke. *Chinese Journal of Criminal Law, 1,* 39-57.

Riekkinen, J. (2019). Electronic Evidence in Criminal Procedure: On the Effects of ICT and the Development towards the Network Society on the Life-Cycle of Evidence. *Digital Evidence and Electronic Signature Law Review, 16,* 6-10. https://doi.org/10.14296/deeslr.v16i0.5014

Xie, D. (2022). Technical Forensics of Electronic Data. *Journal of Legal Studies, 2,* 209-224.

Zhang, H. (2021). Research on the Rules for Reviewing Illegal Electronic Data in Criminal Proceedings. *Beijng Juridical Journal, 2,* 55-76.