International Journal of Law, Crime and Justice 64 (2021) 100453

Contents lists available at ScienceDirect

International Journal of Law, Crime and Justice

journal homepage: www.elsevier.com/locate/ijlcj

Rules of electronic data in criminal cases in China

Fan Yang [a], Jiao Feng [b,*]

[a] Law School, Yangzhou University, Yangzhou, China
[b] Law School, Zhejiang University of Finance & Economics, Hangzhou, China

ARTICLE INFO

Keywords:
Electronic data
Cybercrime
Criminal proceedings
Blockchain
Privacy rights

ABSTRACT

As the core evidence in the Internet era, electronic data has been readily incorporated into criminal proceedings. In China, it was not until the Criminal Procedure Law was amended in 2012 that electronic data was classified as an independent type of evidence. Apart from the Criminal Procedure Law, there are three main regulations pertaining to the use of electronic data. Even though great endeavors have been made by Chinese authorities to integrate novel technologies into electronic data and the basic framework for the regulations of electronic data has been formed, there are still some lingering weaknesses in the current regulations: vulnerable rights of criminal suspects, the absence of the special investigation department, unclear provisions in relevant regulations, and improper remedy mechanisms. To further develop the rules of electronic data, China is supposed to place emphasis on the idea of rights protection and the interaction between new technologies and evidence theory.

1. Introduction

As the cutting-edge information technology has evolved in leaps and bounds, the Internet has become the motor of innovation-driven development.[1] In the Internet era, people's lives have undergone dramatic and profound changes. On the one hand, the advancement of such technology has brought great convenience to our daily lives; on the other hand, from a legal perspective, the collection, custody and authentication of electronic data have plagued investigators, prosecutors, and judges across different jurisdictions.[2] Although the proportion of cybercrime cases in all criminal cases varies from country to country, it is undeniable that almost all countries are wrestling with cybercrimes in the Internet era. In criminal proceedings, electronic data has proven to be the lynchpin in cybercrime cases. In response to the situation, more and more countries have enacted legislation to fight against the rampant cybercrimes and deal with the emerging evidence in electronic form. With the increasing emphasis on electronic data when handling criminal cases especially cybercrime cases, it is of vital importance to review the current rules of electronic data in different

* Corresponding author.
E-mail address: fengjiaolingxiao@163.com (J. Feng).

[1] See the White Paper on Chinese Court and Internet Judiciary, published by the Supreme People's Court of the People's Republic of China on December 4, 2019.

[2] In the US, scholars attach more attention to the constitutionality of search and seizure in the digital world, see Orin S Kerr, 'Compelled Decryption and the Privilege against Self-Incrimination' (2019) 97 Tex L Rev 767; Carol Nackenoff, 'Only the Beginning, Only Just the Start - Mostly I'm Silent: New Constitutional Challenges with Data Collection Devices Brought into the Home' (2019) 79 Md L Rev 88; Aaron Chase, 'Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments' (2020) 17 Hastings Race & Poverty LJ 577. By way of comparison, scholars researching the Chinese context primarily focus on the procedural issues at the stage when regulations pertaining to electronic data have not been completely laid down.

https://doi.org/10.1016/j.ijlcj.2020.100453
Received 26 June 2020; Received in revised form 27 October 2020; Accepted 25 November 2020
Available online 8 December 2020

jurisdictions to ensure that they are suitable for the present issues the legal system (and the society more broadly) are facing.

Since China gained access to the internet in 1994,[3] China's authorities have reacted actively to the influence of the Internet on criminal cases. According to the Special Report on Cybercrime Based on Judicial Big Data released by the Supreme People's Court of the People's Republic of China, more than 48,000 cybercrime cases were conducted in courts at all levels in China between 2016 and 2018, which accounted for 1.54% of all the criminal cases during that period.[4] Nonetheless, China's current evidence rules cannot adequately confront the challenges brought about by new forms of electronic evidence. It should be noted that this situation is not unique to China. British scholar Stephen Mason devotes himself to drafting the Draft Convention on Electronic Evidence in order to pursue a common international policy on electronic evidence.[5] To date, there has yet to be an official convention on electronic data.

In view of Chinese authorities' efforts to integrate electronic data into the criminal justice system, this article focuses on the rules covering electronic data in China. As for the structure of this article, Section 2 reviews the legal history of electronic data in China, which although only recently recognized as an independent category of evidence has proven to be controversial in the past decades. Section 3 elaborates on China's current regulations relating to the collection, custody, and authentication of electronic data. Section 4 evaluates the strengths and weaknesses of China's current regulations concerning electronic data so as to shed light on the enhancement of relevant rules in the future. The final section, Section 5, details several suggestions for the further improvement of China's rules on electronic data.

2. Legal history of electronic data in criminal cases in China

The use of electronic data as evidence in criminal proceedings has had a relatively short developmental history in China. Based on some significant points in time over the development of electronic data in China, this section reviews the legal history of electronic data in criminal cases in the Chinese context. Generally speaking, its development can be roughly divided into three periods. Prior to 2012, the Criminal Procedure Law of the People's Republic of China did not regard electronic data as an independent type of evidence, despite the appearance of electronic data in judicial practice. As the law inherently lags behind judicial practice, scholars have heatedly debated what kind of evidence electronic data should be and whether it should be admissible in criminal cases. The amendment to the Criminal Procedure Law of the People's Republic of China in 2012 confirmed that electronic data shall be recognized as an independent type of evidence which was neither physical evidence nor documentary evidence. The Case of Qvod Player occurred in 2014 obviously exposed the flaws of China's broad legislative model of electronic data at that time and the rapid development of technology pertaining to electronic data continuously brings new challenges for Chinese authorities. To better understand the legal history of electronic data in China, some of the key points in time are detailed in Table 1, with further exploration provided in the following sections.

2.1. Before 2012: fierce debates on the attributes of electronic data

Cybercrimes began to take hold by 1997, and the Criminal Law of the People's Republic of China has been used to address it since then. At the same time, Chinese scholars began to devote more time and attention to studying electronic data. In the beginning, there was no unified legal term covering what is now considered electronic data, with scholars using the terms "electronic data", "computer evidence", "digital evidence", and "electronic evidence" interchangeably.[6] "Electronic data" first appeared as a legal term in the Provisions on the Procedures for Handling Criminal Cases by Public Security Organs, published by the Ministry of Public Security of the People's Republic of China in 1998. Subsequently, the Ministry of Public Security issued the Rules of Electronic Data Identification of Public Security Organs in 2005, which defined electronic data as "data stored, processed, and transmitted in digital form".[7] However, according to the Legislation Law of the People's Republic of China, these two regulations are departmental regulations (their legal force is relatively lower than actual legislation), so that heated debates on electronic data are still ongoing amongst legal practitioners.[8] In the two documents Provisions on Several Issues Concerning the Examination and Judgment of Evidence in Death Sentence Cases[9] and Opinions on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling[10] jointly published in 2010 by multiple authorities, the term "electronic evidence" still prevailed, rather than "electronic data".

Besides, in terms of the attributes of electronic data, some scholars have argued that electronic data should be seen as the sub-type

[3] See Xingdong Fang & Shuai Chen, 'Twenty-five Years of Internet in China' (2019) 4 Modern Communication (Journal of Communication University of China) 1.

[4] See the Special Report on Cybercrime Based on Judicial Big Data, which was released by the Supreme People's Court of the People's Republic of China on November 19, 2019.

[5] See explanatory notes to the Draft Convention on Electronic Evidence, published as the supplement at (2016) 16 Digital Evidence and Electronic Signature Law Review s1-s11.

[6] See Weiqiu Long & Wei Pei, 'Concept and Authentication of Digital Evidence' (2016) 2 Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition) 40.

[7] See Article 2 of Rules of Electronic Data Identification of Public Security Organs (2005).

[8] See Minyan Wang, 'Electronic Evidence in China' (2008) 5 Digital Evidence and Electronic Signature Law Review 45.

[9] It was jointly issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security of the People's Republic of China on June 13, 2010.

[10] It was also jointly issued by the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security of the People's Republic of China on August 31, 2010.

Table 1
Main points in time of Chinese development concerning electronic data.

Year	Document or Case	Significance
1998	Provisions on the Procedures for Handling Criminal Cases	The term "electronic data" first appeared in the official document
2005	Rules of Electronic Data Identification of Public Security Organs	Electronic data was defined as "data stored, processed, and transmitted in digital form"
Debates on whether electronic data should be regarded as evidence were still fierce		
2012	Criminal Procedure Law (2012 Amendment)	Electronic data became an independent category of evidence
2014	The Case of Qvod Player	The astounding case revealed the shortcomings of rules of electronic data at that time since there were no special provisions on the collection, custody and authentication of electronic data
2016	Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases	The exact meaning of electronic data was set out as "data that is formed in the process of occurrence of a case, stored, processed, and transmitted in digital form, and can prove the case facts" and the testimony of witness, statement of victim, and confession and argument of criminal suspect or defendant recorded in the digital form and other evidence were not electronic data
2019	Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases	The collection methods were refined and more attention were paid to the protection of privacy rights
Arguments of the attributes of electronic data finally came to an end, but rules of electronic data remained to be improved		

of physical evidence, documentary evidence, or audio-visual recordings because the electronic data only serves as a tool for the storage or authentication of these evidence.[11] Contrastingly, other scholars hold that electronic data should be considered as an independent type of evidence and new rules tailored to electronic data should be made because electronic data inherently has characteristics that previous types of evidence do not.[12]

It can be seen that electronic data, as a relatively new phenomenon, had attracted scholarly interest but remained poorly defined as scholars had no in-depth understanding of electronic data at this stage. It is noteworthy that in China, discussions of electronic data's attributes are not nonsense. Regarding the collection, custody, and authentication of evidence, investigators should abide by different rules for different categories of evidence. Moreover, if electronic data is not recognized by law as a type of evidence, judges will not admit it in court, even though it holds substantial evidential value. Due to the issues outlined above, the use of electronic data in judicial practice during this period was rare.[13]

2.2. Since 2012: electronic data regarded as an independent form of evidence

With the advancement of judicial practice, a lot of problems about electronic data were exposed, particularly in relation to the collection, custody, and authentication of electronic data. Cases that were not able to involve electronic data as an independent type of evidence were increasingly yielding unjust outcomes. These great differences between electronic data and other categories of evidence were finally realized by legislators and they took them into account in the amendment to the Criminal Procedure Law of the People's Republic of China in 2012. Article 48 of the Criminal Procedure Law of the People's Republic of China (2012 Amendment) provides that electronic data shall be the eighth category of evidence, separating electronic data from physical evidence, documentary evidence, and audio-visual materials. This is the first piece of Chinese legislation to fix electronic data as a formal legal term and also regard electronic data as a new type of evidence, which is inherently different from any of the existing categories of evidence. Since then, there have been fewer controversies about the attributes of electronic data in Chinese academic circles, and more scholars have turned their attention to how the relevant rules on electronic data can be improved, including the collection, custody, authentication of electronic data and the exclusion rules that apply to illegally obtained electronic data.

As the amendments to Criminal Procedure Law of the People's Republic of China always stick within the broad legislative model, corresponding provisions on electronic data in the Criminal Procedure Law are refined through sequential judicial interpretation afterwards.[14] As often, the Supreme People's Court issued the Judicial Interpretation of the Application of Criminal Procedure Law of

[11] See Hao Cui, 'Legal Thinking of Electronic Evidence in Cybercrime' (2007) 2 Criminal Research 51; Peng Guo &Huaiyu Qin, 'The Admissibility and Classification of Electronic Evidence' (2007) 4 Lanzhou Academic Journal 8; Dong Zhang, 'On the Legal Status of Electronic Evidence' (2009) 6 Dongyue Tribune 179.

[12] See Pinxin Liu, 'On the Legal Status of Electronic Evidence: Thinking Based on the Current Evidence Law of China' (2002) 4 Studies in Law and Business 42; Wenjiang Hao, 'A Probe on the Independent Status of Electronic Evidence in Procedure Law' (2007) 3 Journal of Political Science and Law 40; Yanping Xu, Juping Wu & Xiaowen Li, 'The Legal Status of Electronic Evidence in Criminal Procedure' (2007) 12 Legal Science 131.

[13] Relevant case notes, see Rong-Shu-Xia Computer Ltd. v China Society Publisher, by Minyan Wang (2007) 4 Digital Evidence and Electronic Signature Law Review 95; Beijing Han-Hua-Kai-Jie Technology development Ltd. v Chen Hong, by Minyan Wang (2007) 4 Digital Evidence and Electronic Signature Law Review 96; Zhang Hua v Shanghai Danwei Information Consultation Co. Ltd, Shanghai People's Court of Jing'an District, by Minyan Wang (2009) 6 Digital Evidence and Electronic Signature Law Review 275–276. Besides, translations of related cases, see Yang Chunning v Han Ying (2005) hai min chu zi NO.4670, Beijing Hai Dian District People's Court, commentary by Jihong Chen (2008) 5 Digital Evidence and Electronic Signature Law Review 103–105.

[14] See Minyuan Wang, 'A Study on the Judicial Interpretations of Criminal Procedure Law after the Amending in 2012' (2015) 1 Journal of National Prosecutors College 131.

the People's Republic of China on December 20, 2012, and the Supreme People's Court, Supreme People's Procuratorate and Ministry of Public Security of the People's Republic of China jointly promulgated the Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases on May 4, 2014 (hereinafter referred to as Issues 2014). However, these two judicial interpretations fail to specifically focus on electronic data, such that relevant articles regarding electronic data in these two regulations are few and far between. Meanwhile, those provisions that pertain to electronic data are not sufficiently clear to solve the application problems of electronic data in judicial practice.

2.3. The Case of Qvod Player (2014) and the regulations on electronic data that followed

The case of Qvod Player ("Kuaibo" in Chinese) is a landmark case in the development of electronic data in China. When this case came to court in 2014, it shocked the public, triggered fierce forensic arguments, perplexed the presiding judges, and served as an impetus for the refinement of the broad regulations of electronic data in China. Qvod Player, the dominant media player enterprise in China at that time with over 300 million users,[15] was accused of broadcasting pornography as part of its online service. Controversies among scholars about the criminal proceedings of the case stemmed from the integrity and authenticity of electronic data for conviction, particularly the process of collection, custody and authentication of electronic data.[16]

First, the defender pleaded that the collection of electronic data was illegal on the grounds that the seizure of four servers presented as the key evidence in the case was conducted by the collectors who were not authorized to obtain evidence under Chinese Criminal Procedure Law since the case was initially regarded as an administrative case and four servers were seized by the administrative officials, as per administrative procedures. When collected by investigators from the public security authority, the models, capabilities and other key characteristics of these four servers were not recorded yet, which contravened relevant rules of the collection of electronic data and cast doubt on the authenticity of the electronic data collected from the four servers. Second, the custody of the servers was arbitrary because the four servers were passed on by four departments successively, and even a company that had a stake in one of Qvod Player's rivals[17] kept the four serves without any supervision from the authorities. The broken chain of custody allowed for the possibility that the electronic data saved on the four servers could have been modified. Apart from the custody of these four servers, the custody of 21,251 porn videos extracted from the four serves was also questionable since most of the videos were decoded on the basis that they were their originals and not of replicas, thereby jeopardizing the integrity of the electronic data. Moreover, when the servers were preserved in the investigation department, no specific staff was designated to keep guard of the servers, with the result that almost all the personnel in the department had the chance to tamper with the electronic data saved on the servers. Third, the authentication of the 21,251 porn videos was conducted by the company who was the rival of Qvod Player and not qualified to conduct the authentication, again meaning that the electronic data could easily have been tampered with.[18] Besides, in the Chinese forensic identification system, there are only three kinds of forensic identification and certain requirements must be met to become a competent forensic authenticator. However, the judicial authenticator who was in charge of assuring the quantity of pornography lacked the qualifications needed. All of these issues were raised by the defendants and the counsels, which placed the prosecutor in a highly embarrassing situation.

Because of the broad provisions on electronic data at that time, four executives of Qvod Player were handed down prison sentences ranging from three years to three and a half years for broadcasting pornography online. Among them, Wang Xin, the chief executive of Qvod Player, received the longest sentence and was fined 1 million yuan according to a verdict from the Beijing Haidian District People's Court. Even though the case has been decided, discussions on the refinement of relevant regulations pertaining to electronic data have continued in the following years. Shortly after the Case of Qvod Player, two regulations specializing in the application of electronic data came into force: Provisions on Several Issues concerning the Collection, Taking, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases jointly issued by the Supreme People's Court, Supreme People's Procuratorate and Ministry of Public Security of the People's Republic of China in 2016 (hereinafter referred to as Provisions 2016) and Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases solely promulgated by the Ministry of Public Security of the People's Republic of China in 2019 (hereinafter referred to as Rules 2019). The issuance of these two judicial interpretations of electronic data after 2014 was expedited by the Case of Qvod Player. It was in the Provisions 2016 that the exact definition of electronic data was set out as "data that is formed in the process of occurrence of a case, stored, processed, and transmitted in digital form, and can prove the case facts". The testimony of witnesses, statements of victims, and confessions and arguments of criminal suspects or defendants recorded in the digital form or other evidence are not classed as electronic data. Only by setting out a concise definition have the arguments regarding the meaning of electronic data come to an end.

3. Current regulations of electronic data in criminal cases in China

In China, the current regulations for electronic data broadly involve three aspects: collection, custody, and authentication.

[15] See https://www.sohu.com/a/225871325_389304, last accessed on May 15, 2020.

[16] See Beijing Haidian District People's Court [2014] Criminal Judgement Nr. 512.

[17] Wenchuang Dongli Information Technology Company was the rival of Qvod Player and had ever reported the illegal acts of Qvod Player to the National Copyright Administration of the People's Republic of China, but the claim was not approved by the court. See Pinxin Liu, 'The Authentication of Electronic Evidence: from the QVOD Case' (2017) 1 Peking University Law Journal 92.

[18] See Pinxin Liu, 'The Authentication of Electronic Evidence: from the QVOD Case' (2017) 1 Peking University Law Journal 92.

Concretely speaking, there are three key relevant regulations governing this area: (1) Issues 2014; (2) Provisions 2016; (3) Rules 2019. These three regulations set out comprehensive and systematic provisions on electronic data, almost covering the entire judicial application process of electronic data, and also clarify some important concepts related to electronic data.

3.1. Collection of electronic data

According to the regulations mentioned above, the collection of electronic data must strictly comply with the following rules on collectors, objects collected, and collection methods. In the instance that these regulations are violated, electronic data evident shall not be admissible in court.

(1) Collectors: In a typical criminal case the evidence should be collected by investigators. However, when it comes to electronic data, this process may be different. Initially, Article 13 of Issues 2014 stipulates that the collection of electronic data shall be conducted by two or more investigators with corresponding professional knowledge. However, Article 7 of Provisions 2016 removes the requirement of "corresponding professional knowledge". In other words, whether the two investigators possess the necessary professional knowledge in relation to the collection of electronic data is no longer taken into account. Nevertheless, pursuant to Article 6 of Rules 2019, the collection of electronic data shall be carried out by two or more investigators and when necessary, a professional technician may be engaged to collect electronic data at the instruction of the investigators.

It can be seen that the changes in China's regulatory requirements for the qualification of collectors actually reflects the dilemma of Chinese judicial practice.[19] The most salient problem in Chinese judicial practice is that there are insufficient investigators with the relevant professional knowledge operating within the investigative bodies. Besides, third-party institutions are increasingly being recognized as qualified subjects for collecting electronic data. For instance, China's three giant Internet corporations, Alibaba, Tencent and Baidu, are authorized to collect electronic data. As they are deemed professional in this regard they are able to gather evidence on the behalf of investigators. It should also be noted that according to Article 5 of Rules 2019, electronic data collected by another state agency in the course of administrative law enforcement may be used as evidence in criminal cases, so long as it was collected in accordance with relevant administrative laws. Nowadays, collectors of electronic data are becoming increasingly diverse. If the requirements of Issues 2014 are strictly complied with, it is far beyond the capacity of investigation departments. However, people may question or take issue Internet companies assisting in the collection of electronic data in criminal cases.

(2) Objects Preferred: Based on general evidence theory, all electronic data related to criminal cases should be collected in a comprehensive, objective, and timely manner. However, when referring to the medium of electronic data collected, the three associated regulations do not perfectly align with the general evidence theory. Pursuant to Article 14 of Issues 2014, the priority of the collection of electronic data is given to the original medium. Meanwhile, under Article 15 of Issues 2014, in the case where the original medium is unavailable, relevant electronic data may be collected online. One piece of empirical research shows that of 483 cases in Zhejiang Province, China, 210 contained electronic data and used the original medium.[20] The use of the original medium has its advantages since the original medium contains a vast amount of raw data which can potentially aid investigators to ascertain the facts of a case. In the circumstances when the original medium cannot be obtained, the investigators often turn to the online collection way. However, there are some potential risks associated with pursuing this course of action. For instance, the three regulations fail to specify restrictions on the online collection of electronic data and fail to delineate the search area of the original medium, which may endanger both the privacy and property rights of criminal suspects in the online space. Moreover, in the long term, electronic data will increasingly be collected online instead of in the original medium due to the widespread use of cloud computing. In the cloud, there is no original medium; therefore, from this perspective, it is somewhat outdated to give priority to the original medium.
(3) Collection Methods: Rules 2019 refines the general provisions on the collection methods prescribed in Rules 2014 and Provisions 2016, and subdivides the collection methods into five specific categories: impounding or placing a seal on and preserving the original storage medium, taking electronic data on site, taking electronic data online, freezing electronic data, and requesting electronic data.[21] In practice, four ways are often used to collect electronic data: online distance collection, extraction from the original medium, requesting from the third party, and providing by the parties concerned. The frequency of each collection way in one piece of empirical research covering 483 cases in Zhejiang Province, China is listed in Table 2.[22] It also should be noted that one or several collection ways may be applied at the same time in one case.

According to Rules 2019, investigators are empowered to utilize the most suitable collection method in judicial practice so as to complete the collection procedure efficiently and reasonably. Despite China having expanded the collection methods applicable to electronic data, the current five collection methods are nonetheless subject to some potential shortcomings. For example, both Article 10 of the Provisions 2016 and Article 8 of Rules 2019 prescribe that in the cases where electronic data fails to be collected or taken for

[19] See Haisong Yu, 'Criminal Electronic Data: Regulatory Approaches and Key Issues' (2019) 1 Global Law Review 39.
[20] See Jiao Feng, 'The Collection of Internet Evidence' (2018) 5 Journal of National Prosecutors College 34.
[21] See Article 7 of Rules 2019.
[22] See Jiao Feng, 'The Collection of Internet Evidence' (2018) 5 Journal of National Prosecutors College 34.

Table 2
Collection ways used in judicial practice.

Collection way	Online distance collection	Extraction from original medium	Requesting from third party	Provided by the parties concerned
Number of cases	99	210	109	4

any objective reason, or it is inappropriate to collect or take electronic data in accordance with other provisions, the relevant evidence may be fixed by printing, by picture-taking, or by video recording. These two articles clearly aim to facilitate the handling of cases and improve the judicial efficiency; however, they ignore the reality of how electronic data is often concealed, making it difficult to crack down on criminal cases in the long run. Besides, due to the lack of original data, it is harder for the defence to identify potential flaws in the electronic data, thereby eroding their position in the trial. It is interesting to note that when interviewed, a number of judges indicate that they prefer electronic data to be presented in print form as it makes it easier for them to evaluate the evidential value of the electronic data submitted.[23]

3.2. Custody of electronic data

There are no specific provisions in Issues 2014 pertaining to the custody of electronic data because the evidence against traditional crimes can be more readily stored. Therefore, China's previous theories and regulations give priority to the authenticity of evidence whilst largely ignoring the importance of the custody of evidence in the broader process of authentication.[24] The authenticity of electronic data is no trivial matter, and it goes beyond demonstrating that it has remained in an unbroken chain of custody.[25] It was only in 2016 that China's first regulation involving the custody of electronic data (see Provisions 2016) came into force. Subsequently, when Rules 2019 were enacted, they largely followed the relevant articles of Provisions 2016. Yet, the poorly drafted articles in Provisions 2016 and Rules 2019 hardly attend to the needs of judicial practice.

Specifically, Provisions 2016 and Rules 2019 have set forth the following rules for the custody system relating to electronic data.[26] First, if the original storage medium of electronic data can be seized in the custody process, it shall be sealed. Following this, a transcript shall be prepared to record the seal status and photographs shall be taken to show the state of the original storage medium. If necessary, the photographs shall also clearly capture the details of the electronic equipment's built-in storage media. When an original storage medium with wireless communication functionality (i.e., a mobile phone on mobile internet device) is preserved, measures such as signal jamming, signal blocking, and cutting off the power shall be adopted. Second, electronic data may be taken in the circumstances where the original storage medium cannot be seized. In this instance, the reasons why the original storage medium could not be seized, the place where the original storage medium is stored, and the source of electronic data shall be indicated in the transcript, and meanwhile the integrity check shall be conducted on the electronic data taken. The electronic data seized may be compressed, and the corresponding method and checksum of the compressed file shall be clearly detailed in the transcript. Third, electronic data may be frozen due to its large volume, the extended period of time required, or in the circumstances where electronic data may be better exhibited visually through web applications. Electronic data shall be frozen by using one or several of the following methods: (1) Computing the checksum of electronic data; (2) Locking accounts for web applications; (3) Adopting write protection measures; (4) Other measures employed to prevent the addition, deletion, and modification of electronic data.

From the rules above, it can be seen that technical measures over procedural matters are emphasized to ensure the integrity and authenticity of electronic data. However, these rules ignore the reality of the situation: the custody of electronic data is more of a procedural issue. In China, the chain of custody is not well established enough to ensure the continuity of electronic data, meaning that electronic data could be altered, manipulated or damaged between the time it is created and the time it is brought forward in court as evidence. This opens up the possibility that the authenticity of electronic data being attacked in court by the defence, whilst also exacerbating the deterioration of the admissibility of electronic data.[27] Besides, as the capacities and resources of the authorities vary across locations in China, some regions of China do not even have special rooms designated to store evidence, not to mention relevant technologies used to ensure the integrity of electronic data. Therefore, practical needs and procedural issues are supposed to be taken into consideration before specific technologies are applied in the custody process of electronic data.

3.3. Authentication of electronic data

As electronic data is volatile and can easily be altered — even by the simple act of switching a computer on or off[28] — the

[23] See Jiao Feng, 'The Production of Internet Evidence' (2020) 4 Journal of Harbin Institute of Technology (Social Sciences Edition) 22.
[24] See Jiao Feng, 'On the Custody of Internet Evidence' (2018) 1 Nanjing University Law Review 298.
[25] See Stephen Mason & Daniel Seng, editors, 'Electronic Evidence (Fourth Edition)' (2017) Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London 196.
[26] See Articles 8–10 of Provisions 2016 and Articles 10–40 of Rules 2019.
[27] Stephen Mason & Daniel Seng, editors, 'Electronic Evidence (Fourth Edition)' (2017) Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London 196.
[28] Graeme B Ball & Richard Boddington, 'Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?' (2010) 5 Journal of Digital Forensics, Security and Law 1.

authentication of electronic data has always been a central issue in criminal trials. Therefore, the authenticity and integrity of electronic data are stressed in all three of the regulations mentioned above, whereas relevant articles involving the authentication of electronic data are rare and principled in Issues 2014 and Provisions 2016. Compared to Issues 2014 and Provisions 2016, Rules 2019 refines the technical methods applied to ensure the veracity of electronic data.

In Issues 2014, Article 17 only briefly touches on this issue, requiring the public security organ to issue remarks on data statistics and data identity without detailing any specific methods for authentication.[29] Encouragingly, Provisions 2016 includes sophisticated articles on the authentication of electronic data. Under Article 25 of the Provisions 2016, methods for verifying the relevant IP address, network activity records, attribution of Internet terminals, the testimony of the relevant witnesses, as well as the confession and arguments of the accused, may be applied to comprehensively judge the identicalness of the accused's online identity and real identity. Nevertheless, the authentication methods of electronic data in Provisions 2016 are notably similar to those of methods applied to conventional evidence, such that the unique characteristics of electronic data are ignored. For instance, in terms of the identicalness, Provisions 2016 attaches emphasis to the judgment of whether the online identity and real identity of the accused are identical while ignoring the difficulties that arise when judging the real person hiding behind the online identity. In addition, for all types of evidence to be authentic, it must be demonstrated that the evidence is what it purports to be. However, Provisions 2016 fails to answer these questions about electronic data.

In Rules 2019, Chapter 3 focuses on the examination and investigative reenactment of electronic data. Pursuant to Article 50 of Rules 2019, if necessary, an investigative reenactment of electronic data may be conducted with the approval of the individual in charge of the public security authority at or above the county level. Investigative reenactments of electronic data are typically conducted to verify certain abnormalities or changes in electronic data, verify whether certain operational actions on electronic data can be completed within a given time, verify whether certain software or hardware can be used to perform a specific act or have specific consequences, and determine whether a certain computer information system application can modify specific electronic data.[30] At the same time, the investigative reenactment of electronic data shall meet the following requirements: (1) Technical measures shall be used to protect the integrity of the data on an original storage medium; (2) If conditions permit, the investigative reenactment of electronic data shall be conducted twice or more; (3) The electronic equipment, network environment and the like used in the investigative reenactment shall be consistent or basically consistent with the crime scene; and if necessary, relevant technical methods may be used to simulate or conduct a controlled experiment on the relevant environment; (4) Conduct that may divulge citizen's information or affect the normal operation of computer information systems in non-experimental environments shall be prohibited.[31] As can be seen from the above articles in Rules 2019, detailed provisions have been formulated to demonstrate the authenticity of electronic data. However, to what extent is the investigative reenactment effective?

To sum up, the above-mentioned rules elaborate on the applicable conditions, procedures and requirements of the authentication process for electronic data. The key point here is that the existing rules fail to directly address the technical issues that are central to the authentication of electronic data. In practice, third parties are often commissioned by investigative authorities to authenticate electronic data. Meanwhile, the required qualifications of third parties are not specified and the capabilities of third parties in China vary. Thus, there is a pressing need to implement unified guidelines for the standardization of electronic data authentication.

4. Evaluation of China's current regulations on electronic data

4.1. Strengths

4.1.1. Emphasis on the incorporation of novel technologies into electronic data

In recent years, China has embraced the era of big data and artificial intelligence, with Chinese President Xi Jinping attaching great importance to the incorporation of modern science and technology into judicial reform.[32] This emphasis from authorities also entails financial support and human resources. As "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way",[33] blockchain technology has propelled Internet finance into the blockchain era since Satoshi Nakamoto created bitcoin in 2008. Also thanks to the rise of blockchain technology, sweeping changes have taken place in the field of law, particularly in relation to evidence.[34] According to the White Paper on Chinese Court and Internet Judiciary, the Supreme People's Court of the People's Republic of China has set up the Judicial Blockchain Unified Platform, which collates and stores over 194 million pieces of data from courts at all levels around the country.

In June 2018, the Hangzhou Internet Court, located in the Alibaba headquarters, conducted a trial case involving the dispute over

[29] See Mengshuang Wu & Qingqi Hou, 'The Understanding and Application of Several Issues concerning the Application of Criminal Procedures in the Handling of Cyber Crime Cases' (2017) 1 People's Procuratorial Semimonthly 29.
[30] See Article 51 of Rules 2019.
[31] See Article 52 of Rules 2019.
[32] See http://www.xinhuanet.com/politics/2017-07/14/c_1121317456.htm last visited on May 8, 2020.
[33] See Marco Iansiti & Karim R Lakhani, 'The Truth about Blockchain'(2017) 95 Harvard Business Review 118.
[34] See Pinxin Liu, 'On Big Data Evidence' (2019) 1 Global Law Review 24.

the right of dissemination on the Internet.[35] As China's first case recognizing the legal effect of electronic data stored by blockchain, blockchain (in this case) was considered as more of a storage device for electronic evidence, rather than an evidence-generating means. In its decision, the Hangzhou Internet Court avoided focusing on the superiority of decentralized storage and the tamper-proof nature of blockchain over that of traditional electronic evidence, maintaining a conservative attitude towards blockchain technology.[36] The reason for this is that blockchain was not formally considered as a new form of electronic data that could prove its own authenticity by any law or judicial interpretation at the time. The case attracted the interest of legal scholars to examine how blockchain technology can be applied in judicial practice. Meanwhile, scholars specializing in criminal proceedings have argued that even the case is a civil dispute, blockchain will be of great significance for the future reform of the evidence system in criminal proceedings.[37]

It is noteworthy that the Shangyu District People's Court in Zhejiang Province of China applied blockchain technology to criminal proceedings for the first time on October 30, 2019.[38] The case concerned an offline fraud crime involving a great number of victims across many different regions of China. In this instance, blockchain was used as the tool to store other types of evidence by encoding the relevant evidence and then decoding it in the process of evidence transfer between different authorities in different regions to ensure the integrity and authenticity of the evidence. The future value of blockchain in criminal proceedings should not be underestimated, in particular for online crimes, since blockchain is capable of tackling the long-standing authenticity problem of the use of electronic data as evidence particularly in cybercrime cases. Blockchain allows for the authentication of electronic data because the trust structure of a blockchain is established on the basis of transaction subjects' trust in computer codes, rather than locating an external third party as the trust centre.[39] By overcoming its possible shortcomings, the use of blockchain in criminal cases will become increasingly common in the near future. It can be believed that widespread admissibility of blockchain evidence could be fostered not only by reviewing the existing rules governing electronic signatures and electronic evidence, but also via greater use of ODR by courts.

4.1.2. The formulation of preliminary regulatory framework

As mentioned above, Chinese regulatory framework governing electronic data is based on the Criminal Procedure Law of the People's Republic of China. This basic framework has been supplemented by Rules 2019, Provisions 2016 and Issues 2014, which broadly cover the collection, custody, and authentication procedures for electronic data. Specifically, although the Criminal Procedure Law of the People's Republic of China regards electronic data as an independent category of evidence, it fails to provide specific rules for its judicial application, which reflects the potential shortcomings of the broad legislative model of the Criminal Procedure Law of the People's Republic of China.

Focusing on the application of criminal procedures in cybercrime cases, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of the Public Security of the People's Republic of China jointly published Issues 2014. This step was notable in the history of electronic data as it clarified the provisions relating to the seizing and examination of electronic data, the qualifications of investigators, principles of evidence-taking, and rules of evidence-transfer, amongst others. As a response to the Case of Qvod Player, Provisions 2016, as the first special judicial interpretation concentrating on electronic data, further refined the associated articles in Issues 2014. Moreover, Provisions 2016 are notable for detailing a number of technical methods for the collection, custody, and authentication of electronic data. Rules 2019, issued by the Ministry of the Public Security of the People's Republic of China closely follows the relevant regulations found in Provisions 2016 and sets out more detailed provisions on the collection of electronic data.

4.1.3. A prime opportunity to develop electronic data theory

The Internet era offers a golden opportunity for the innovation of traditional evidence theory. For example, it is typically assumed that the chain of custody begins when police officers seize the evidence.[40] However, this theory needs to change when it is applied to electronic data. Presently, Internet companies are increasingly involved in the collection of electronic data, and in some cases investigators cannot even obtain the electronic data without the assistance of technicians. The function of the chain of custody is to ensure the integrity of evidence; accordingly, when handling electronic data, the starting point for the chain of custody needs to move forward. The same is true in relation to authentication. In general, attention is usually attached to the storage medium of the electronic data, as well as the information held within when verifying its authenticity. However, due to advancements in Internet technologies, the actual person using the given account should also be taken into consideration since the owner and the actual user of the account are

[35] See Hangzhou Huatai Yimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd. (2018) Zhe 0192 Civil Case, First CourtNo. 81, Hangzhou Internet Court of the People's Republic of China, translated by Jiong He, 16 Digital Evidence and Electronic Signature Law Review (2019) 61–70.

[36] See Hong Wu & Guan Zheng, 'Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity' (2020) 36 Computer Law & Security Review 105401.

[37] See Yujie Zhang, 'Judicial Application, System Problems and Evidence Law Reform of Blockchain Technology' (2019) 3 Oriental Law 100.

[38] See the report of China's First Criminal Case with the Assistance of Blockchain for evidence storage, People's Court Daily, November 1, 2019. The digital version of the report, see the official website of the newspaper, http://rmfyb.chinacourt.org/paper/html/2019-11/01/node_4.htm, last visited on May 16, 2020.

[39] See Hong Wu & Guan Zheng, 'Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity' (2020) 36 Computer Law & Security Review 105401.

[40] According to the rule, for fungible objects such as drugs, authentication may have to be accomplished by establishing a chain of custody that tracks the object from its receipt through its various travels (which may include laboratory analysis) to its ultimate courtroom destination. See 2 Crim. Prac. Manual § 63:4.

no longer necessarily the same person. Thus, the authentication process of electronic data will inherently be much more complicated than that of other types of evidence.

Moreover, the use of big data, cloud computing, and blockchain technology in the justice system will also pose new challenges for electronic data theory. For instance, big data emphasizes relevancy, which is one of the most important aspects of evidence. Meanwhile, there is the possibility that relevancy in the context of big data will refine the definition of "relevancy" in the evidence theory. The proliferation of cloud computing has prompted privacy concerns, particularly in relation to the theft of data by third parties. To summarize, these new conditions which have flourished in the Internet era are a prime opportunity for theoretical innovations of the current evidence theory of electronic data.

4.2. Weaknesses

4.2.1. Vulnerable rights of criminal suspects in judicial practice

Overall, at the investigation stage, the right to know, privacy and property rights of criminal suspects are vulnerable. On the one hand, a criminal suspect's right to know is not soundly protected under the current regulations because the investigation authorities are empowered to take technical investigation measures without informing the criminal suspect who is under investigation.[41] As pointed out above, investigators are authorized to undertake a series of measures to collect electronic data under the current regulations. In judicial practice, measures of online electronic data collection, online distance investigation, and technical investigation measures are often undertaken in secret without the consent or cooperation of the criminal suspects, which is primed to infringe upon the rights of criminal suspects.[42] It also needs to be mentioned that under Chinese criminal procedure, the obtaining of evidence is classed as an investigative activity, meaning that police officials alone can decide to undertake such activities. During this process, neither the judge nor the prosecutor will interfere, which affords the investigators a lot of discretion and may have negative impact on the right to know of criminal suspects. On the other hand, the privacy and property rights of criminal suspects are also at risk of infringement at the investigation stage. Article 23 of Rules 2019 provides that when investigators take electronic data online, all data stored in the domestic distance computer information system can be taken, no matter whether the data is publicly accessible or not. Besides, Article 6 of the Provision 2016 stipulates that all data stored both at home and abroad can be taken online. This article has proven to be particularly controversial and many countries have viewed it as a violation of cyberspace sovereignty. Therefore, Article 23 of Rules 2019 provides that only the publicly accessible electronic data stored abroad can be taken online. However, this method of taking electronic data online is still applicable to electronic data stored in China, meaning that the privacy and property rights of criminal suspects are still jeopardized during the investigation stage.

A digital search is inherently different from a traditional search. Typically, a traditional search is a one-step process, whilst computer technologies tend to split the process into two steps: the police first execute a physical search to seize computer hardware and they then carry out a second electronic search to obtain data from the seized computer storage device.[43] However, it is disheartening to see that the current rules on electronic data in China are premised on the traditional model. By way of contrast, in view of the Fourth Amendment to the Constitution of the United States, the scope of search warrants issued in the United States must be clearly defined and delineated, which means that the warrant must "particularly describe the place to be searched, and the persons or things to be seized."[44] Rules in the United States are designed to prevent "general searches" and limit "the discretion of the officer executing the warrant."[45] In Chinese judicial practice, however, the search warrant merely offers the general description of the search area. Undoubtedly, this authorization model will leave much room for the discretion of investigation authorities and exacerbate their infringements of the suspect's rights.

4.2.2. Absence of special investigation department

The absence of a special investigation department is the root cause of the revisions of the provisions in Issues 2014, Provisions 2016 and Rules 2019 on the investigator's qualification of "corresponding professional knowledge".[46] Since electronic data is highly related to modern technologies, it is necessary to establish a special investigation department. Many Western countries have founded special departments that are dedicated to investigating cybercrime cases.[47] For example, America has established the Cyber Division at the FBI headquarters to address cybercrimes in a coordinated and cohesive manner. As part of this effort, America has trained cyber squads at FBI headquarters and in each of its 56 offices to protect against and investigate relevant crimes carried out online.[48] In China, the Cyberspace Administration, founded in 2011, is responsible for the overall planning and coordination of cyber-security work and any

[41] See Article 9 of Rules 2019.

[42] See Tonghui Zhu & Yuqing Wang, 'Due Process Regulation of Electronic Data Collection' (2020) 1 Journal of Soochow University (Law Edition) 130.

[43] See Orin S. Kerr, 'Search Warrants in an Era of Digital Evidence' (2005) 75 Mississippi Law Journal 85.

[44] See Payton v. New York, 445 U.S. 573, 585 (1980); See also Kentucky v. King, 563 U.S. 452, 459 (2011).

[45] See United States v. Blake, 868 F.3d 960, 973 (11th Cir. 2017).

[46] See Section 3.1 of the paper.

[47] See Galina Borisevich et al., 'A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and Under the Convention on Cybercrime of the Council of Europe' (2012) 39 N. Ky. L. Rev. 267.

[48] See the official website of FBI, https://www.fbi.gov/investigate/cyber, last visited on May 12, 2020.

relevant routine supervisory and administrative work.[49] Nevertheless, the Cyberspace Administration of China falls under the governance of the State Council Information Office and it merely performs administrative functions without having any actual power to investigate cybercrimes. Under the umbrella of the public security and state security authorities, which have jurisdiction over the vast majority of criminal cases, the Department of Network Supervision primarily assuming administrative responsibilities assists the Department of Criminal Investigation in the public security and state security authorities to investigate cybercrime cases.

In a word, the investigation of cybercrime cases tends to be carried out by the Department of Criminal Investigation with the assistance of other administrative departments.[50] The ensuing problem is that squads in the Department of Criminal Investigation usually have little expertise in handling cybercrime cases, which is clearly detrimental to the collection, custody, and authentication of electronic data in criminal proceedings. For instance, failing to follow the correct provisions when collecting electronic data may render the data inadmissible in court because it will be deemed illegally obtained evidence. Also, inappropriate custody measures may destroy the integrity of electronic data. In a nutshell, it is highly likely that teams in the Department of Criminal Investigation may undermine the integrity and authenticity of the electronic data. Hence, a special department responsible for investigating cybercrimes is supposed to be established and professional squads need to be trained to specifically investigate cybercrime cases.

4.2.3. Unclear provisions in relevant regulations

Even though the basic framework of regulations for electronic data has been formed, some provisions in relevant regulations are so ambiguous that authorities are prone to expounding the provisions for their own convenience. For instance, Article 28 of Rules 2019 provides that online distance investigations shall be undertaken by relevant case-handling county public security authorities, and for any cases which have significant facts and a complicated scene, the higher-level public security authority may directly organize an online distance investigation as it deems necessary. However, no explanation or definition of what constitutes necessary is given. As a consequence, the authorities are given huge scope to determine the jurisdiction of relevant cases. Furthermore, Article 9 of Provisions 2016 stipulates that where it is deemed necessary to take technical investigation measures in an online distance investigation, approval formalities shall be strictly handled. Yet, on the legal status of online distance investigations in criminal proceedings, the consensus has not been reached between legislators and scholars. What is even worse here is that these ambiguously worded articles on the approval procedures of online distance investigations leave room for authorities to undertake investigation measures arbitrarily, at their own convenience.

In terms of the interactions with other departments in the collection of electronic data, there are some latent dangers in the current regulations. For example, according to Article 5 of Rules 2019, electronic data accepted or requested by public security authorities that has been collected or taken by another state agency in the course of administrative law enforcement or investigation and handling of cases may be used as evidence in criminal cases. This article may trigger a series of problems: what kind of procedures should other state agencies follow when collecting evidence to be used in criminal cases? What measures should be taken to ensure the integrity of the electronic data in the collection process?

4.2.4. Poorly constructed remedy mechanisms

The remedy mechanisms involve three key routes of action: the right to sue the acts of investigation authorities, to apply the exclusion of illegally obtained evidence, and to seek the state compensation. Unfortunately, none of these three aspects are properly constructed.

Firstly, being deprived of relevant rights during the investigation stage alone is not sufficient reasonable cause to sue in China since the public security authority is the administrative department and it assumes the duty of investigation in addition to other routine administrative affairs. According to Article 12 of the Administrative Litigation Law of the People's Republic of China, 12 kinds of complaints filed by citizens, legal persons, or other organizations will be accepted by the court, however, the improper action undertaken by the public security authority in criminal proceedings is not one type of the acceptable complaints. Thus, under the current Chinese rules, the remedy mechanisms exclude the pursuit of litigation for the inappropriate acts conducted by investigation authorities. Secondly, and more worryingly, is that illegally obtained electronic data may not fall within the rules for the exclusion of illegally obtained evidence under the Criminal Procedure Law of the People's Republic of China.[51] Under Article 56 of the Criminal Procedure Law of the People's Republic of China (2018 Amendment), the rules covering the exclusion of illegally obtained evidence span five types of evidence: physical evidence, documentary evidence, witness statements, victim statements, confessions, and defense of a criminal suspect or defendant, respectively. According to Article 50 of the Criminal Procedure Law of the People's Republic of China (2018 Amendment), electronic data is a type of evidence independent from the above five categories. Even though illegally obtained electronic data could be excluded in the future,[52] it is extremely hard for the accused to prove that the electronic data is illegally obtained because investigations of electronic data are usually carried out confidentially. In addition, the high-tech nature of

[49] See Article 8 of the Cybersecurity Law of the People's Republic of China.

[50] See Yongsheng Chen, 'The Challenges of the Cybercrime to Criminal Procedure and its Systematic Response' (2014) 3 Science of Law (Journal of Northwest University of the Political Science and Law) 149.

[51] Pursuant to Article 56 of the Criminal Procedure Law of the People's Republic of China (2018 Amendment), a confession of a criminal suspect or defendant extorted by torture or obtained by other illegal means and a witness or victim statement obtained by violence, threat, or other illegal means shall be excluded. If any physical or documentary evidence is not gathered under the statutory procedure, which may seriously affect justice, correction or justification shall be provided; otherwise, such evidence shall be excluded.

[52] See Yongsheng Chen, 'Construction of the System of Search and Seizure of Electronic Communication Data' (2019) 1 Global Law Review 19.

electronic data may also frustrate attempts to prove it is obtained illegally. Thirdly, the criminal compensation under the State Compensation Law of the People's Republic of China only covers physical harm and infringements to property rights,[53] meaning that other rights do not fall within the range of state compensation. For example, citizens' privacy of correspondence guaranteed by the Constitution of the People's Republic of China[54] is easily encroached upon in the investigation process of electronic data. Despite this, citizens are not entitled to apply for state compensation on the basis of the fact.[55] The State Compensation Law of the People's Republic of China had been amended twice since its enactment in 1994 and eight years had passed since its last revision. It is suggested that the next revisions should include provisions clearly stating that any harm stemming from the actions of authorities during the investigation process should fall within the remit of the State Compensation Law of the People's Republic of China.

5. Prospects

To summarize, great efforts have been dedicated by Chinese authorities to enhancing the regulations on electronic data in the past decades. Nevertheless, there is still room for further development of relevant regulations. The prospective reinforcement involves the idea of rights protection and the interaction between new technologies and evidence theory. On the one hand, it is urgent to strengthen the idea of rights protection of those individuals against illegal investigation, especially their right to know, privacy and property rights. Data protection is emphasized by the EU and the US but it has been neglected by China in relation to the process of collecting electronic data. Under Directive (EU) 2016/680, a string of requirements are detailed to intentionally protect privacy rights during the investigation process of criminal cases,[56] because the privacy protection guarantees are sector-specific and are located in a myriad of legislative instruments and case law, and the principles of lawfulness, fairness and transparency are also ingrained in the process of criminal investigation.[57] In contrast to the comprehensive legislative framework of the European Union, in China, according to Provisions 2016 and Rules 2019, even network service providers are required to assist with the collection of electronic data without any other restrictions on the process. It should also be noted that there are no provisions pertaining to the rights protection of the individuals being investigated. The significance of data protection in the collection process of electronic data should be considered in the draft of China's first Personal Information Protection Law.[58] What's more, from a legislative perspective, illegally obtained electronic data urgently needs to be included in the exclusion range of illegally obtained evidence under the Criminal Procedure Law of the People's Republic of China. Only by taking these steps can the criminal suspect's privacy rights be fully protected during the collection process of electronic data. On the other hand, the development of new technologies has challenged the current evidence theories and rules. In addition to the blockchain technology which can be used as a tool for the authentication of electronic data according to the Several Issues Concerning the Trial of Cases by Internet Courts,[59] a number of new technologies have come to prominence in judicial practice with no clear definition of them in the current rules, which leads the court to shoehorn them into existing rules by regarding them as other categories of evidence.[60] For example, Alibaba Group has devised several algorithms to prove the propensity of a certain user. What is the legal status of this kind of material produced by those algorithms? In other jurisdictions, some scholars have advocated that the evidence produced by new technologies should be treated separately from the existing evidence types and listed as an independent type of evidence,[61] while some others hold that it should be included in the existing types of evidence.[62] The particular prospect is that new rules peculiar to the evidence produced by new technologies should be made for better proving the credibility of its conveyance. It's right what the electronic data has gone.

Acknowledgments

This research was funded by the National Social Science Fund of China (No. 20FFXB062).

[53] See Article 17 of the State Compensation Law of the People's Republic of China (2012 Amendment).
[54] See Article 40 of the Constitution of the People's Republic of China (2018 Amendment).
[55] See Hua Guo & Hongxia Li, 'Remedy of Rights in the Collection of Electronic Data in Criminal Proceedings of China' (2019) 11 Social Sciences in Guangxi 121.
[56] See DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of the personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
[57] See Shawn Marie Boyne, 'Data Protection in the United States' (2018) 66 Am. J. Comp. L. 299.
[58] See Rong Hu, 'Application of the Location Service and Its Legislation in the Criminal Investigation' (2020) 4 Study & Exploration 60.
[59] Under Article 11 of the Several Issues Concerning the Trial of Cases by Internet Courts issued by the Supreme People's Court of the People's Republic of China, the Internet court shall confirm the electronic data submitted by the party concerned, provided that the authenticity of the electronic data can be proved through electronic signature, trusted time stamp, hash value check, blockchain or any other evidence collection, fixation or tamper-proofing technological means, or through the certification on an electronic evidence collection and preservation platform.
[60] See Andrea Roth, 'Machine Testimony' (2017) 126 Yale L. J. 1972. The situation in China is almost the same, see Pinxin Liu, 'On Big Data Evidence' (2019) 1 Global Law Review 24.
[61] See He Jiahong et al., 'Over the Challenge on Evidence Law in View of Investigation via Big Data' (2018) 1 People's Procuratorial Semimonthly 56.
[62] See Andrea Roth, 'Machine Testimony' (2017) 126 Yale L. J. 1972.