On the Nature of Online Retrieval of Electronic Data

WU Yingfei[*]

Abstract: *With the development of information technology, the online retrieval of remote electronic data has become an important method for investigative agencies to collect evidence. In the current normative documents, the online retrieval of electronic data is positioned as a new type of arbitrary investigative measure. However, study of its actual operation has found that the online retrieval of electronic data does not fully comply with the characteristics of arbitrary investigative measures. The root cause is its inaccurately defined nature due to analogy errors, an emphasis on the authenticity of electronic data at the cost of rights protection, insufficient effectiveness of normative documents to break through the boundaries of law, and superficial inconsistency found in the mechanical comparison with the nature of existing investigative measures causes. The nature of electronic data retrieved online should be defined according to different circumstances. The retrieval of electronic data disclosed on the Internet is an arbitrary investigative measure, and following procedural specifications should be sufficient. When investigators conceal their true identities and enter the cyberspace of the suspected crime through a registered account to extract dynamic electronic data for criminal activities, it is essentially a covert investigation in cyberspace, and they should follow the normative requirements for covert investigations. The retrieval of dynamic electronic data from private spaces is a technical investigative measure and should be implemented in accordance with the technical investigative procedures. Retrieval of remote "non-public electronic data involving privacy" is a mandatory investigative measure, and is essentially a search in the virtual space. Therefore, procedural specifications should be set in accordance with the standards of searching.*

Keywords: electronic data ♦ online retrieval ♦ compulsory investigation ♦ search ♦ right to privacy

The popularization of information networks makes life increasingly convenient for people, who can rely on them for online communication, shopping, payment and settlement and other activities that were only previously possible offline. However, while making people's lives more convenient, information networks also create concealed conditions for criminals to exploit them to perpetrate illegal and criminal activities such as remote communication with intention of committing crimes, payment and settlement. In the face of the growing trend of criminals using information networks to perpetrate crimes, particularly cyber fraud, online gambling, and other new types of crimes committed using information networks, it not only

[*] WU Yingfei (吴影飞), Doctoral Candidate, School of Law, People's Public Security University of China. This paper is the phased research result of the Supreme People's Procuratorate's procuratorial theory research program "Research on the Governance Problems of the Crime of Aiding Information Network Criminal Activities" (Project Approval Number GJ2023D28).

requires a lot of manpower, material and financial resources, but may also miss the best time to collect evidence and weaken the quality and efficiency of the fight against crime if the investigative organs still follow the outmoded method of conducting offline investigation and evidence collection at the place of the crime. In particular, the application of cloud storage, network disks and other network storage technologies pose new challenges to traditional methods of investigation and evidence collection. In the context of such crimes, the investigative organs also follow the new business form of fighting crimes in the Internet era, and actively adopt new technologies and methods for investigation and evidence collection in the information age. The remote online retrieval of electronic data has emerged as an effective means of evidence collection in the era of information networks for investigative organs. To this end, in September 2016, the Supreme People's Court and the Supreme People's Procuratorate, in conJunection with the Ministry of Public Security, formulated the *Provisions on Issues Concerning the Collection, Retrieval, Review and Judgment of Electronic Data in the Handling of Criminal Cases* (hereinafter referred to as the "*Electronic Data Provisions*"), which stipulate online retrieval of electronic data as a new investigation and evidence collection measure. The *Rules on the Evidence Collection of Electronic Data in the Handling of Criminal Cases by Public Security Organs* (hereinafter referred to as the "*Rules on the Evidence Collection of Electronic Data*"), formulated by the Ministry of Public Security in 2019, contain a special section detailing online retrieval of electronic data in the chapter on the collection and retrieval of electronic data. The nature of online retrieval of electronic data as a new type of investigative behavior is directly related to the regulation and procedural design of such investigative behavior, but it also seriously affects the protection of the rights of electronic data holders. Therefore, the nature of online retrieval of electronic data deserves further study. In order to effectively fight crimes and improve the efficiency of investigation and evidence collection in the era of information networks, the human rights protection function in criminal procedures should be taken into account when carrying out investigative measures, so that the investigative measure of online retrieval of electronic data can perform under the framework of the rule of law in criminal procedure, the abuse of investigative power is prevented with strict and standardized procedures, and citizens' right to privacy and information is effectively protected. This paper first explains the nature of the online retrieval of electronic data from the perspective of current normative documents. Then, starting with the practical operation pattern of online retrieval of electronic data after the implementation of the above two normative documents, this paper analyzes, judges and studies whether the nature of online retrieval of electronic data is consistent with the positioning of normative documents from an empirical viewpoint. Next, it analyzes the root cause of the conflict between the nature of the positioning and the practice of online retrieval of electronic data in the normative documents. Finally, it proposes the "should-be" nature of online retrieval of electronic data.

I. The Actual Nature of Online Retrieval of Electronic Data

Electronic data embodies basic rights such as property rights and the right to

privacy. Ensuring rights protection in the evidence collection of electronic data is a basic requirement of the *Criminal Procedure Law* to "respect and protect human rights."[1] Online retrieval is a measure for remote investigation and evidence collection of electronic data, and its nature is directly related to the rights protection of electronic data rights holders and the degree of regulation for the right to investigate in information cyberspace. The *Electronic Data Provisions and the Rules on the Evidence Collection of Electronic Data* stipulate online remote inspection as well as online retrieval. Some scholars elaborated on online retrieval and online remote inspection respectively in the research process.[2] In order to clarify the internal relationship, the author first expounds on the relationship between the two, and interprets the nature of online retrieval of electronic data from the perspective of the normative documents.

A. The relationship between online retrieval and online remote inspection

Previously, no clear distinction was made between online retrieval and online remote inspection in criminal justice practice, and remote inspection was a generic term[3]. The *Electronic Data Provisions* differentiate the two and present them in a progressive relationship, that is, online retrieval is generally performed through the network, and if necessary, online remote inspection is carried out. The *Rules on the Evidence Collection of Electronic Data* make a more detailed distinction: online retrieval includes online remote inspection because: first, the name of Section 4 of the *Rules on the Evidence Collection of Electronic Data* is "online retrieval of electronic data," and online remote inspection is stipulated under Section 4. Therefore, from the perspective of the system arrangement of the *Rules on the Evidence Collection of Electronic Data*, online remote inspection should be a method of online retrieval of electronic data, and this also meets the basic requirements of system interpretation. Second, it is also clear from the provisions of Article 27 (6) of the *Rules on the Evidence Collection of Electronic Data*[4] that online remote inspection is a method of online retrieval. It should be understood that online retrieval includes online remote inspection. Third, online retrieval and online remote inspection are stipulated in parallel in the relevant provisions, such as the acquisition of access rights and the circumstances under which the whole process should be recorded simultaneously. Fourth, according to the interpretation of the relationship between online remote inspection and online retrieval by the author of the *Rules on the Evidence Collection of Electronic Data*, online retrieval can be understood as a download action, including the download after online remote inspection.The ultimate purpose of online remote inspection is also online retrieval of electronic data, only that there is an inspection

---

[1] Xie Dengke, "Intervention with Fundamental Rights in Electronic Data-based Criminal Evidence Collection: Analysis Based on Six Typical Cases", *Human Rights* 1 (2021): 73.

[2] For example, Xie Dengke, "Reflection on and Reconstruction of Rules on Online Remote Inspection of Electronic Data," *Criminal Science* 1 (2020): 58-68; Xie Dengke, "Reflection on and Reconstruction of Rules on Online Retrieval of Electronic Data," *Oriental Law* 3 (2020): 89-100.

[3] Liu Haoyang, "Interpretation and Practice Guide to the Rules for Electronic Data-based Evidence Collection in Criminal Cases Handled by Public Security Organs," (Beijing: People's Public Security University of China Press, 2020), 124.

[4] See Article 27(6) of the *Rules on the Evidence Collection of Electronic Data*: Other situations where further discovery is required for online retrieval.

process.[5] Based on the above analysis, the author concludes that the nature of online remote inspection is the same as that of online retrieval, and it is a kind of online retrieval. Because this paper studies the nature of online retrieval of electronic data, and online remote inspection is a kind of online retrieval, online retrieval and online remote inspection are both taken into account in the process of discussion.

B. Nature of online retrieval of electronic data

According to the *Electronic Data Provisions* and the *Rules on the Evidence Collection of Electronic Data*, the author concludes that online retrieval of electronic data is a non-coercive investigative measure. Compulsory investigation means that the investigative organ will interfere with the basic rights of others when performing the investigative act and this is compulsory, while non-coercive investigation means that the investigative organ will not interfere with the basic rights of others when performing the investigative act and this is not coercive.

First, in accordance with article 174 of the *Provisions on the Procedures for the Handling of Criminal Cases by Public Security Organs* (hereinafter referred to as the "*Public Security Provisions*") and Article 169 of the *Criminal Procedure Rules of the People's Procuratorate*, only non-coercive investigative measures that do not restrict the personal and property rights of the object of investigation may be taken during the investigation and verification stage (formerly the preliminary investigation stage), and compulsory investigative measures are not allowed. Moreover, when interpreting the *Electronic Data Provisions*, the drafters hold that compulsory investigative measures can only be taken after a criminal case has been filed.[6] According to Article 6 of the *Electronic Data Provisions*, electronic data obtained through online retrieval in the preliminary investigation process can be used as evidence in criminal proceedings. This means that online retrieval is a kind of non-coercive investigation, because it is forbidden to take compulsory investigative measures before a case is filed, and it is much less likely that it can be used as evidence.

Second, judging from the provisions of the *Rules on the Evidence Collection of Electronic Data* on online retrieval and online remote inspection, it is basically the same as the *Criminal Procedure Law* and the *Public Security Provisions* in terms of retrieval procedures and on-site inspection procedures, such as making retrieval records, inviting witnesses for inspection and making an inspection record, the signatures of investigators and witnesses for the record, and one-by-one supplementary records for multiple inspections. According to the drafters of the *Rules on the Evidence Collection of Electronic Data*, online retrieval and remote inspection are similar to traditional on-site inspection and collection of trace items.[7] According to the *Public Security Provisions*, both investigative measures of retrieval and inspection are non-coercive investigative measures. Citing the works of Taiwan

---

[5] Zhou Jiahai and Yu Haisong, "Understanding and Application of 'Provisions on Issues Concerning the Collection, Retrieval, Review and Judgment of Electronic Data in Handling Criminal Cases'," *People's Judicature (Application)* 28 (2017): 34-35.

[6] Ibid., 33.

[7] Tian Hong, Zhai Xiaofei and Wang Yixiao, "Understanding and Application of 'Rules for Electronic Data-based Evidence Collection in Criminal Cases Handled by Public Security Organs'," *Police Station Work* 3 (2019): 10.

scholars, some scholars believe that there is a "compulsory investigation theory"[8] in inspections, but the scope for investigation defined in Taiwan is wide, including not only investigation in the narrow sense, but also searches and so on. Therefore, it is not appropriate to make comparisons.

Third, according to Article 33 of the *Rules on the Evidence Collection of Electronic Data*,[9] when performing online retrieval of electronic data or online remote inspection, the username and password provided by the holder or network service provider must be used, and the electronic data cannot be forcibly retrieved against the will of the electronic data holder or network service provider. This means that the consent of the holder of electronic data or the network service provider has been obtained when performing online retrieval of electronic data or online remote inspection. An act of prior consent does not interfere with basic rights, and is undoubtedly a type of non-coercive investigation. For example, the search itself is a compulsory investigative measure, and a writ of approval must be obtained before it can be performed, but if the party concerned agrees to the search, the search can be carried out without the writ. The search carried out with consent does not interfere with the basic rights of the party concerned, that is, it is a type of non-coercive investigation.

Fourth, compulsory investigation can only be performed outside the territory after the issuance of a writ by a neutral court. Although compulsory investigation in China does not require a writ from a judge, in China, an arrest must be approved by the people's procuratorate, and other compulsory investigative measures such as searches, account freezing, and detention shall be performed after being approved by the head of a public security organ at or above the county level in accordance with the *Criminal Procedure Law* and the *Public Security Provisions*. In principle, non-coercive investigative measures do not need to be approved by the head of a public security organ at or above the county level, such as freezing accounts as a compulsory investigative measure. The *Rules on the Evidence Collection of Electronic Data* also stipulate that the freezing of electronic data shall be subject to the approval of the head of a public security organ at or above the county level, but neither online retrieval nor online remote inspection requires approval from the head of a public security organ at or above the county level. Although the *Rules on the Evidence Collection of Electronic Data* require that county-level public security organs be responsible for online remote inspections, responsibility and approval do not belong to the same concept. In fact, any investigative act is the responsibility of public security organs at or above the county level, but the different internal organizations of the public security organs at or above the county level are specifically responsible for handling the matter, because, in China, the organs that can exercise the investigative power must be the investigative organs at or above the county level.

---

[8] Xie Dengke, "Reflection on and Reconstruction of Rules on Online Remote Inspection of Electronic Data," *Criminal Science* 1 (2020): 62-63.

[9] Article 33 of the *Rules on the Evidence Collection of Electronic Data* stipulates that when performing online retrieval or online remote inspection, access permissions for remote computer information systems such as usernames and passwords provided by the electronic data holder and network service providers shall be used.

Based on the above analysis of the relevant provisions of the *Electronic Data Provisions* and the *Rules on the Evidence Collection of Electronic Data*, it can be concluded that according to the current normative documents, online retrieval of electronic data includes online remote inspection, and both are non-coercive investigative measures.

II. The Operation Pattern of Online Retrieval of Electronic Data

Through the analysis of the normative documents mentioned above, it is confirmed that online remote inspection is a kind of online retrieval and both are non-coercive investigative measures. In order to learn more about the implementation of online retrieval and online remote inspection in practice, the author retrieved practical cases that were handled in recent years through China Judgements Online, to observe the operation pattern of online retrieval in practice, providing empirical support for further research. In order to verify the relationship between online retrieval and online remote inspection, the author also investigated the operation status of online remote inspection in practice.

A. The practical operation pattern of online retrieval of electronic data

Through searches on China Judgments Online, the author found that online retrieval is primarily manifested in the following types in practice: First, online retrieval of information published on webpages, WeChat public accounts, Weibo and others. For example, in the case of Liao spreading obscene materials for profit, the cybersecurity brigade of a public security organ lawfully retrieved a total of 27 screenshots online from the website "xxx.com" involved in the case in accordance with the law.[10] Second, online retrieval of personal registration information, information on operation records, organizational structure information, capital transaction information, etc.of criminal suspects who exploit the network to commit crimes.For example, in the case of Zhang operating a casino, the investigative organ obtained Zhang's agent account zy66xx from the "HaoXLi" overseas gambling website through online retrieval. The agent account has a total of five agent accounts with betting records and 32 membership accounts, and the total losses of members were more than 2.39 million yuan.[11] Third, online retrieval of electronic data from servers, such as in the case of Wang's infringement of citizens' personal information. From August to September 2020, the defendant Wang produced and sold software on the internet that could read all the text messages and address books of other people's mobile phones, and information on longitude and latitude positioning of the mobile phone and upload them to a designated server. The investigative organ conducted online retrieval of the electronic data in the server, which stored over 90,000 pieces of contact information,over 400 pieces of longitude and latitude location information and more than 40,000 text messages from other people's mobile phones.[12] Fourth, online

---

[10] See the (2021) Gui 01 Xingzhong No. 600 *Criminal Ruling* by the Intermediate People's Court of Nanning City, Guangxi Zhuang autonomous region.

[11] See the (2020) Yun 0521 Xingchu No. 143 Criminal Judgement by the People's Court of Shidian County, Yunnan Province.

[12] See the (2021) Jing 0101 Xingchu No. 13 Criminal Judgement by the Dongcheng District People's Court of Beijing.

retrieval of detailed capital transactions between suspects and others, for example, online retrieval of records on the Alipay transaction of criminal suspect Liu purchasing the game plug-in service from Yang, the records on the Alipay transaction of sale of game plug-ins, and WeChat payment transaction details in the case of Liu providing programs and tools for intrusion and illegal control of computer information system.[13] Fifth, online retrieval of electronic data such as WeChat chat records, QQ chat records, information from other instant messaging tools, information stored in personal space, and notepads on the suspect's mobile phone.For example, in the case of Ma transporting drugs, a public security organ's cybersecurity brigade retrieved defendant Ma(a)'s WeChat chat records, and defendant Ma(b)'s WeChat chat records and WeChat transfer records.[14] Sixth, online retrieval of electronic data stored by the criminal suspect on the internet cloud disks such as Baidu and Google. For example, in the case of Chen spreading obscene materials for profit, the investigative organ performed online retrieval of electronic data stored by Chen and others on the Baidu network disk.[15] Seventh, online retrieval of electronic data such as website background and database's system items, user management information, account information, system settings, operation steps, operation logs, parameter settings, and plug-ins installed. For example, in the fraud case of Xue, the investigative organ performed online retrieval of backend data from "hc.zhx.top" and other websites[16].

B. The practical operation pattern of electronic data from online remote inspection

After searches on the China Judgments Online, the author found that online remote inspection is primarily manifested in the following types in practice: First, electronic data on the public network such as webpages, WeChat public accounts, and apps involved in a case are retrieved through online remote inspection, and fixed retrieval is performed on webpage columns. For example, in the case of Luo operating a casino, a public security organ performed a remote inspection of the website www.h13x. On the website, there are sports events, chess and card games, lottery games, agency cooperation and other sections, and users need to log in to the account to use the services. The interface provides an online deposit function.The public security organ fixed and stored relevant content.[17] Second, online remote inspection of relevant WeChat groups, QQ chat groups and other communication groups for retrieving the information on communication groups' personnel, chat records, images, documents, group activity rules and other electronic data. For example, in the case of Song spreading obscene materials for profit, policemen from the cybersecurity brigade of a public security organ conducted a remote inspection of a WeChat group

---

[13] See the (2020) Su 0703 Xingchu No. 32 Criminal Judgement by the Lianyun District People's Court of Lianyungang City, Jiangsu Province.

[14] See the (2020) Qing 02 Xingzhong No. 114 Criminal Ruling by the Intermediate People's Court of Haidong City, Qinghai Province.

[15] See the (2020) Gan 0922 Xingchu No. 113 Criminal Judgment by the People's Court of Guazhou County, Gansu Province.

[16]See the (2019) Lu 09 Xingzhong No. 191 Criminal Judgment by the Intermediate People's Court of Tai'an City, Shandong Province.

[17] See the (2021) Gan 09 Xingzhong No. 59 Criminal Ruling by the Intermediate People's Court of Yichun City, Jiangxi Province.

named “First Grade X” from 10 o’clock on February 18, 2020 to 13 o’clock on February 22.It was found that the WeChat group had 205 members, and the member nicknamed “*labang wuren x*” posted a wealth of “notes” and URL links in the group. The policemen clicked on “notes” to reveal two short videos, and saved these in a folder on the local computer.[18] Third, an online remote inspection of the computer information system revealed a suspicious object and the IP address. The suspicious object attacked and damaged the computer information system to add, delete, and modify the computer information system.For example, in the case of Yao destroying the computer information system, the cybersecurity detachment of a public security organ conducted a remote inspection of the “internet service quality inspection system” developed by a technology limited liability company in Shenyang from 6 o’clock on November 4, 2018 to 12 o’clock on February 25, 2019. It was found that four IPs that illegally intruded the detection systems modified and deleted the system data.[19] Fourth, retrieval of electronic data stored on Baidu and other network disks through online remote inspection. For example, in the case of Qiu infringing on citizens’ personal information, policemen from a public security organ’s cybersecurity brigade conducted an online remote inspection in accordance with the law by logging in to Gao’s and Song’s accounts on 115 Network Disk and retrieved relevant documents online[20]. Fifth, retrieval of electronic data on websites and inspection of the relationship between superiors and subordinates of website account holders as well as capital transactions through online remote inspection.For example, in the case of Wang operating a casino, the cybersecurity detachment of a public security organ remotely inspected the website “Kai x”. It was found that the agent accounts b8x and b1x accepted bets totaling more than 3.01 million yuan from the subordinate accounts cqx and c0x from September 1 to September 30, 2015.[21] Sixth, conduct an online remote inspection to retrieve the page data disclosed by the website involved in the case, register and log in to the website according to the website requirements to inspect the posts, videos, and payment rules, and inspect the website’s backend data, such as the rules for background setting, the users of the website, the time when the website was established, management personnel, and the registration time of management personnel. For example, in the case of Li selling obscene materials for profit, the cybersecurity brigade of a public security organ retrieved and fixed the website www.vrfx.com involved in the case and its back-end management from 10:30 to 14:00 on September 13, 2020.[22]

C. Reflection on the operation pattern

First, through the observation of the operation pattern of online retrieval and

---

[18] See the (2021) Lu 09 Xingzhong No. 72 Criminal Ruling by the Intermediate People’s Court of Tai’an City, Shandong Province.

[19] See the (2021) Liao 01 Xingzhong No. 789 Criminal Ruling by the Intermediate People’s Court of Shenyang City, Liaoning Province.

[20] See the (2017) Su 0481 Xingchu No. 465 Criminal Judgment by the People’s Court of Liyang City, Jiangsu Province.

[21] See the (2021) Liao 0911 Xingchu No. 123 Criminal Judgment by the People’s Court of Xihe District, Fuxin City.

[22] See the (2021) Su 0830 Xingchu No. 2 Criminal Judgment by the People’s Court of Xuyi County, Jiangsu Province.

online remote inspection in practice, it can be found that there is basically no difference between the two in practice. Both can retrieve public electronic data on webpages and others, retrieve information such as details of capital transactions on Alipay and other platforms, online chat records, etc., as well as network backend data and internal structure relationships of the network, etc., only that their names are different. When the author communicated with the evidence collection personnel from the cybersecurity department of the investigative organ, they also said that it was difficult to distinguish between online retrieval and online remote inspection, and this is consistent with the above analysis of normative documents. Furthermore, some scholars note that "online retrieval" is a distinctive electronic inspection measure.[23] When explaining the difference between online retrieval and online remote inspection, drafters of the *Rules on the Evidence Collection of Electronic Data* pointed out that if electronic data is retrieved remotely in practice, the relevant circumstances can be recorded in both the *Remote Inspection Record* and the *Online Retrieval Record*.[24] It can be seen that online retrieval and online remote inspection are used interchangeably in practice, and the theoretical difference between the two is unclear.

Second, the definition of online retrieval as a non-coercive investigative measure is inconsistent with the actual situation. It somewhat stands to reason to define online retrieval of information publicly released on the internet, such as webpages and public accounts, as a non-coercive investigative act, because information disclosed on webpages, public accounts, etc., is voluntarily disclosed by the actor. An actor's willingness to disclose information means that the actor has waived his basic rights, and it is believed that the public disclosure of information does not affect his basic rights or has little impact, and it basically does not involve the actor's right to privacy, personal information right, or property rights. In addition to the investigative organs that collect relevant electronic data through online retrieval, anyone who logs in to the webpage or public account can retrieve such electronic data by taking screenshots or photos, recording videos, and downloading, among others. The *Personal Information Protection Law* (PIPL) also stipulates that information disclosed by individuals on their own or legally may be processed directly without the individual's consent.[25] However, in addition to retrieving electronic data publicly released online such as that on webpages and public accounts, online retrieval and online remote inspection also retrieves an actor's chat records on instant messaging tools such as WeChat, sensitive personal information on an actor's financial accounts on online platforms such as Alipay, and the backend data of websites. Such information involves basic rights and interests such as the right to privacy, property rights, and personal information rights. Despite the fact that the act of retrieving such information is not as obvious as the traditional interference with personal rights and property rights, modern rights such as the right to privacy and the right to personal information become increasingly important to people in the information age. This not only is stipulated in laws such as the *Civil Code* and the PIPL, but also has a constitutional basis. Clearly, it is not in

---

[23] Liu Pinxin, *Electronic Evidence Law* (Beijing: China Renmin University Press, 2021), 213.

[24] Tian Hong, Zhai Xiaofei and Wang Yixiao, "Understanding and Application of 'Rules for Electronic Data-based Evidence Collection in Criminal Cases Handled by Public Security Organs'," *Police Station Work* 3 (2019): 11.

[25] See Article 13 of the *Personal Information Protection Law*.

accord with the norms of criminal procedure to classify investigative acts that interfere with citizens' basic rights, such as the right to privacy and the right to information, as non-coercive investigative acts, because non-coercive investigative acts mean few constraints on investigators and can be independently performed by the case-handling departments or investigators of investigative organs, without the need for approval from a neutral judicial organ or even the head of an investigative organ at or above the county level. There is little control over investigative power. Therefore, there is a huge risk that the investigative organs or investigators will abuse the investigative powers.

Investigative acts that interfere with citizens' basic rights should be treated as compulsory investigative measures, because compulsory investigative measures are subject to more rigorous procedural control and constraints, and the abuse of compulsory investigative power by the investigative organs in criminal proceedings will be subject to corresponding procedural sanctions. According to the *Rules on the Evidence Collection of Electronic Data*, online retrieval and online remote inspection of electronic data should be performed using the username and password provided by the data holder or network service provider. This seems to mean that the consent of the electronic data holder or network service provider has been obtained for online retrieval, but is it really a fact that the electronic data holder or network service provider voluntarily provides the username and password to the investigative organs to collect evidence? In the case where the criminal suspects are deprived of their personal liberty and cannot realize their freedom of will, can the provision of the username and password be deemed consent? The "consent" to compulsory measures must be free and voluntary consent.[26] In criminal case investigation, it is rarely from suspect to case, but mostly from case to suspect. How can a suspect provide a username and password when the suspect is not present at the court? Moreover, electronic data is evolving rapidly, and it is lost if it is not retrieved in a timely manner. In practice, there have been cases where the investigative organs conduct remote online inspections to retrieve electronic data before the criminal suspect is present at a court of law. For example, in the case of Liu operating a casino, the public security organ conducted an online remote inspection on August 28, 2018, when Liu was not yet present at the court of law. The username and password obtained by remote inspection were obviously not provided by Liu, the holder of the electronic data. The investigation record does not specify the source of the data. Evidence retrieval is not in line with procedural provisions, and the defense does not recognize the legality of the electronic data.[27]

Third, there is the case of using online retrieval or online remote inspection to circumvent statutory investigative measures stipulated in the *Criminal Procedure Law*. For example, in the "July 11 online gambling case", investigators registered an account and password on a gambling website, and then used the account and password to enter the website system to remotely inspect the chip exchange rules,

---

[26] Lin Yuxiong, *Criminal Procedure Law* (General Part of Volume I) (Beijing: China Rennin University Press, 2005), 236.

[27] See the (2019) Lu 0683 Xingchu No. 262 Criminal Judgment by Laizhou Municipal People's Court, Shandong Province.

gambling process, and betting, among others.[28] On the surface, there is nothing wrong with performing such investigation acts through online remote inspection, but if such investigation act is analyzed in a traditional environment, it can be found that is this not the investigator or the person appointed by the investigative organ going to the casino to investigate and collect evidence disguised as a gambler? This is the investigation under concealed identity as stipulated in the *Criminal Procedure Law*, and this can only be conducted after going through strict approval procedures. If it is allowed to use online retrieval or online remote investigation to conduct concealed identity investigation when performing online remote evidence collection, is it not to substitute non-coercive investigation for statutory investigative measures? Moreover, it can be performed before a case is filed, thus circumventing the norms and restrictions of the *Criminal Procedure Law* on the concealed identity investigation, so that statutory investigative measures stipulated in the *Criminal Procedure Law* can be circumvented in cyberspace.

III. The Root Cause of the Mispositioning of the Nature of Online Electronic Data Retrieval

In order to facilitate the timely collection of electronic data by the investigative organs and to meet the needs of online retrieval of electronic data, the supreme judicial organs and the Ministry of Public Security creatively stipulate the investigative measure of online retrieval in normative documents in response to the needs of investigation and evidence collection in the information age. However, through the jurisprudential analysis of practical cases, the specific circumstances of electronic data retrieval are not differentiated for online retrieval, and they are all positioned as non-coercive investigative measures not in line with the classification characteristics of investigative measures. As a result, there is insufficient procedural regulation for such investigative measures and it is not consistent with the procedural jurisprudence of restricting the exercise of investigative power through standardized procedures. In order to position the nature of online retrieval of electronic data, the author tries to analyze the root cause of the mispositioning of the nature of online electronic data retrieval.

A. Wrong analogy of nature causes in accurate definition

Since the names of online retrieval and online remote inspection contain "retrieval" and "inspection," it is considered to be equivalent to or subordinate to retrieval and on-site inspection measures. Not only do some theoretical scholars believe that "remote inspection is a subordinate concept of inspection,"[29] but in practice, there are also judgments that classify remote inspection records as inspection records.[30] However, electronic data is special to some extent, and even if the same

---

[28] Liu Haoyang, *Interpretation and Practice Guide to the Rules for Electronic Data-based Evidence Collection in Criminal Cases Handled by Public Security Organs* (Beijing: People's Public Security University of China Press, 2020), 151-157.

[29] Xie Dengke, "Reflection on and Reconstruction of Rules on Online Remote Inspection of Electronic Data," *Criminal Science* 1 (2020): 60.

[30] See the (2021) Lu 09 Xingzhong No. 72 Criminal Ruling by the Intermediate People's Court of Tai'an City,

name applies, it should not be taken for granted that the two are of the same nature. Sometimes, even the same terms are not exactly the same if used in different contexts.For example, the close relatives stipulated in Article 108 of the *Criminal Procedure Law* of China and the persons counted as close relatives stipulated in Article 1045 of the *Civil Code* are not exactly the same. There is a certain jurisprudential basis for classifying on-site inspection as a non-coercive investigative measure. On-site inspection is an investigative act in which investigators conduct an examination and inspection of persons, items, and places related to the crime scene after the victim or other person reports a case, in order to collect traces and physical evidence left by criminals at the crime scene. If a victim chooses to report the case to the investigative organ after being assaulted by a criminal act, it means that the victim gives consent to the investigative organ's conducting of an inspection at the scene, hoping that the evidence of the crime can be found through on-site inspection, so that the criminal suspect can be captured, justice can be upheld for himself, and the losses he suffers can be recouped. This is why the victim seeks help from the investigative organ after being harmed by a criminal act. However, the investigative organ conducts online remote inspection mainly based on the username and password for the network information system provided by the holder of the electronic data, who is usually the criminal suspect in such cases. The criminal suspects are generally reluctant to provide evidence of their crime according to the psychology of seeking profit and avoiding harm, and the criminal suspect has the privilege against self-incrimination. Given the loss of personal freedom after being detained or arrested or under intense interrogation pressure, we can hardly say that the criminal suspect voluntarily provides a username and password, and allows the investigative organ to retrieve online his chat records, transaction details, and even the network system he uses to perform criminal activities, and collect electronic data unfavorable to him. Under the EU Regulation, consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[31] Even if a criminal suspect gives his username and password for the information network during interrogation, it does not mean that he naturally gives consent to the investigative organ's retrieving of online electronic data that is unfavorable to him, just as in the traditional process of evidence collection, can the investigative organ directly retrieve the physical evidence without going through the approval procedures after the criminal suspect is captured, and the key is searched from the body of the criminal suspect or is found according to the criminal suspect's confession? The answer is negative.The investigative organ must obtain a search warrant issued by the person responsible from the investigative organ at or above the county level before conducting the search. Therefore, retrieval of electronic data on the information network through online remote inspection here is essentially different from the retrieval of traces and physical evidence through the inspection of the crime scene.It is not comparable and is different in nature. Therefore, it cannot be attributed to non-coercive investigation. The practice of obtaining a password from an accused

---

Shandong Province.

[31] See Article 42 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

person to access a computer system also exists outside the territory, but approval must be obtained from the court of law. In the United Arab Emirates (UAE), for example, an access password obtained during the investigation is a highly important method of obtaining information. For the purposes of investigation, the accused offender is required to provide the authorities with the password to the computer system. The accused must provide information on their safe deposit box only if the court has issued a lawful order.[32]

The investigative organ's use of usernames and passwords provided by network service providers for online retrieval is actually online retrieval of electronic data with the consent of a third party (primarily network service provider). The case of the United States v. Blocker[33] gives us a good inspiration that the police obtained the consent of Blocker's mother to search the house they shared, but there was a locked cabinet in Blocker's room. The court ruled that the consent given by Blocker's mother to search could not extend to Blocker's cabinet, and that Blocker had the expectation of privacy for the locked cabinet in the room and that it was not allowed to conduct a search without a warrant based solely on the consent of Blocker's mother. Can the investigative organ directly retrieve the electronic data of the registered account solely with the consent of the network service provider? This is completely doable from a technical viewpoint, but the regulation of legal procedures cannot be simply based on whether it is technologically realizable, just like Blocker's locked cabinet, even if the police could open it. The crux of the question involves reasonable expectation of privacy. The practice of registering a username on the internet and setting a password means that network users do not want it to be found and used by others. It is the exclusive right of individuals in cyberspace, and belongs to the privacy space of individuals, but the privacy space here refers to virtual cyberspace. According to the Constitution, citizens' freedom of correspondence and privacy of correspondence are protected. The investigative organ can obtain information for the purposes of investigating crimes, but it can only be performed after the investigative organ goes through legal procedures. We can hardly say that the requirements of legal procedures are met if the investigative organ can retrieve personal electronic data on the information network online using the username and password provided by the network service provider. The United States distinguishes whether it is a public provider or a non-public provider when it comes to whether network service providers are allowed to disclose user or customer information. Public network service providers are generally not allowed to voluntarily disclose to government law enforcement agencies, and non-public service providers are allowed to make voluntary disclosure. Information disclosed by network service providers is subdivided, and five different mechanisms are set up according to different types of information, by which the government can compel network service providers to disclose information.[34] The five mechanisms are: subpoena, subpoena for prior notice

---

[32] See Khaled Aljneibi, "Search and Seizure for Electronic Evidence: Procedural Aspects of UAE's Legal System," *Digital Evidence and Electronic Signature Law Review* 10 (2013): 120.

[33] See United States v. Block, 590 F. 2d 535, 539 (4th Cir. 1978).

[34] H. Marshall Jarrett, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," United States, Department of Justice, Office of Legal Education, 2009, page 138, accessed June 6,

to the user or customer, court order, court order for prior notice to the user or customer, and search warrant. The five measures are mandatory information disclosure measures and are coercive. Investigators can compel disclosure of a user's basic information according to a federal or state grand jury, trial summons, or administrative summons authorized by federal or state code; and obtain most account logs and transaction records according to a court order issued by a federal magistrate, district tribunal, or equivalent state court judge. Investigators can obtain any information on the account based on a search warrant issued by a judge. The Council of Europe is reluctant to confirm that service providers will validly and voluntarily consent to the disclosure of their users' data under Article 32, because service providers are only data holders. They do not control or own the data, and therefore they do not have the right to give valid consent.[35]

B. Focus on the authenticity of evidence collection ignores the protection of rights

Through careful study of the provisions of the *Electronic Data Provisions* and the *Rules on the Evidence Collection of Electronic Data*, we can determine that in the process of retrieval of electronic data for evidence collection, the normative documents pay attention to the authenticity and integrity of electronic data collected and retrieved. For example, measures such as seizing the original storage medium of electronic data, calculating the integrity check value of retrieved electronic data, recording the evidence collection process and calculating its integrity check value, and making electronic data backups ensure the integrity and authenticity of electronic data. The exclusionary rules established for electronic data are also primarily made due to the fact that the authenticity and integrity of the collected and retrieved electronic data cannot be guaranteed. The Commission of Legislative Affairs of the Standing Committee of the National People's Congress also holds that electronic data retrieved online can be used as evidence as long as the authenticity and integrity of the electronic data can be ensured during the evidence collection process.[36] It can be seen that the main purpose of the aforementioned normative documents is to ensure the authenticity and integrity of electronic data. Although these lay down the legality requirements for electronic data, there are obvious deficiencies regarding the authenticity and integrity of electronic data, much less the protection of the rights of electronic data holders and owners, and there is apossibility that non-coercive investigation is used to circumvent compulsory investigation. Since electronic data is a novel thing, it is understandable that the first step is to ensure the authenticity and integrity of the collected and retrieved electronic data when regulating the collection of evidence, because progress in the rule of law needs to be explored step by step. This imperfection is manifested not only in the definition of the nature of the online retrieval of electronic data, but in the scope of online retrieval as well. The *Electronic Data Provisions* stipulate that online retrieval of electronic data stored in overseas

---

2022, https://www.justice.gov/file/442111/download.

[35] Anna-Maria Osula, "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study," 24 *International Journal of Law and Information Technology* 4 (2016): 354.

[36] Wan Chun et al., "Understanding and Application of 'Provisions on Issues Concerning the Collection, Retrieval, Review and Judgment of Electronic Data in Handling Criminal Cases'," *People's Procuratorial Semimonthly* 1 (2017): 52.

computer information systems may be performed. Considering that online retrieval of electronic data stored in overseas computer information systems will involve the cyber sovereignty of other countries and is likely to give rise to diplomatic problems, the Ministry of Public Security formulated the *Rules on the Evidence Collection of Electronic Data*, which stipulate that online retrieval conducted by the investigative organ is limited to electronic data stored in domestic remote computer information systems. As electronic data is a new type of evidence, it is practical and relatively reasonable to emphasize the guarantee of authenticity when formulating normative documents, but the pursuit of authenticity is not the sole purpose in criminal proceedings. It is also crucial to pay attention to protecting the basic rights of parties in criminal proceedings while pursuing truth, and to establish different procedural norms according to the types of rights that investigative acts may interfere with. This is the basic requirement of modern criminal proceedings and the inevitable requirement of human rights protection in criminal proceedings. Evidence collection from electronic data should not be an exception.

C. Limited validity of normative documents makes it hard to achieve breakthroughs

Whether it be online retrieval or online remote inspection, both are new remote evidence collection measures added under the *Electronic Data Provisions* according to the needs of electronic data-based evidence collection in the information network era, but these are not provided for in the *Criminal Procedure Law* and other basic laws. If they are defined as compulsory investigative measures, there is a risk of violating the legal provisions, since compulsory investigations involve interference with the basic rights of citizens. In accordance with the principle of law reservation, the legal basis of authorization must first be obtained for intervention in fundamental rights.[37] Therefore, investigative acts that deprive or restrict citizens' basic rights can only be stipulated by the supreme legislature by enacting or amending laws, and normative documents jointly formulated by the Ministry of Public Security, the Supreme People's Court, and the Supreme People's Procuratorate lack such powers. We can see that neither the *Electronic Data Provisions* nor the *Rules on the Evidence Collection of Electronic Data* define online retrieval and online remote inspection as compulsory investigations, but set a variety of preconditions to circumvent situations that may involve the deprivation or restriction of citizens' basic rights, such as clearly stipulating online retrieval and online remote inspection can only be performed using the username and password provided by the electronic data holder, so that online retrieval and online remote inspection are on the surface performed with the prior consent of the electronic data holder. They are not mandatory but non-coercive investigative measures. Therefore, the normative documents jointly formulated by the Ministry of Public Security, the Supreme People's Court, and the Supreme People's Procuratorate do not violate the corresponding legislative authority, and have legitimacy and legality. However, such provisions do not conform to the objective reality of electronic data-based evidence collection, restricting the means of evidence collection adopted by the investigative organs. For the purpose of fighting cyber

[37] Lin Yuxiong, *Coercive Measuresand Criminal Evidence* (Beijing: Peking University Press, 2010), 19.

crimes, the electronic data-based evidence collection departments of investigative organs are prone to violate the procedures stipulated in the current normative documents and abuse the investigative power in order to collect electronic data in a timely manner to prove crimes. This goes against effectively protecting the basic rights of electronic data holders, such as the right to privacy and the right to information, and it is also not conducive to maintaining authority in criminal proceedings.

D. Mechanical comparison of existing investigative measures causes outward discrepancies

According to the classification of verbal evidence and physical evidence, electronic data should belong to physical evidence. For the collection of physical evidence, there are compulsory investigative measures such as attachment, seizure, freezing, and search. After analyzing the *Electronic Data Provisions* and *Rules on the Evidence Collection of Electronic Data*, we can find that there are provisions for the attachment, seizure and freezing of electronic data for evidence collection, but no provisions for the search of electronic data. On the surface, the search for electronic data is different from that of traditional physical evidence, which is a tangible object that can be seen and touched. Therefore, the provisions of the *Criminal Procedure Law* on the object of search mainly refer to the person, objects, and residence, and the procedure design for the search is also conducted for the real space. For example, the search warrant must be presented to the person being searched, and the search record must be signed by the person being searched. Even the crime of unlawful search is provided for in Article 245 of the *Criminal Law* of China, and the targets of unlawful searches are also limited to people and homes, and are limited to real-world people and living spaces.

If online retrieval is positioned as a search act, the investigative organ may be unable to present the search warrant to the person being searched in advance when performing online retrieval. On the one hand, it is based on the need to collect evidence in cyberspace in a timely manner. If the investigative organ informs the other party in advance before collecting evidence, the other party may remotely destroy the electronic data involved in the case. On the other hand, the electronic data holder may not have been locked in when online evidence collection is being performed. Therefore, it may be unable or inconvenient to perform the obligation of advance notification during online retrieval, which is not completely in accordance with the current norms of search procedures in China. According to the *Criminal Procedure Law*, a search warrant must be presented to the person being searched at the time of the search. As regards whether the investigative organ must perform the obligation of advance notification when performing electronic data search, the idea stated in Article 35 of the PIPL is worthy of study: A state organ may handle personal information through notification in principle, and notification may not be made if such notification will hamper the performance of the duties of the state organ. Foreign experience can also provide a reference for us. The Council of Europe also discussed the issue of notification for searches in the process of drafting the *Convention on Cybercrime*. Considering that the laws of some parties do not specify an obligation to

notify in traditional search procedures, the issue of notification is left to the domestic law of each party. If a party takes into account the mandatory notice of the person concerned, notice may prejudice the investigation.If such a risk exists, delayed notice should be considered[38]. Section 2705 of the *Electronic Communications Privacy Act of 1986* of the United States stipulates an application to seek a court order, including a request. If the court decides that there is reason to believe that notice of the court order may have the effects of endangering the life or physical safety of an individual, escaping prosecution, destroying or falsifying evidence, threatening witnesses, seriously prejudicing an investigation, or unduly delaying a trial, the court shall allow a delay of not more than 90 days for notice.[39] It can be seen that notice in advance of a search is not a necessary element for performing a search, and post-event notice can be given according to the circumstances of the search.

Compared with traditional searches, online retrieval of electronic data or remote inspection is indeed not completely in line with the norms of search procedures.For investigative measures, we should not take a superficial look, but examine the essence of such investigative measures, that is, whether it interferes with the basic rights of citizens. Moreover, the object of search will continue to evolve with the progression of the times. New types of evidence such as electronic data did not yet emerge when search measures were provided for in China's *Criminal Procedure Law*, and it was all the more impossible at the time to foresee the issue of remote evidence collection based on electronic data. However, as social life is evolving and technology is being innovated, we must understand legal provisions in keeping with the times. The *UAE Code of Criminal Procedure* also did not take into account electronic data when being enacted, and the objects of searches primarily refer to human bodies, clothing, baggage or articles related to a crime. However, according to Article 51 of the *UAE Code of Criminal Procedure*, "articles" are defined broadly to include any object in any form. Therefore, police investigators can search computers for electronic data, because computers fall within the scope of "articles"[40]

IV. The Should-be Nature of Online Retrieval of Electronic Data

Through the above analysis, we can draw a basic conclusion that the definition of online retrieval of electronic data as non-coercive investigation is inconsistent with the objective reality of investigation, which does not favor the protection of the rights of electronic data holders or rights holders, nor the regulation of the exercise of investigative power. Given the characteristics of the types of electronic data, this paper distinguishes and defines the nature of online retrieval of electronic data according to the rights that online retrieval may interfere with as well as the extent under different circumstances.

A. Define the nature based on specific types of electronic data

Different scholars have performed different classifications according to different

---

[38] See Article 204 of Council of Europe, *Explanatory Report to the Convention on Cybercrime,* accessed June 10, 2022, https://rm.coe.int/16800cce5b.

[39] See Section 2705 of the *Electronic Communications Privacy Act of 1986*.

[40] Khaled Aljneibi, "Search and Seizure for Electronic Evidence: Procedural Aspects of UAE's Legal System," *Digital Evidence and Electronic Signature Law Review* 10 (2013): 120.

characteristics of electronic data,[41] such as static electronic data and dynamic electronic data; data message data, ancillary information data and system environment data; electronic data in closed systems, electronic data in open systems, and electronic data in dual systems; electronic data generated by electronic equipment, electronic data stored in electronic equipment, and electronic data mixed by electronic equipment; raw electronic data and transmitted electronic data; encrypted electronic data and unencrypted electronic data. On the basis of the above classification, the author analyzes the nature of online retrieval of electronic data in conJunection with the characteristics of online retrieval of electronic data.

1. **The nature of static electronic data and dynamic electronic data for online retrieval**

Static electronic data refers to the electronic data processed, stored, and output in digital information processing, storage, and output equipment. Static electronic data can be stored in a computer information system or in an external storage device. If static electronic data is stored in a computer information system that is not connected to the Internet or stored in external storage media such as a hard disk, online retrieval cannot be performed. Such electronic data can only be retrieved through traditional investigative measures such as search and seizure stipulated in the *Criminal Procedure Law*. If static electronic data is stored in a computer information system that is connected to the internet, it can be retrieved online through the network. If the electronic data to be retrieved does not involve the basic rights of others such as the right to privacy, the investigative organ may conduct online retrieval by means of non-coerciveinvestigation. If the electronic data involves the basic rights of others such as the right to privacy, it cannot be retrievedby non-coercive investigation, but should be retrieved online by the investigative organ through compulsory investigation.

Dynamic electronic data refers to the electronic evidence transmitted via the digital information network, such as e-mails transmitted through the network, webpages browsed, and network audio and video. Remote dynamic electronic data primarily relies on the internet for online evidence collection. For the retrieval of dynamic electronic data, different data types should be distinguished for the definition of nature. If it is the retrieval of dynamic electronic data such as webpages, audio and video that the public can browse and download by accessing the internet, the disclosure of electronic data by the electronic data rights holder means that others are allowed to browse and download such dynamic electronic data, and this basically does not involve interference with the rights of the data holder. It is a non-coercive investigative act, and it can be regulated with the retrieval procedure. If the dynamic electronic data on the internet may be suspected of being involved in criminal activities, the investigators can log in to gambling websites, pyramid selling system and other cyberspace through registered accounts under concealed identities, and

---

[41] For the classification of electronic data, see Pi Yong: *Research on Electronic Evidence Rules in Criminal Procedure* (Beijing: People's Public Security University of China Press, 2005), 8-21; Wang Zhenlin, “Research on Electronic Data Classification,” *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)* 3 (2013): 21-26; Liu Pinxin, *Electronic Evidence Law* (Beijing: China Renmin University Press, 2021), 6-7.

retrieve the dynamic electronic data used by the criminals to perpetrate criminal activities. Such acts of retrieving dynamic electronic data are essentially undercover investigations in cyberspace. Because investigators inevitably participate in some illegal and criminal activities during undercover investigations, the implementation of such investigative measures requires legal authorization.[42] Therefore, it should be performed in accordance with the procedures for undercover investigations as stipulated in the *Criminal Procedure Law*. Such investigative activities must be conducted only with the approval of the head of a public security organ after a case is filed, and they should not induce others to commit crimes in the process of undercover investigation. Only electronic data collected in accordance with statutory procedures can be used as evidence in criminal proceedings. Otherwise, it will amount to circumventing the implementation of statutory investigative measures on the grounds of new technologies, and this will easily give rise to the abuse of investigative powers. Moreover, the legality of collecting dynamic electronic data will also become a problem. The retrieval of dynamic electronic data in the private space involves citizens' freedom of correspondence and privacy of correspondence. It is an act of network electronic surveillance, and is a technical investigation measure that is part of compulsory investigation. Because it gravely interferes with the basic rights and interests of citizens, the *Criminal Procedure Law* sets strict conditions for technical investigative measures. Not all cases necessitate technical investigation. The cases involved must be major cases stipulated in the *Criminal Procedure Law*, and they must be implemented after a case has been filed through rigorous approval procedures. While the *Electronic Data Provisions and the Rules on the Evidence Collection of Electronic Data* also mention the retrieval of electronic data through technical investigative measures, they do not specify the conditions and circumstances under which technical investigative measures are adopted to collect electronic data.Technical investigative measures are investigative measures that significantly interfere with citizens' rights. When improving the rules in the future, the conditions and circumstances under which technical investigative measures may be applicable to remote online retrieval of electronic data should be clarified.

2. The nature of electronic data in online retrieved content information and electronic data in ancillary information

Electronic data from content information refers to electronic data that records the content of certain social activities, such as the body of emails or the content of online chats. The retrieval of electronic data from content information should be determined to be investigative acts of different natures based on their content. If the content information involves information that individuals are unwilling to disclose such as chat records and bank transaction details, the investigative organ will interfere with citizens' basic rights and interests such as the right to privacy and communication secrets when retrieving electronic data from such content information, and it should be positioned as a compulsory investigative act. If the content of the electronic data from content information does not involve the basic rights of individuals, it is a

[42] Li Shouwei, *Interpretation of the Criminal Procedure Law of the People's Republic of China* (Beijing: China Legal Publishing House, 2018), 363-364.

non-coercive investigative act.

Electronic data from ancillary information means that the electronic data does not record the content of social activities, but records the generation, storage, transmission, modification and addition of electronic data, such as system logs and file attributes. The electronic data of ancillary information exists on the basis of electronic data of the content information, and it can prove that the electronic data of the content information is generated and whether it has been added, deleted, modified, etc. Therefore, the electronic data of ancillary information should be retrieved remotely online at the same time as the electronic data of content information to prove whether the electronic data of retrieved content information is complete and true. The remote line retrieval of electronic data of ancillary information is generally the same as the retrieval of electronic data of content information in nature, but there are also situations where electronic data of content information does not involve privacy or freedom of correspondence, while electronic data of ancillary information involves privacy or freedom of correspondence.The act of the investigative organ to retrieve such electronic data of ancillary information shall belong to a compulsory investigation.

3. The nature of online retrieval of public electronic data and non-public electronic data

The distinction between public and non-public electronic data is made by the author based on the external presentation of electronic data. Public electronic data refers to the electronic data published on the public network, and it makes no distinction between domestic or foreign networks, such as the Internet and WeChat public accounts. Anyone can browse, copy, and download relevant information if they visit webpages and WeChat public accounts. Such information basically does not have the expectation of privacy. Publishing information in the public domain by the information holder and owner means that the expectation of privacy for such information is waived. General users can remotely browse, copy, and download it online through the Internet. Naturally, the investigative organs also have the right to browse, copy and download freely. Performing online retrieval of such data will not interfere with the electronic data holder's right to privacy and right to information, and it should be a non-coercive investigative act. Online retrieval can be performed in accordance with the retrieval procedures stipulated in the *Public Security Provisions*. This is also a common rule in Europe. Any party can retrieve computer data that people can access publicly, regardless of the geographical location of the data, even if the other party does not grant authorization.[43]

Non-public electronic data refers to electronic data stored in all kinds of computer information systems, apps, trading platforms, instant messaging tools, etc. Generally, network users set user names and passwords for non-public electronic data, and you can only use the correct username and password to log in to the information system for access. Such electronic data holders do not want others to freely access it by setting access permissions. The nature of non-public electronic data in information

---

[43] Council of Europe, *Convention on Cybercrime*, Article 32 (a), accessed June 5, 2022, https://rm.coe.int/1680081561.

systems should be defined according to different situations. The actor deliberately sets access permissions for the purpose of concealing the use of information networks for illegal and criminal activities. According to the "theory of no privacy for illegal information," the retrieval of such non-public electronic data involving illegal and criminal activities should be a non-coercive investigation, and online retrieval can be performed in accordance with the retrieval procedures stipulated in the *Public Security Provisions*. Online retrieval of non-public electronic data that does not involve the right to privacy, right to information, and others, shall also be a non-coercive investigation, and shall also be performed in accordance with the retrieval procedure. If the content of non-public electronic data in the information system is private information such as chat records and transaction records, it means that the electronic data holder does not want others to learn about it and there is reasonable expectation of privacy. Such online retrieval of electronic data by the investigative organ should not be positioned as a non-coercive investigative act, but should be a compulsory investigation act. The procedures should be designed in accordance with the requirements for compulsory investigation in the *Criminal Procedure Law*.

The nature of online retrieval of electronic data may vary according to the types of electronic data. Therefore, it cannot be generalized as a non-coercive investigative act.The nature of the electronic data should be accurately positioned according to its characteristics, in order to regulate the exercise of the investigative power and prevent the abuse of the investigative power and infringement on the rights of the electronic data holder, such as the right to privacy and right to information. In the above analysis of the types of electronic data, online retrieval of static electronic data involving citizens' right to privacy and right to privacy of correspondence, electronic data of content information involving the right to privacy and right to privacy of correspondence, electronic data of ancillary information involving the right to privacy and right to freedom of correspondence, and non-public electronic data involving the right to privacy is characterized as compulsory investigation. After it is characterized as a compulsory investigation, it is necessary to make clear whether it is a statutory investigative measure stipulated in the *Criminal Procedure Law*. Pursuant to the basic requirements of the statutory principle of compulsory investigation, compulsory investigation can only be performed with the express authorization of the law. The protection of the privacy of correspondence is an integral part of the protection of the individual's right to privacy[44]. The value of privacy is enshrined in Article 40 of the *Constitution* on freedom of correspondence and privacy of correspondence.[45] Therefore, the above types of electronic data can be summarized as non-public electronic data involving the right to privacy in the information network.For the convenience of argument, it is collectively referred to as "non-public electronic data involving the right to privacy."

B. The positioning of online retrieval of "non-public electronic data involving the

---

[44] Xu Chongde and Hu Jinguang, *The Constitution* (Beijing: China Renmin University Press, 2018), 164.

[45] Li Zhongxia, "The Constitutional Construction of the Right to Privacy in the Digital Age," *ECUPL Journal* 3 (2021): 46.

right to privacy"

After the online retrieval of "non-public electronic data involving the right to privacy" is characterized as a compulsory investigation act, should online retrieval or online remote inspection be redefined as a compulsory investigation measure or should a new type of compulsory investigation measure be established? The explanatory report to the *Convention on Cybercrime*[46] points out that some domestic criminal procedure laws stipulate that search and seizure refer to the power over tangible objects, and that many jurisdictions do not regard computer data as tangible objects. Therefore, it is impossible to conduct criminal investigations and proceedings in a way similar to that for tangible objects. The traditional search environment encompasses documents or records, and evidence used to be collected by search is in a tangible form, but in the context of new technology, many of the characteristics of traditional search are still maintained in terms of search for special computer data: for example, data collection takes place during the search and it targets the data that exists at the time; the preconditions for obtaining legal rights before performing a search are the same; regardless of whether the data is in tangible or electronic form, there is no difference in the trust degree required by legal authorization. Therefore, Article 19 (2) of the *Convention on Cybercrime* stipulates that each Party shall adopt such legislative and other measures as may be necessary to ensure that its authorities search or similarly access a specific computer system or part of it.[47] The use of the traditional concept of search expresses the exercise of the coercive power of the state. "Access" here is a neutral word that reflects the computer terminology more accurately and is the use of a modern term for a traditional concept.[48] The Council of Europe has adopted the search measure for the remote retrieval of electronic data from computer systems. According to the Fourth Amendment to the U.S. Constitution, search rules apply to the acquisition of data stored in computer systems based on the protection of reasonable expectation of privacy. "Where a search is performed for the purpose of retrieving data, such search must be in line with the premise and basis for exercising the general right to search," which shows that the search procedure is also applicable to the retrieval of electronic data in the Netherlands.[49]

Therefore, it is a consensus and a common practice to establish norms on electronic data-based evidence collection under the legal framework of the *Criminal Procedure Law* on investigation and evidence.[50] After analyzing the compulsory investigative measures stipulated in China's *Criminal Procedure Law*, the compulsory investigative measures that are targeted at people can be excluded, and the

---

[46]See Articles 184-186 of Council of Europe, *Explanatory Report to the Convention on Cybercrime*, accessed June 10, 2022, https://rm.coe.int/16800cce5b.

[47] Council of Europe, *Convention on Cybercrime* Article 19 (2), accessed June 5, 2022, https://rm.coe.int/1680081561.

[48] See Article 191 of Council of Europe, *Explanatory Report to the Convention on Cybercrime*, accessed June 10, 2022, https://rm.coe.int/16800cce5b.

[49] J.H.J. Verbaan: "Research on the Electronic Data Acquisition Procedure System in Criminal Investigation in the Netherlands," translated by Pei Wei, editor-in-chief Chu Dianqing, *Beihang Law*, vol. 2 (Beijing: China University of Political Science and Law Press, 2016), 7.

[50] Long Zongzhi, "Seeking a Balance between Effective Evidence Collection and Rights Guarantee: Comment on the Provisions on Electronic Data Evidence by the Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security," *Law Science* 11 (2016): 12.

compulsory investigative measures for objects mainly include attachment, seizure and search.Attachment and seizure are basically inconsistent with the characteristics of online retrieval of electronic data and can be excluded. Can the online retrieval of "non-public electronic data involving the right to privacy" be equivalent to the search measures as stipulated in China's *Criminal Procedure Law*? Below is a comparative analysis, and the similarities are as follows:

First, from the perspective of the subject of evidence collection, the traditional way of search requires that the subject of evidence collection is an investigator. The subject is also required to be an investigator for the online retrieval of electronic data. Of course, the retrieval of "non-public electronic data involving the right to privacy" in the remote computer information system is mainly performed by investigators with expertise in electronic data-based evidence collection, but the subjects of evidence collection are essentially investigators, except for the different division of labor.

Second, from the perspective of the purpose of investigation, traditional searches are for collecting evidence of crimes and capturing criminal suspects, while online retrieval is also for collecting evidence of crimes, that is, collecting "non-public electronic data involving the right to privacy" stored in remote computer systems. From the perspective of the purpose of investigation and evidence collection, the scope of traditional search is greater than that of online retrieval, because the scope of evidence obtained by traditional search includes not only electronic data, but also tangible evidence such as physical evidence and documentary evidence, while online retrieval only collects electronic data.

Third, from the perspective of the object of investigation and evidence collection, a traditional search is a search of the person, objects, residence, and other physical spaces conducted by the investigators of the investigative organs by means of the coercive force granted by the law, while the online retrieval of "non-public electronic data involving the right to privacy" is the online retrieval of electronic data from the remote network computer information system, that is, the virtual space. This is also the key to the difference between the two. Traditional searches are generally understood to be performed in real space. Can the investigative measures stipulated for real space equally apply to virtual information network space? To answer this question, we should not mechanically interpret the textual meaning, but should examine it for the purpose of regulation and protection. The *Criminal Procedure Law* stipulates that the purpose of such investigative measures is to regulate the search behavior of the investigative organs and to protect citizens' personal rights, right to privacy and other rights against wanton infringement by the investigative organs. As people attach greater importance to the right to privacy, the right to privacy is stipulated in the basic civil law, and the scope of the right to privacy is also broadened. Private space also falls into the category of the right to privacy[51]. It can be said that from the perspective of protecting legal interests, the right to privacy has become the superordinate concept of the right to housing, and the act of violating the right to housing is also a violation of the right to privacy. "Private space" includes not only

[51] See Article 1032 of the *Civil Code*, privacy is the undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others.

specific physical space such as residences, but also virtual space such as email addresses.[52] Therefore, improper searches may infringe on citizens' right to privacy. In some countries, whether it is allowed to interfere with citizens' right to privacy is used as an important criterion for judging whether an investigative act constitutes a search. The Fourth Amendment to the U.S. Constitution follows earlier legal texts and historical traditions for the scope of searches, and physical intrusion into tangible objects such as persons, residences, documents, and property constitutes a search. This was affirmed by the U.S. Supreme Court in the case of Olmstead v. United States (1928).[53] However, the objects of search changed significantly in the case of Katz v. United States in 1967.[54] Instead of the original tangible objects, the Fourth Amendment protects the people rather than places based on a reasonable expectation of privacy. As long as it interferes with another's reasonable expectation of privacy, it constitutes a search, and it is not limited to the real physical space.

Online retrieval of "non-public electronic data involving the right to privacy" is different from a search because in some cases, the online retrieval of "non-public electronic data involving the right to privacy" may not satisfy the requirements of the search procedure to produce a search warrant to the person being searched. The search of electronic data should be different from the traditional search of persons, objects, places, etc., because in a traditional search scene, the investigative organ can control the person being searched and their family members in a timely manner during a search after presenting a search warrant. It is difficult for the person being searched to destroy the evidence to be searched at the search scene. Even if the person wants to destroy it, the search personnel of the investigative organ can stop it in a timely manner. In particular, investigators now carry video recording equipment such as law enforcement recorders during a search, which can objectively record the search act. In comparison, electronic data can be easily forged, tampered with, or destroyed. An electronic data holder may destroy the electronic data with one click. If the traditional procedure of presenting a search warrant before a search is followed, electronic data may be added, deleted, or modified. In particular, if the search warrant is presented in advance in the process of remote search of electronic data, it will give the electronic data holder or the criminal suspect the opportunity to forge, tamper with, or destroy the electronic data, making it more difficult to collect electronic data. Moreover, it is impossible to identify the owner of the electronic data when performing an online search of electronic data, let alone present a search warrant. For an online remote search of electronic data, Article 132[55] of *New Zealand Search and Surveillance Act 2012* stipulates that the investigative organ shall first conduct a remote online search of the electronic data, and upon completion of the search, it may perform the

---

[52] See the Publicity and Education Bureau of the Publicity Department of the CPC Central Committee, the Civil Law Office of the Legislative Affairs Commission of the Standing Committee of the National People's Congress, and the Bureau of Law Popularization and Rule of Law of the Ministry of Justice, *Reader of Personality Rights Part of the "Civil Code of the People's Republic of China"* (Beijing: China Democratic Legal Publishing House, 2021), 116.

[53] See Olmstead v. United States, 277 U.S.438 (1928).

[54] See Katz v. United States, 389 U.S.347 (1967).

[55] Article 132 of *New Zealand Search and Surveillance Act 2012*, accessed June 9, 2022, https://www.legislation.govt.nz.

obligation to inform. Considering that the person being searched is far away from the investigative organ during the remote search, notification can take the form of modern communication methods such as by telephone or email, together with the electronic version of the search warrant, the start time of the search, electronic data retrieved (including integrity value check), the name and address of the case-handling authorities, etc. This not only ensures the effectiveness of the online search, but safeguards the right to know of the persons being searched and criminal suspects as well.

Accessing information stored in a computer breaks down the boundaries between public information and private information. It is more like entering a home or unpacking a package.[56] By comparing the similarities and differences between online retrieval of "non-public electronic data involving the right to privacy" and traditional search measures, we can see that retrieving "non-public electronic data involving the right to privacy" from a remote computer information system is essentially a search of the virtual space in the information age. Information technology has promoted the development of the internet, extending people's living space from the physical space to the electronic space and digital space, and gradually creating a virtual world.[57] Instead of sticking to traditional cognition, our understanding of place should take into account the development of information networks in order to broaden the cognition of space. Places should include not only the physical space of the real world, but also virtual space in the internet age. In New Zealand, search measures are also taken to retrieve electronic data from remote networks. For example, under the *Search and Surveillance Act 2012*, the "objects" of a search can also include intangible items such as email addresses or data information on network storage facilities.[58]

Therefore, regarding the "non-public electronic data involving the right to privacy" in the network information system, both online retrieval and online remote inspection are essentially a search of the non-public information system. Online retrieval of "non-public electronic data involving the right to privacy" should be regulated in accordance with the procedures for search measures in the *Criminal Procedure Law*, so as to regulate the exercise of the investigative power, prevent its abuse, and protect the rights of owners and holders of electronic data in the information age, such as the right to privacy and right to information.

Positioning the online retrieval of "non-public electronic data involving the right to privacy" as a search can solve the real dilemma.When it is necessary to crack the username and password for a remote computer information system, but it fails to meet the requirements of technical investigative measures, and the person being searched refuses to cooperate with the investigative organ in search, the investigative organ can forcibly search without the consent of the person being searched, because the search itself is compulsory. If the person being searched refuses to cooperate with the search, the investigative organ may unlock the door using technical or destructive means.

---

[56] Orin S. Kerr, "Searches and Seizures in a Digital World," 119 *Harvard Law Review* 2 (2005): 550.

[57] Zhang Kangzhi and Xiang Yuqiong, "The Construction of Policy Issues in Cyberspace," *Social Sciences in China* 2 (2015): 123.

[58] Article 97 of the *New Zealand Search and Surveillance Act 2012*, accessed June 9, 2022, https://www.legislation.govt.nz.

Like a physical door lock in real space, the username and password used on the computer information system are the "door locks" in the cyberspace. If the holder of the electronic data refuses to provide the username or password, the investigative organ may use technical means to crack the password and log in to retrieve relevant electronic data. Such an act of using technology to crack the username and password is not a technical investigative measure as stipulated in the *Criminal Procedure Law*.

Positioning the online retrieval of "non-public electronic data involving the right to privacy" as a search act under compulsory investigative measures not only regulates the nature of online retrieval, but also fully protects the basic rights of electronic data owners and holders such as the right to privacy, and will not have a material impact on investigation and evidence collection. The investigative organ is not required to obtain a writ in advance for any search. While China's *Criminal Procedure Law* does not provide for a consent search system, it can be concluded that a search can be performed with the consent of the person being searched without the need for a writ according to the basic legal principles of criminal procedure. If, in the case of an online search for "non-public electronic data involving the right to privacy," an online search can be conducted without the need to apply for a search warrant after the consent of the electronic data holder is obtained, the act of online search of electronic data with consent can completely supersede the online retrieval and online remote inspection based on the username and password provided by the electronic data holder as provided in the *Rules on the Evidence Collection of Electronic Data*. Of course, a search warrant must be obtained in advance for the search of "non-public electronic data involving the right to privacy" of an internet service provider.

When the holder of electronic data consents to the investigative organs' online search of electronic data, the investigative organ must ensure that the consent is given voluntarily. Before conducting an online search, the investigative organ shall inform the electronic data holder of the reasons for conducting an online search of electronic data, and expressly inform the electronic data holder of their right to freely choose to consent or refuse the search. If the holder of the electronic data refuses to provide the username and password, the investigative organ can only apply for a search warrant for an online search. If the holder of the electronic data consents to an online search by the investigative organ, they shall sign the letter of consent search for confirmation. Witnesses shall be present in the process of the holder of electronic data giving consent. Where there is no qualified person to serve as a witness, a video recording of the entire process of consent giving shall be conducted simultaneously, thus proving that the holder of electronic data voluntarily consents to an online search, and also serving as the basis for a later review of the criminal suspect's voluntary confession of guilt and acceptance of punishment.

Conclusion

Before 2017, the nature of the online search of electronic data in Germany was also highly controversial. In 2017, when the *Criminal Procedure Law* was amended, Article 100b provided for online search measures, thus establishing the compulsory

investigation attribute of online search of electronic data in the form of law.[59] China's *Criminal Procedure Law* stipulates electronic data as a type of evidence, but there are no provisions on the collection and retrieval of electronic data in the investigation chapter. This is incompatible with the positioning of electronic data as an independent type of evidence. It goes against regulating the procedures for the collection and retrieval of electronic data by the investigative organs, and also against protecting the litigation rights of the parties. On the basis of summarizing the practical experience in electronic data collection and retrieval, in conjunction with the theoretical research results, the author suggests that in the subsequent amendment to the *Criminal Procedure Law*, a special section should be added to the investigation chapter to stipulate the procedures for the collection and retrieval of electronic data, or the provisions on electronic data should be stipulated in the current investigative measure section according to the situation of electronic data collection and retrieval, so as to meet the needs of electronic data collection and retrieval. For online retrieval of electronic data, different situations should be distinguished: For electronic data publicly disclosed on the Internet that can be seen by people by logging in to the Internet, the investigative organ can achieve the purpose of standardization by retrieving electronic data. Investigators' act of entering cyberspace suspected of being involved in a crime under a fictitious identity to retrieve dynamic electronic data shall be determined to be undercover investigations in cyberspace. The retrieval of dynamic electronic data from private cyberspace should be an act of network electronic surveillance under technical investigative measures because its content involves citizens' freedom of correspondence and privacy of correspondence. The conditions and circumstances under which technical investigative measures may be applicable to the remote retrieval of electronic data should be made clear when the rules are going to be improved in the future, so as to regulate the application of technical investigative measures in network investigations. Search procedures should apply to "non-public electronic data involving the right to privacy" stored in computer information systems for regulation, and a flexible search notification system should be established according to the actual situation, so that notification can be made before or after the fact. A consent search system should be established simultaneously. This accommodates the types of rights that the act of online evidence collection may interfere with, and is also compatible with the investigative measures stipulated in China's *Criminal Procedure Law*. It can also balance the relationship between the protection of human rights and the fight against crimes in online evidence collection, thereby upholding procedural justice in the information network era.

(Translated by *NI Weisi*)

[59] Lin Yuxiong, Wang Shifan and Lian Mengqi, *Annotated Code Criminal Procedure of Germany* (Taipei: Sharing Publishing Co., Ltd., 2023), 174-180.