17

Digital Evidence and Cooperation of Service Providers in China

Li Zhe and Jin Zhenan

17.1 INTRODUCTION

China has persistently insisted on respecting cyberspace sovereignty and data sovereignty.[1] In the National Cyberspace Security Strategy launched by the Cyberspace Administration Office, China explicitly declares that state sovereignty has expanded into cyberspace, and that cyberspace sovereignty has become an important part of state sovereignty.[2]

Service providers in China are under quite strict control. They are obliged to retain certain data and to cooperate with authorities in both administrative proceedings and criminal investigations, as required by criminal and administrative laws, as well as more than thirty administrative regulations targeting different types of service providers. Due to the comprehensive and multifaceted administrative regulations on service providers and the mandatory requirement to store certain data within the territory of China, the cooperation of service providers in the process of both administrative proceedings and criminal investigations is quite successful domestically. There is no strong demand from the Chinese government for data retention by service providers; only a limited number of service providers are required to retain traffic data, normally for a period of sixty days.[3]

As to evidence collection in criminal proceedings, the Chinese Criminal Procedure Law (CPL)[4] does not satisfactorily differentiate collection of electronic evidence from collection of other physical evidence, nor does it distinguish the cooperation obligations of service providers from those imposed on other persons or entities, since there is only a general provision requiring that all the concerned personnel or entities shall provide evidence when ordered to do so by the investigative authority. As will be explained in this chapter, these provisions are supplemented by interpretations, guidelines and provisions adopted by different authorities; these supplementary documents function as 'loophole fillers' in some way, to meet the needs of specific investigative situations. But this approach results in some conflicts between the various applicable

[1] See, e.g., Yu Zhigang, 'The Concept of Cyberspace Sovereignty and the Innovation of Theories on the Rule of Law', *Guangming Daily*, 11 September 2016, 1, https://epaper.gmw.cn/gmrb/html/2016-09/11/nw.D110000gmrb_20160911_7-01.htm?div=-1 (in Chinese).

[2] Cyberspace Administration of China, The National Cyberspace Security Strategy, 27 December 2016, www.cac.gov.cn/2016-12/27/c_1120195926.htm (in Chinese).

[3] For example, Interim Provisions on the Administration of Internet Culture (IPAIC), 15 December 2017, Art. 20, http://zwgk.mct.gov.cn/zfxxgkml/zcfg/bmgz/202012/t20201204_905340.html (in Chinese); Provisions on the Administration of Internet Live-Streaming Services (Provisions AILSS), 4 November 2016, Art. 16, www.cac.gov.cn/2016-11/04/c_1119847629.htm (in Chinese).

[4] Adopted in 1979 and amended in 1996, 2012 and 2018. The following discussion is based on the 2018 version unless specified otherwise Chinese Criminal Procedure Law (CPL), 26 October 2018, www.npc.gov.cn/zgrdw/npc/xinwen/2018-11/05/content_2065631.htm (in Chinese).

documents – conflicts that need to be resolved. Without being rooted in the CPL, the newly created investigative methods[5] described by such documents actually lack justification. This chapter will examine this multilayered legal framework for electronic evidence collection, as well as the cooperation obligations thereof, followed by several comments to improve current Chinese practice.

Furthermore, in response to the rapid progress in data-dominated society, China has promulgated several laws, including the Cybersecurity Law,[6] the Data Security Law[7] and the Personal Information Protection Law (PIP Law),[8] to form a new order of data governance. However, with regard to cross-border cooperation in collection of electronic evidence, according to the Law on International Criminal Judicial Assistance (ICJA Law),[9] traditional mutual legal assistance is still the main approach, or even the only feasible approach.[10]

Partly serving as a response to the American Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[11] China has strengthened data localisation as a criterion to claim jurisdiction,[12] and requires that certain operators or service providers store certain types of data domestically. This includes information domestically generated or collected by critical information infrastructure operators, and the data domestically generated or collected by personal information processors that deal with a huge quantity of personal information.[13] Meanwhile, institutions, agencies and individuals within the territory of China are forbidden from providing evidentiary material and assistance prescribed by this Law to foreign countries without the approval of the competent authority of China.[14] Although the mandatory data localisation policy reduces the difficulty of collecting electronic evidence for Chinese law enforcement authorities (LEAs), the issue of cross-border cooperation in collecting electronic evidence is still an unavoidable question.

17.2 SETTING THE SCENE

17.2.1 *General Approach to the Collection of Electronic Evidence*

The laws adopted by the legislature, the National People's Congress and its Standing Committee, are usually abstract, which leaves space for interpretations, administrative regulations, guidelines and rules. There are two main types of interpretations: legislative interpretations by the Standing Committee of the National People's Congress; and judicial

[5] These methods include on-site extraction of electronic data, online extraction of electronic data and freezing electronic data.

[6] Cybersecurity Law, 7 November 2016, www.npc.gov.cn/zgrdw/npc/zfjc/zfjcelys/2016-11/07/content_2034939.htm (in Chinese).

[7] Data Security Law, 10 June 2021, www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (in Chinese).

[8] Personal Information Protection Law (PIP Law), 20 August 2021, www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (in Chinese).

[9] Law on International Criminal Judicial Assistance (ICJA Law), 26 October 2018, www.npc.gov.cn/zgrdw/npc/xinwen/2018-10/26/content_2064576.htm (in Chinese).

[10] ICJA Law, Art. 4; PIP Law, Art. 41; Data Security Law, Art. 36.

[11] Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of March 2018, www.justice.gov/criminal-oia/page/file/1152896/download.

[12] ICJA Law, Art. 25.

[13] Cybersecurity Law, Art. 37; PIP Law, Art. 40; Data Security Law, Art. 31.

[14] ICJA Law, Art 4; PIP Law, Art. 41; Data Security Law, Art. 36.

interpretations by the Supreme People's Court and the Supreme People's Procuratorate.[15] Contrary to an interpretation of law in a specific case or cases, the judicial interpretations of law by the prosecution offices and courts in China supplement the laws and are issued as guidance in a general manner.[16] Administrative regulations, guidelines and rules are enacted by the central government (the State Council), local governments and the ministries of the State Council.

The collection of electronic evidence is regulated very generally in the CPL, while most of the provisions concerning the collection of electronic evidence can be found in legislative interpretations, judicial interpretations, administrative regulations, guidelines and rules. This complex legal framework will now be analysed in more detail.

According to the 1996 CPL, the only type of evidence in electronic form was audiovisual material. In 2012, electronic data was added to the CPL as another type. However, the collection, identification and appraisal of electronic evidence was still not concretely regulated in the CPL.

In 2016, in order to meet the needs of judicial practice, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security jointly issued the Provisions on Several Issues Concerning the Collection, Taking, Examination and Judgment of Electronic Data in the Handling of Criminal Cases (Joint Provisions).[17] In 2019, based on the Joint Provisions, the Ministry of Public Security issued Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases (Rules MPS)[18] to further elaborate and clarify the Joint Provisions. The Rules MPS and the Joint Provisions have become the main resources for regulating collection of electronic evidence in Chinese criminal procedure, including the cooperation of service providers. The detailed provisions on this cooperation will be analysed in Section 17.4.2. Moreover, the Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies (Provisions PSA),[19] previously published by the Ministry of Public Security in 2012, were amended in 2020, adding some collection methods of electronic evidence provided in the Rules MPS.

To ensure their cooperation in criminal and administrative proceedings, service providers are required to retain data, preserve and disclose electronic data, as well as protect data privacy, respect data localisation and meet obligations with regard to cross-border transfer. Such obligations can be found in recently promulgated laws, namely the Counterterrorism Law,[20] the Cybersecurity Law, the Data Security Law and the ICJA Law. There are also more than thirty administrative regulations that specify these obligations of service providers.[21] To summarise,

[15] The People's Procuratorate is the official English name of what is called the public prosecutor's office in other legal systems. The following discussion will use the terms prosecution office and prosecutor, except when referring to the Supreme People's Procuratorate.

[16] Chen Chunlong, 'On the Status and Functions of Chinese Legal Interpretations' (2013) 1 *China Legal Science* 24–25 (in Chinese).

[17] Supreme People's Court, Supreme People's Procuratorate and Ministry of Public Security, 'The Provisions on Several Issues Concerning the Collection, Taking, Examination and Judgment of Electronic Data in the Handling of Criminal Cases' (Joint Provisions), 9 September 2016, www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml (in Chinese).

[18] Ministry of Public Security, 'Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases' (Rules MPS), 2 January 2019, https://app.mps.gov.cn/gdnps/pc/content.jsp?id=7449892 (in Chinese).

[19] Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies (Provisions PSA), 20 July 2020, www.gov.cn/zhengce/2021-12/25/content_5712867.htm (in Chinese).

[20] Counterterrorism Law, 27 April 2018, www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm (in Chinese).

[21] Among these regulations, some are general, namely the Decision of the Standing Committee of the National People's Congress on Strengthening Online Information Protection and the Provisions on Protecting the Personal

rules on data retention and the cooperation of service providers in criminal investigations in China can be found in criminal laws, supplementary legal documents, administrative laws and administrative regulations, as will be discussed in Sections 17.2.2 and 17.4.3.

17.2.2 *Data Retention Obligations*

17.2.2.1 Introduction

The PIP Law safeguards the security and privacy of users' information by setting up basic principles for the processing of personal information. Personal information refers to all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymised. Personal information processing includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information (Article 4 of the PIP Law). Information processing must follow the principle of lawfulness, legitimacy, necessity and good faith (Article 5) as well as the principle of openness and transparency (Article 7). Also, the following conditions must be fulfilled: obtaining the consent of users (Article 13); limiting the processing to that directly related to the processing purpose and in a manner that has the minimum impact on the rights and interests of individuals; and limiting the collection to the minimum scope necessary for achieving the processing purpose (Article 6).

Besides the collection and preservation of users' personal data for their own business purposes, service providers are under certain data retention obligations. However, the scope of data retained in China has a wider scope than personal information. Service providers are mostly required to retain users' traffic data, but certain types of service providers must also keep content data. That said, the content data to be retained is not the content of users' private communication but rather that of the products published by service providers or users. For example, online publishing service providers must retain the content of digital works they published online;[22] internet live-streaming service providers must retain the content that their users published.[23]

In most data retention cases, data is required to be retained in the servers of the service provider for a certain period (see Section 17.2.2.2), but in certain special circumstances, data must be handed over for record-filing to the Cyberspace Administration Office of China (in Chinese: Bei An) (see Section 17.2.2.3).

17.2.2.2 Data Retention in the Data Servers of Service Providers

The period for data retention varies according to the different types of service providers, as regulated in different administrative regulations. Service providers must preserve the data for a certain period of time, usually sixty days. For example, Article 20 of the Interim Provisions on

Information of Telecommunications and Internet Users, while others regulate only certain types of service provider, such as internet culture service providers (IPAIC), online publishing service providers (Provisions on the Administration of Online Publishing Services (Provisions AOPS), 4 February 2016, Art. 34, www.nppa.gov.cn/nppa/contents/770/103241.shtml (in Chinese)) and information service providers (Administrative Measures for Internet Information Services). Information service provider is a typical type that includes mobile internet applications information service providers (Provisions AMIAIS), news information service providers (Provisions for the Administration of Internet News Information Services (Provisions AINIS), CLI.4.293919, 2 May 2017, www.cac.gov.cn/2017-05/02/c_1120902760.htm) and so on.

[22] Provisions AOPS, Art. 34.

[23] Provisions AILSS, Art. 16.

the Administration of Internet Culture[24] states that internet cultural entities must retain the times of dissemination, the uniform resource locators (URLs) or domain names and the content of internet cultural products they provide for sixty days; Article 16 of the Provisions on the Administration of Internet Live-Streaming Services requires that internet live-streaming service providers retain logs of internet live-streaming service users and the content that they published for sixty days.

Sometimes the preservation period will be longer, depending on the applicable legislation. For example, the Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions[25] provide that network-based lending information intermediary agencies must record the internet access log, particulars of information interaction and other data of both lenders and borrowers and keep such data for five years from the expiry of the loan contract (Article 18, paragraph 2).

17.2.2.3 Record-Filing of Information to the Cybersecurity Administration Office of China

Ordinarily, data retention is conducted as storing the retained data on the service providers' own data servers. Nevertheless, certain types of service providers must preserve the data in another way: by putting it on record with the corresponding national or local Cyberspace Administration Office.

This record-filing method is a stricter approach to ensure cybersecurity, only targeting microblog service providers, public account information service platforms, internet news information services and public information services provided through instant messaging tools. The rationale for this more stringent requirement is that public accounts must fulfil their social responsibilities, avoiding the publishing of illegal information on mass or social media.

Article 9 of the Provisions on the Administration of Microblog Information Services,[26] Article 14 of the Provisions for the Administration of Internet News Information Services[27] and Article 7 of the Interim Provisions on the Administration of the Development of Public Information Services Provided through Instant Messaging Tools[28] contain similar requirements about this record-filing obligation. Providers of such information services must put users' accounts, service qualification of users' public accounts (to permit or license posting certain kinds of information, such as public news) and certain other information on record.

[24] IPAIC, Art. 20.

[25] Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions (IM for BAOLI), 17 August 2016, https://wap.miit.gov.cn/zcfg/xxtxl/art/2016/art_704cdd6af63c4071baf9ac837c5b08fd.html (in Chinese). The term 'online lending information intermediary institution' refers to financial information intermediary institutions legally formed to specially conduct online lending information intermediary business activities. Such type of institutions take the internet as the primary channel and provide information search, information release, credit rating, information exchange, credit matching and other services for direct lending between borrowers and lenders (IM for BAOLI, Art. 2).

[26] Provisions on the Administration of Microblog Information Services (Provisions AMIS), 2 February 2018, www.cac.gov.cn/2018-02/02/c_1122358726.htm (in Chinese).

[27] Provisions AINIS, Art. 14.

[28] Interim Provisions on the Administration of the Development of Public Information Services Provided through Instant Messaging Tools, 7 August 2014, Art. 7, https://www.cac.gov.cn/2014-08/07/c_1111983456.htm (in Chinese).

17.3 TERMINOLOGY AND CATEGORISATIONS

17.3.1 *Data*

17.3.1.1 Terminology

The Joint Provisions define the term 'electronic data' in Article 1: 'Electronic data is stored, processed and transmitted in electronic form and can be used to prove the facts of the case.'[29] In judicial practice, electronic data and electronic evidence are the two commonly used terms, with no significant difference between them.

17.3.1.2 Categorisations

Article 1 of the Joint Provisions also includes a non-exclusive list of forms of electronic data:

> Electronic data includes but is not limited to the following information and electronic documents:
>
> (1) Information published through such network platforms as webpage, blog, microblogs,[30] moments,[31] post bar,[32] and network drive.
> (2) Communication data in such network application services as SMS, e-mail, instant messaging, and group chat.
> (3) Information including user subscriber information, identity authentication information, electronic trading records, communication records, and log-on logs.
> (4) Electronic documents including documents, pictures, audio and video records, digital certificates, and computer programs.

The first type of electronic data published on internet platforms can be seen as public information, the collection of which does not entail infringement of individual rights and can thus take place with fewer limitations. The other three types of electronic data are more related to communication information of individuals, privacy and business secrets, the obtainment of which is more likely to cause conflict with individual rights[33] and requires a more stringent approval procedure. However, whether 'moments' postings on Wechat (a very popular communication app) are private or public information is still under discussion.[34] Moments are supposed to be open to all the contacts of the Wechat account owner who posted the moments, but if you are not listed in the contacts of the Wechat account owner, then either you cannot get access to the moments or you can get only limited access to them, depending on the settings of the Wechat account owner.

[29] All provisions quoted in this chapter have been translated into English by the authors.

[30] A microblog is a similar format to X (formerly Twitter) that is popular in China; it allows users to instantly update short texts and publish them publicly.

[31] Here, 'moments' refers in particular to a function of Wechat. Wechat is an instant messaging tool developed by Tencent Co Ltd. On the Moments page, users can publish photos and text (referred to as 'moments') and choose who can view them and comment on them.

[32] Post bar, or *Tieba* in Chinese, is a bulletin board system website where people sharing the same interests discuss and interact under their interested topics. Currently, the largest Chinese post bar is *Baidu Tieba* hosted by Chinese search engine company *Baidu*.

[33] Long Zongzhi, 'Seeking for the Balance of Effective Evidence Collection and the Guarantee of Rights: A Comment on Provisions in the Joint Provisions about Electronic Evidence' (2016) 11 *Law Science* 8 (in Chinese).

[34] See Pan Xiaoshuang and Yue Yuanzheng, 'Analysis on the Tendency of Compromising Private and Public Space of Wechat Moments' (2016) 4 *Radio &TV Journal* 147–148 (in Chinese).

17.3.2 *Service Provider*

The term 'service provider' appears in several laws and regulations. The first definition of 'service provider' in criminal law can be found in 2019 in a supplementary document jointly issued by the Supreme People's Court and the Supreme People's Procuratorate, entitled Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network (Interpretations IN).[35] That said, the term 'service provider' has been used in legislation long before it was defined in legal documents.

The Regulation on Telecommunications (RT)[36] first gives a list of all the types of telecommunication services[37] provided in China, as well as the corresponding licences that are needed before operating telecommunication services. The term 'telecommunication' here refers to 'the use of wired or wireless electromagnetic systems, or photoelectric systems, to transmit, emit or receive speech, text, data, graphics or any other form of information' (Article 2 of the RT). Telecommunication service providers are divided into basic telecommunication business providers and value-added telecommunication business providers (Article 8 of the RT). Basic telecommunication business refers to the provision of infrastructure of public networks, public data transmission and basic speech communication. So the providers of basic telecommunication business are the so-called carriers or telecommunication operators. Value-added telecommunication business refers to the provision of telecommunication and information services by using the infrastructure of public networks. There are eleven types of value-added telecommunication businesses. Among the eleven types, operators of internet access services (Type B14) must apply for an ISP (internet service provider) licence, whereas operators of internet information services (Type B25) must apply for either an ICP (internet content provider) licence, if the service is provided via the internet, or an SP (service provider) licence, if the service is provided via a non-internet network such as a fixed telecommunication network or a mobile communication network. However, the term 'service provider' in criminal procedure does not merely refer to providers with ISP, SP or ICP licences; it embraces all eleven types and even new types of telecommunication business that have not yet been regulated in the list.[38]

The Cybersecurity Law uses the term 'cyberspace operators', which refers to the owners and managers of cyberspaces, and cyberspace service providers (paragraph 3 of Article 76). However, the law does not further define the terms 'cyberspace owner', 'manager' and 'service provider'. Next, Article 24 of the Cybersecurity Law states that the service involved includes cyberspace access services, domain name registration services, access formalities for fixed-line telephone or mobile phone, information release and instant messaging. Articles 18 and 19 of the Counterterrorism Law[39] mention the terms 'telecommunication operators' and 'internet service

[35] Supreme People's Court and Supreme People's Procuratorate, 'Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network' (Interpretations IN), 21 October 2019, www.cac.gov.cn/2019-10/25/c_1573534999086260.htm?from=singlemessage (in Chinese).

[36] Regulation on Telecommunications (RT), 6 February 2016, www.gov.cn/zhengce/2020-12/26/content_5574368.htm (in Chinese).

[37] The list in force was issued in 2015 and amended in 2019.

[38] Based on Article 9 of the RT, telecommunication operators can operate new-type telecommunication business not covered by the list after they record the business at the telecommunication administrative authority.

[39] Counterterrorism Law, 27 April 2918, www.npc.gov.cn/npc/c30834/201806/d256505a5c254abdb07e2ff5d892d5d6.shtml (in Chinese) is administrative law in nature, regulating the system through which the government prevents and responds to terrorist activities. The crimes with regard to terrorism are provided in Articles 120 and 120-1 to 120-6 of the Criminal Law, 26 December 2020, www.npc.gov.cn/wxzlhgb/gb2021/202104/3a338df89b0a415481a9bf0571588f88/files/3d9248e01141484ead7d01b58958e0ae.pdf (in Chinese).

providers' when talking about the cooperation of service providers with the government and the police to fight against terrorism.

Furthermore, moving to the sphere of criminal law, Article 286-1 of the Criminal Law,[40] as amended in 2015, first used the term 'service providers' when it incriminated the action of 'refusing to perform the information network security management obligation'.[41] A service provider may commit the crime of failure to perform the information network security management obligation if it fails to fulfil its network security management obligation and refuses to correct its acts upon the competent authorities' order, thereby causing serious consequences.

The first definition of the term 'service provider' in the criminal law field appears in 2019 in the Interpretations IN. The Interpretations IN specify in Article 1 the elements of the aforementioned crime, 'refusing to perform the information network security management obligation', including a definition of service provider.

In accordance with Article 1 of the Interpretations IN, agencies, companies and individuals providing the following services shall be considered 'network service providers' as provided in paragraph 1 of Article 286-1 of the Criminal Law:

(1) Network access, DNS (or Domain Name Server) resolution, and other information network access, computing, storage, or transmission services;
(2) Information releasing, search engines, instant messaging, online payment, online booking, online sales, online games, online live-streaming, website construction, security protection, advertisement promotions, app stores, and other information network application services;
(3) public services such as e-governance, communications, power, transportation, water, finance, education, and medical care provided via information networks.

However, the service providers defined under the cooperation obligation provided in the CPL may cover a far more extensive range: all the 'relevant entities or individuals' as provided in Article 54 of the CPL are indiscriminately under the obligation to cooperate with the police in the framework of a criminal investigation. This includes, for instance, the suspect's school, employer or bank which may store individuals' data, but the relevant entity may also include any type of telecommunication operator and network service provider. Therefore, it can be concluded that in China, all telecommunication-related and internet-related entities are under a general obligation to cooperation with the prosecution office and the public security agency[42] in criminal investigations, although the details of cooperation agencies may slightly vary depending on the type of organisation.

17.4 DOMESTIC COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

17.4.1 *Introduction*

As explained in Section 17.3.2, the CPL entails a general cooperation obligation for service providers, as well as other relevant entities and individuals, to provide evidence and assistance during criminal investigations. In accordance with Article 52 of the CPL, judges, public prosecutors and investigators must ensure that all citizens who are involved in a case or who

[40] Criminal Law, Art. 286-1.
[41] For the definition of information network security management obligation, see Section 17.4.4.2.
[42] Usually, it is the public security organisations that investigate criminal cases, but the prosecution offices, the state security organisations and the prisons are responsible for investigation of certain crimes as provided by law.

have information about the case provide all available evidence and, except under special circumstances,[43] may ask such citizens to provide assistance in the investigation.

In China, the term LEAs covers all the authorities that enjoy investigative powers in criminal cases. The public security organisation is not the only authority investigating criminal cases; the national security authority,[44] the armed forces, the China Coast Guard, the prison,[45] the oversight commission (i.e. the anti-corruption agencies in China)[46] and the prosecution office[47] also enjoy certain investigative powers in specific cases. The provisions in the CPL generally describe the collection of electronic evidence powers of all the investigative agencies, except the investigative power of the oversight commissions, which is regulated in the Oversight Law. The concrete methods applicable to each authority are described in their corresponding supplementary documents, which results in slightly different investigative methods for each authority. For convenience, the following discussion will focus on the police and their powers, representing LEAs more in general.

Article 54 of the CPL states that when the courts, the prosecution offices or the public security agencies[48] collect and obtain evidence from the relevant entity or individual, the latter shall truthfully provide the requested evidence. The Counterterrorism Law, the Cybersecurity Law and the Data Security Law contain a specific cooperation obligation for service providers. In accordance with Article 18 of the Counterterrorism Law, both telecommunications business operators and internet service providers must provide technical interface, decryption and other technical support and assistance to the public security authorities and the national security authorities for the prevention and investigation of terrorist activities. Article 28 of the Cybersecurity Law states that service providers must provide technical support and assistance to public security agencies and national security agencies that are safeguarding national security and investigating criminal activities as required by law. Additionally, in accordance with Article 35 of the Data Security Law, service providers must cooperate with public security authorities or national security authorities for the purpose of maintaining national security or investigating crimes.

Moreover, according to Article 54 of the CPL, the evidence obtained during administrative proceedings can also be used as evidence in a criminal case. This shows that there is a close connection between criminal and administrative proceedings.

[43] For example, a physically or mentally handicapped person or a minor who cannot distinguish between right and wrong or cannot correctly express themselves will not serve as a witness (CPL, Art. 62). The spouse, a parent or a child of the defendant has the right to refuse to testify before court as a witness (CPL, Art. 193).

[44] Article 4 of the CPL provides that when handling criminal cases regarding compromising national security, the national security authorities perform the same functions as those of public security authorities.

[45] The security department of the armed forces has the authority to investigate criminal cases that occur within the armed forces; the China Coast Guard exercises the authority to investigate criminal cases that occur at sea; the prison investigates crimes committed by convicts within the prison (CPL, Art. 308).

[46] The oversight commission is responsible for investigating duty-related violations and crimes committed by public officials that exercise public power, such as suspected corruption, bribery, abuse of power, neglect of duty, power rent-seeking, tunnelling, practice of favouritism and falsification, as well as the waste of state assets (Oversight Law, 20 March 2018, Arts. 3, 11, www.npc.gov.cn/npc/c30834/201803/ce9c51c278f24ebab91b2178a4498404.shtml).

[47] The prosecution office is competent to investigate crimes committed by any justice functionary of false imprisonment, extortion of a confession by torture, or illegal search or any other crime that infringes upon a citizen's rights or damages the fair administration of justice by taking advantage of his or her functions. Where a case regarding a serious crime committed by any staff member of a government authority by taking advantage of his or her functions under the jurisdiction of a public security authority needs to be directly accepted by a prosecutor, the prosecutor may also have investigative power (CPL, Art. 19).

[48] In China, 'public security organisations' refers to a type of police that is responsible for maintaining public order and for preventing and investigating crimes. The police in China consist of police in public security organisations, state security organisations, prisons and organisations in charge of re-education through labour, as well as judicial police in courts and prosecution offices.

Therefore, in this section, we will discuss two questions. Firstly, we will present the detailed criminal procedures of how service providers cooperate with the police as stipulated in the CPL and the complementary regulations, guidelines and rules (see Section 17.4.2). Secondly, we will analyse how criminal investigations are connected to and influenced by the daily process of administrative supervision and control (see Section 17.4.3).

17.4.2 *Cooperation in Criminal Investigations*

In judicial practice, there are many cases where service providers cooperate with investigators in criminal investigations. Case-law research was conducted in Zhejiang Province (where China's biggest e-commerce company, Alibaba, is situated). The research was conducted on a sample of 483 cases from 1996 to 2016 in which the use of electronic evidence was explicitly mentioned. The results show that 109 out of the 483 cases include electronic evidence provided by a third party.[49]

Some cooperation practices have developed into conventional mechanisms, although they are not regulated in any specific legal documents. For example, in 2015, the State Council approved the establishment of the Inter-ministerial Joint Meeting on Matters Concerning the Work of Combating and Controlling New Telecommunication Network-Related Illegal and Criminal Activities. The government entities involved are the Ministry of Public Security and twenty-two other ministries. This joint meeting is a long-term multi-sector cooperation mechanism to fight against crimes of fraud through telecommunication networks. In the framework of this joint meeting, each province has established an anti-fraud centre that includes representatives of the three basic telecommunication companies – China Mobile, China Unicom and China Telecom – to facilitate the operations of the centre. This centre quickly disconnects phone numbers allegedly involved in telemarketing scams and shares relevant information with service providers and the police to suspend payments immediately.[50] This cooperation mechanism has already proven to be effective in 1,550,000 telecommunication fraud cases and, in the first nine months of 2020, a direct loss of 100 billion CNY was retrieved.

In Section 17.4.2.1, we will discuss the legislation of electronic data collection methods. This includes historical data and real-time data, and how service providers are required to cooperate in each of the methods.

17.4.2.1 Cooperation Obligations of Service Providers in the Collection of Historical Electronic Data

Service providers' participation and cooperation play an important role in gathering or extracting electronic data. Such participation and cooperation are basically regulated in the Provisions PSA, the Joint Provisions and the Rules MPS,[51] including obligations to provide assistance, to

[49] See, e.g., Feng Jiao, 'The Collection of Internet Evidence' (2018) 26 *Journal of National Prosecutors College* 36 (in Chinese). The author studied the criminal cases included in the judicial database PKULAW that happened in Zhejiang Province from 1996 to 2016 and were related with electronic data. The author identified 1,020 cases in total and 483 after excluding those that were substantively irrelevant.

[50] Zhang Yang and Wei Zhezhe, 'Focus on Fights against Telemarketing Scams: Inter-ministerial Joint Meeting of 23 Ministries', *People's Daily*, 14 September 2016, 2 (in Chinese).

[51] The Rules MPS have been developed from the Joint Provisions. The methods of electronic evidence collection provided in these two regulations are the same, but the Rules MPS adjust some details of the provisions. In the discussion that follows, we will therefore focus more on the Rules MPS.

preserve the original storage media, to produce electronic evidence at the request of the police and to freeze electronic data.

17.4.2.1.1 PROVIDING ASSISTANCE TO THE POLICE FOR COLLECTING ELECTRONIC DATA. Service providers may need to provide assistance when the police seize the original storage medium or extract electronic data on site[52] or online. In view of this seizure, the police must follow certain procedures as regulated in the Provisions PSA and the Rules MPS.

To seize original storage media, the police must deliver a written seizure order approved by the director of the case-handling department. Where it becomes necessary to seize property or assets on site during an inspection or a search, the person in charge at the scene has to make the decision. Where the property is highly valuable or its seizure might seriously impact routine business, the seizure must be done with a written Seizure Decision approved by the principal of the public security organisation at the county level or above (Article 228 of the Provisions PSA).

To extract electronic data on site, a record of on-site extraction of electronic data must be made. The investigators and the person in possession of, or providing, the electronic data are to sign it or affix a seal; if the aforementioned person is unable to sign or refuses to do so, this shall be noted in the record and an authenticating witness is to sign or affix a seal (Article 19 of the Rules MPS).

To extract electronic data online, the source, subject, goals and targets of the online extraction of electronic data must be indicated in the record, as well as the time, place, method and process of the extraction, and the reasons for being unable to seize the original storage media. An inventory of extracted and fixed electronic data is to be attached, indicating the type, document format, integrity check value and so on, and the investigators need to sign it or affix a seal (Article 26 of the Rules MPS).

For online remote inspections, the county-level public security agencies handling the case are the responsible authority (Article 28 of the Rules MPS) and the inspection process must be witnessed by qualified personnel (Article 30 of the Rules MPS). After remote inspections are concluded, a Remote Inspection Record must be promptly made, recording in detail the relevant circumstances as well as the inspection content such as pictures or screenshots; the investigators and the authenticating witnesses are to sign it or affix a seal (Article 31 of the Rules MPS).

The assistance given by service providers in this process can be threefold. First, when the police come to seize the original storage media or extract electronic data on site, service providers must not interfere with the police's work.

Second, when the investigators seize the original storage media, service providers must provide relevant information on request as far as they know, such as information about the original storage media and application systems, network topology and system layout, the identity of the users or managers, the user names and passwords for the original storage media and application systems, and the circumstances of data backups for the original storage media, that is, whether there are encrypted disks or containers, whether there are other mobile media, whether backups have been made, the location of backup storage data and so on (Article 15 of the Rules MPS).

Third, when making online extractions or remote online inspections, investigators must use the remote computer information access system (Article 33 of the Rules MPS), such as user names and passwords provided by the person in possession of the electronic data or network

[52] 'On site' means that the LEAs have the relevant computers or servers at hand.

service providers. This means that without their cooperation, the online extractions and remote online inspections could not succeed.

17.4.2.1.2 PRESERVING THE ORIGINAL STORAGE MEDIA. Service providers may need to preserve the original storage media when the original storage media cannot be seized and the electronic data cannot be extracted at once. In accordance with paragraph 2 of Article 22 of the Rules MPS, service providers must appropriately keep the original storage media and must not transfer, sell or destroy it; they must not unseal it; they must not access networks without the permission of the case-handling departments; and they must not add to, delete or modify electronic data which might be used as evidence. When necessary, the computer information system must be left in a turned-on state.

The procedure to give the original storage media to the service provider for preserving is also regulated in paragraphs 1 and 3 of the same article: The original storage media must be sealed after registering, photographing or video recording. Two copies of a registered preservation list must be made and signed or have a seal affixed by the investigators, the persons in possession (providers) and the authenticating witnesses. One copy of the list must be given to the persons in possession of the original storage media (providers) and the other copy must be put in the file along with the pictures or video. The police must decide on the disposition of the original storage media within seven days; where the decision is not made within this period, the order will be considered automatically lifted. Where they are confirmed as being unrelated to the case under investigation, the devices must be released within three days.

17.4.2.1.3 PRODUCING ELECTRONIC DATA. Service providers must produce data as required by the police. The difference between the obligation of providing assistance and that of producing electronic data lies in that when service providers provide assistance, it is the police that collect the evidence, but when producing electronic data, the electronic data is directly collected by the service providers.

To request service providers to produce data related to a criminal case, in accordance with Article 41 of the Rules MPS, the police must get approval from the director of the case-handling department and issue a notice of evidence collection to the service providers. The notice of evidence collection must specify relevant information about the electronic data targeted. The service providers must sign or seal the notice of evidence collection; if they refuse to sign or seal it, the police must note this. When necessary, methods such as audio or video recording can be used to fix the content of the evidence and the process of evidence gathering. Article 62 of the Provisions PSA states that the notice of evidence collection must clearly specify the evidence to be collected and the time limit for collection.

The Provisions PSA also regulate the procedure for the public security agencies to request service providers to provide emails. The seizure of suspects' email, as well as their mail and telegrams, must be approved by the principal of the public security organisation at or above the county level with a seizure order, requiring the post and telecommunications offices or service providers to check and hand over the relevant mail, telegrams or email for seizure. When there is no longer any need for seizure, the service providers must be notified to end the process (Article 232 of the Provisions PSA). If, upon verification, the email is found to be not relevant to the case, the seizure must be ended within three days (Article 233 of the Provisions PSA).

17.4.2.1.4 FREEZING ELECTRONIC DATA. Freezing will be employed in the following conditions: when there is a large volume of data that cannot be collected, or it is inconvenient to do so;

when the extraction time is long and might cause the electronic data to be tampered with or destroyed; or when the electronic data can be more intuitively displayed through network applications (Article 36 of the Rules MPS).

Service providers must freeze and unfreeze electronic data as ordered by the police. One or more of the following methods must be employed when freezing electronic data: calculating the electronic data's integrity check value; locking network application accounts; employing write-protection measures and other measures to prevent the addition, deletion or modification of electronic data (Article 40 of the Rules MPS).

The police must issue a notification of assistance in freezing electronic data or a notification of unfreezing of electronic data approved by the principal of a public security organisation at the county level or above, to the person in possession of the electronic data, the network service providers or relevant departments. The notification of assistance in freezing electronic data must state information such as the web accounts of the targeted data (Articles 37 and 38 of the Rules MPS).

The period for freezing electronic data is six months. Where it is necessary to extend the time limits due to special circumstances, the public security organisation must complete the procedures for continuation of the freezing before expiry of the freezing period. The period for each extension of freezing must not exceed six months. Where freezing is continued, the freezing procedure must be renewed. Where the period is exceeded without handling procedures, it is viewed as automatic unfreezing (Article 39 of the Rules MPS).

17.4.2.2 Collection of Real-Time Data as a Technical Measure

Paragraph 2 of Article 33 of the Rules MPS encompasses technical measures for collecting data in real time: when using technical measures to collect electronic data, approval procedures must be instituted in strict accordance with the relevant rules. The rules are provided in Part 2, Chapter 2, Section 8 of the CPL.

Technical investigative measures are used in criminal cases to secretly collect evidence related to suspects or persons with direct links to criminal activities, including monitoring records, tracing movements, intercepting communication and surveilling places. The scope of records monitored includes call records, consumption records of credit cards or debit cards, hotel check-in records and internet logs; tracing movements refers to tracing locations and paths; surveilling places refers to installing surveillance equipment in places where there may be evidence or facts of a crime.[53] When public security agencies adopt technical investigative measures, relevant entities and individuals, including service providers, have the obligation of cooperating with those public security organisations (paragraph 4 of Article 152 of the CPL). Because of their secrecy, technical investigative measures can be a serious threat to individuals' privacy and freedom of communication.[54] Therefore, even though not explicitly required by the CPL, the complementary principle[55] for technical investigative measures can be derived from the following rules established in the law to limit their usage.

[53] Liu Meixiang, 'Empirical Study on Supervisory Technical Investigative Measures' (2019) 4 *ECUPL Journal* 99 (in Chinese).

[54] Zhang Jianwei, 'The Procedure Specification and Information Processing of Technical Investigation', *Procuratorate Daily*, 4 July 2012, 3 (in Chinese).

[55] The complementary principle for technical investigative measures is also recognised as the last resort principle, meaning that technical investigative measures will be used only when other investigative measures do not work. Wang Dong, 'On Legal Regulations for Technical Detection' (2014) 5 *China Legal Science* 274 (in Chinese).

Firstly, technical investigative measures can be carried out only after the case is put on file and only to investigate the following crimes: crimes endangering state security, crimes of terrorist activities, organised crimes committed by groups in the nature of criminal syndicates, serious drug-related crimes or other crimes seriously endangering society, serious crimes where state personnel take advantage of their power to gravely infringe upon the personal rights of citizens (Article 150 of CPL) and serious duty-related crimes such as corruption and bribery (Article 28 of the Oversight Law). In pursuit of a fugitive criminal suspect or a fugitive defendant who is on the wanted list, or whose arrest has been approved or decided, necessary technical investigative measures may also be employed.

Secondly, technical investigative measures can be employed only after going through stringent approval procedures. To investigate crimes endangering state security, crimes of terrorist activities, organised crimes committed by groups in the nature of criminal syndicates, serious drug-related crimes or other crimes seriously endangering society, the competent authorities to employ technical investigative measures are the public security agencies at or above the municipal level (Article 150 of the CPL and Article 264 of the Provisions PSA). A report to require technical investigative measures must be sent to the principal of the public security organisation at or above the municipal level for approval (Article 265 of the Provisions PSA). If approved, an order adopting technical investigative measures will be issued and will be valid for three months (Article 151 of the CPL).

17.4.2.3 Comments on the Electronic Data Collection Procedure and Its Effects on the Cooperating Service Provider

Over the past decade we have observed the evolution of the regulations concerning collection of electronic evidence and technical investigative measures, seeking to restrict their application and protect personal privacy and freedom. However, there is still room for improvement. The following are some problems frequently discussed concerning electronic evidence collection procedures, which in some way cause difficulty for service providers in cooperating and are in conflict with service providers' mandate to protect customers.

The most significant problem is the procedure of electronic data collection. As introduced in Section 17.4.2.1, the Provisions PSA, the Rules MPS and the Joint Provisions all focus on different measures to be applied in the collection of electronic evidence, with little concern about the sensitivity of data or the degree of intrusiveness of certain measures. In the future, specific procedures should be designed based on a balance of crime investigation and human rights protection, especially the rights of privacy. As pointed out by some scholars, different types of electronic data must be collected via different procedures.[56] Content data and other data that is highly related to users' correspondence and privacy, namely the subjects of emails and information from big data that reflects personal lifestyle or daily routine, require a higher collection threshold and more procedural protections.[57] By applying some intrusive collection measures, we may need extra preconditions, for example to limit the application of certain

[56] Zhou Jiahai and Yu Haisong, 'The Interpretation and Application of the Provisions on Several Issues Concerning the Collection, Taking, Examination and Judgement of Electronic Data in the Handling of Criminal Cases' (2017) 28 *People's Judicature (Application)* 32 (in Chinese).

[57] Pei Wei, 'Internet Service Provider's Obligation of Disclosing Clients' Data During Criminal Investigation: From the Perspective of the Principle of Proportionality' (2016) 4 *Journal of Comparative Law* 103 (in Chinese); Pei Wei, 'Boundaries of ISP's Obligation in Assisting Law Enforcement: From the Perspective of Personal Data Protection' (2018) 1 *Journal of Cyber and Information Law* 46–47 (in Chinese).

collection procedures to more serious cases or to require approval from entities other than the investigative agencies.

The second problem concerns the principles of proportionality and data minimisation when coordinating concrete methods of electronic data collection. In China, seizure of the original storage media is ranked as the highest priority among all data collection methods.[58] As long as seizure of the original storage media is possible, it has to be conducted (Article 10 of the Rules MPS); only when seizure of the original storage media is not possible can the data be extracted (Article 9 of the Joint Provisions). This hierarchy may exist in consideration of the fact that seizure of the original storage media is a thorough preservation of all the information carried on it, including content information and system environment information, in order to prevent the electronic data from being deleted or altered.[59]

However, seizure of the original storage media when collecting electronic evidence may not always be necessary. Unlike traditional documentary evidence where you have to keep its physical form to maintain the integrity of the evidence, electronic evidence can be copied or extracted without taking its original storage devices and without destroying its evidentiary value.[60] Moreover, seizure may not be always appropriate, for the reason that seized original storage media often contain far more data besides the electronic data that would serve as evidence.

Thus, it is no wonder that such an investigation priority may cause conflicts with the principle of proportionality or data collection minimisation in legal practice. Paragraph 1 of Article 141 in the CPL establishes that all property and documents found during an investigation that may prove a criminal suspect's guilt or innocence must be sealed up or seized, except for property and documents that are irrelevant to the case. Article 4 of the Rules MPS also provides that any material obtained that is irrelevant to the case must be returned or destroyed in a timely manner. A widely discussed case related to seizure of original storage media is the case of QvodPlayer suspected of spreading pornography for profit in 2013.[61] QvodPlayer rented four servers from Beijing Wanglian Guangtong Technology Company. All four servers were seized in the later investigation because the investigators could not merely take the electronic data relevant to the case on the spot within a short period. The servers had a total capacity of 40 TB, among which only 29,841 videos were extracted and 21,251 videos were identified as pornographic.[62] The seizure obviously infringed the principle of proportionality.

The third problem regarding electronic data collection is the lack of differentiation from traditional evidence, disregarding the special nature of electronic evidence. Taking the seizure of emails as an example, as introduced in Section 17.4.2.1.3, the email seizure procedure imitates the traditional mail seizure procedure, leaving out the dissimilarity between traditional paper-based mail and email. Nowadays the electronic data in an email is reproducible and under the control of email service providers, so it is not difficult for the police to get a copy of an email from a service provider, without the knowledge of the email owner. Therefore, the procedure of email

[58] Pan Jingui and Li Guohua, 'The Electronic Evidence Collection Methods' Interference in Basic Rights and Their Improvements of Legislation' (2019) 5 *Social Sciences in Hunan* 75 (in Chinese).

[59] Chen Yongsheng, 'On Construction of Electronic Communication Data Search and Seizure System' (2019) 1 *Global Law Review* 16 (in Chinese).

[60] Pei Wei, 'On the Seizure of Media in Criminal Electronic Evidence Collection' (2020) 4 *Criminal Science* 6 (in Chinese).

[61] Criminal Final Instance of Beijing, First Intermediate Court of 2016 [(2016) Beijing 1 Criminal Final No. 592].

[62] Xie Dengke, 'An Analysis of Electronic Data and the Revolution of Criminal Proceedings from the Perspective of the QvodPlayer Case' (2018) 5 *Oriental Law* 49 (in Chinese).

seizure should be designed in a workable way given its electronic features and provide more protection to the email owner or the suspect.

Lastly, regarding the regulations of electronic data collection, as presented in Sections 17.4.1 and 17.4.2.1, the CPL includes only very abbreviated and ambiguous provisions concerning the collection of electronic evidence and the cooperation obligations of all persons and entities, including service providers. Therefore, the main legal resources of collecting electronic data rely unreasonably and disproportionately on supplementary legal documents, including the Provisions PSA, the Rules MPS and the Joint Provisions. To meet the need of electronic data collection in reality, instead of merely serving as guidelines for or further explanation of the investigative methods that already exist in the CPL, these documents created some new investigative methods that are not regulated in the CPL, and some of the methods are quite intrusive in nature. For example, extracting electronic data on site or online and freezing electronic data (from Article 16 to Article 40 in the Rules MPS; see earlier in Section 17.4.2.1) are the two methods that were created in the aforementioned supplementary legal documents, and their legality cannot be justified because of the lack of root provisions in the CPL.

17.4.3 *Electronic Evidence Collected in Administrative Proceedings to Be Used in Criminal Cases*

Besides the electronic evidence collected in criminal proceedings, the physical evidence (including electronic evidence) obtained by administrative agencies may also be submitted to criminal proceedings as evidence. In accordance with paragraph 2 of Article 54 of the CPL, physical evidence, documentary evidence, audiovisual materials, electronic data and other evidence gathered by administrative agencies during administrative proceedings (i.e. supervision or inspections and investigations resulting potentially in administrative sanctions) may be used as evidence in criminal cases. Therefore, in order to provide a better understanding of how electronic evidence can be introduced into criminal proceedings, it is necessary to discuss the main methods for administrative organisations to obtain electronic evidence and its admissibility in criminal cases.

17.4.3.1 Evidence Obtained in Administrative Proceedings via Cooperation by Service Providers

There are principally four types of cooperation obligations on service providers in administrative proceedings, namely: (1) monitoring and transmitting illegal data to the relevant authority (this may diverge from the principle in other countries that platforms take no responsibility for the content users publish or transmit); (2) submitting information upon the request of relevant administrative agencies; (3) keeping records for a certain period (discussed earlier in Section 17.2.2) and storing data within the territory of China (to be discussed in Section 17.5.2); and (4) complying with a real name registration obligation requiring users to provide real identity information. The details of these obligations vary from one type of service to another.

17.4.3.1.1 MONITORING AND TRANSMITTING ILLEGAL DATA. In principle, service providers take no responsibility for illegal information sent by users. But, with the increasing role the internet plays in people's lives, the laws and regulations, especially in the administrative field, have created exceptions under certain circumstances for certain types of service providers, typically news information service providers (Article 16 of the Provisions for the Administration of Internet

News Information Services), internet forum and community service providers (Article 7 of the Provisions on the Administration of Internet Forum and Community Services)[63] and comments posting service providers (Article 4 of the Provisions on the Administration of Internet Comments Posting Services).[64] When discovering the transmission of illegal information,[65] service providers must immediately cease the transmission, preserve relevant records, delete relevant information and report the event to the relevant authorities.[66]

17.4.3.1.2 SUBMITTING INFORMATION UPON THE REQUEST OF ADMINISTRATIVE AGENCIES. Furthermore, service providers in China are also under an obligation to cooperate at the request of relevant administrative agencies, besides police and prosecutors. There are mainly two types of requests.

The first one consists in providing information. For example, the E-commerce Law[67] provides that e-commerce business operators must produce e-commerce data and information when relevant authorities require them to do so in accordance with laws or administrative regulations (Article 25 of the E-commerce Law).

The second type of request is to cease the transmission of and delete the illegal information. Certain departments of the government have the authority to supervise the information on the internet; when discovering illegal information related to their authority, they will request the service providers to take action, including preserving the relevant records and providing assistance in the investigation.

17.4.3.1.3 REAL NAME REGISTRATION OBLIGATION. Since 2012, businesses that provide network access and domain name registration services, that handle stationary or mobile phone network access or that offer information publication or instant messaging services must require users to provide real identity information at the moment of signing the agreement or when confirming the provision of services. Users that do not register in their real name will not be offered full service.

17.4.3.2 Collection Requirements and Admissibility of Electronic Evidence

For now, no general provisions on electronic data collection – from any laws or regulations – are universally applied to all administrative proceedings. The provisions are scattered over various administrative laws and regulations. For the public security organisation, since it has both criminal and administrative investigative powers, the collection of electronic evidence in both proceedings basically follows the same requirements.[68] Other administrative laws and regulations set even

[63] Provisions on the Administration of Internet Forum and Community Services (Provisions AIFCS), 25 August 2017, Art. 16, www.cac.gov.cn/2017-08/25/c_1121541921.htm (in Chinese).

[64] Provisions on the Administration of Internet Comments Posting Services (Provisions AICPS), 16 November 2022, Art. 4, www.cac.gov.cn/2022-11/16/c_1670253725725039.htm (in Chinese).

[65] In general, the following three types of information are considered illegal: information that endangers national security and public interest; information that infringes private rights; and information that breaks public order and good morals (Cybersecurity Law, Art. 12). The exact range of illegal information may be slightly different depending on the applicable law or regulations.

[66] The procedure may vary depending upon the applicable law or regulations. For example, the Administrative Measures for Internet Information Services do not explicitly require the deletion of illegal information, while the Counterterrorism Law does.

[67] E-commerce Law, 31 August 2018, www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060834.htm (in Chinese).

[68] See, e.g., Provisions on the Procedures for Handling Administrative Cases by Public Security Organisations (Provisions HACPSO), 6 August 2020, Art. 32, www.nia.gov.cn/News/new/content.jsp?id=1460750 (in Chinese). The Provisions were first issued in 2012 and amended in 2014, 2018 and 2020. The discussion here focuses on the 2020 version.

higher standards for electronic data collection. For example, in accordance with Article 4 of the Guiding Opinions of the State Administration for Industry and Commerce on Collection of Electronic Data Evidence by Administrations for Industry and Commerce,[69] electronic evidence must be collected in the presence of at least two law enforcement officers, and at least one officer must have expertise with computer systems. This contrasts with the Joint Provisions and the Rules MPS, which do not specify the qualifications of the investigators.

It is important to highlight that there have been several criminal cases where electronic data collected by administrative authorities was not accepted by the court.[70] As provided by Article 54 of the CPL, evidence collected in administrative proceedings may be excluded because of its potential substantial damage to due process rights.[71] The government is now constructing information-sharing platforms among administrative authorities, police, prosecution offices and courts, so that the electronic data collected by administrative authorities can be safely stored and conveniently transmitted to the criminal proceedings.[72]

17.4.4 *Responsibility for Failure to Cooperate*

The cooperation obligations for service providers are, both in administrative proceedings and in criminal investigations, mandatory in nature. Failure to fulfil those cooperation obligations will result in administrative sanctions or even criminal liability.

17.4.4.1 Administrative Sanctions for Failure to Fulfil Cooperation Obligations

Service providers are obliged to cooperate with the police in administrative proceedings and criminal investigations. Failure to do so will lead to administrative sanctions. These sanctions are primarily laid down in Articles 61, 68 and 69 of the Cybersecurity Law, Article 48 of the Data Security Law and Article 84 of the Counterterrorism Law. Other regulations, such as the Administrative Measures for Internet Information Services,[73] the Provisions on the Administration of Internet Audio-Visual Program Service[74] and the Interim Provisions on the Administration of Internet Culture, also contain sanctions for failure to fulfil the administrative obligations therein provided. The administrative sanctions usually include an order for correction, a suspension or termination of operations, administrative fines and even detention of the director and the responsible personnel.

[69] Guiding Opinions of the State Administration for Industry and Commerce on Collection of Electronic Data Evidence by Administrations for Industry and Commerce, No. 248, 12 December 2011, Art. 4, www.waizi.org.cn/law/11557.html (in Chinese).

[70] See Pei Wei, 'The Connection of the Electronic Forensics Rules Before and After Criminal Recording: From the Perspective of Procedural Nature of Electronic Evidence' (2019) 2 *Contemporary Law Review* 115 (in Chinese).

[71] See ibid., 118.

[72] See Liu Yong, 'Study on the Electronic Data Convergence Mechanism of Administrative Law and Criminal Law under the Background of Big Data' (2018) 5 *Administrative Law Review* 132–135 (in Chinese). The construction of information sharing platforms can be found in documents such as: State Council, Section Legislative Affairs, 'Opinions of Strengthening the Convergence Works of Administrative Legal Enforcement and Criminal Judiciary', 9 February 2011; and State Administration for Industry and Commerce, Ministry of Public Security and Supreme People's Procuratorate, 'Opinions on Several Issues of Strengthening the Convergence and Assistance Works of Industry and Business Administrative Legal Enforcement and Criminal Judiciary', 18 December 2012.

[73] Administrative Measures for Internet Information Services, 8 January 2011, www.gov.cn/zhengce/2020-12/26/content_5574367.htm (in Chinese).

[74] Provisions on the Administration of Internet Audio-Visual Program Service, No. 3, 28 August 2015, www.gov.cn/gongbao/content/2015/content_2975891.htm (in Chinese).

More in particular, Article 61 of the Cybersecurity Law provides sanctions for failure to fulfil the real name obligation. The competent department must order the service provider to take corrective action. If the latter fails to take corrective action or if the circumstances are serious, it shall be fined not less than 50,000 CNY but not more than 500,000 CNY, and the competent department may order it to suspend relevant business operations, cease business operations for rectification or close down the website, or it may revoke the relevant business permit or business licence, and impose a fine of not less than 10,000 CNY but not more than 100,000 CNY on its directly responsible person in charge and other directly liable persons.

Articles 68 and 69 of the Cybersecurity Law provide the sanctions for failure to monitor and transmit illegal data to the relevant authority and failure to submit information upon the request of relevant administrative agencies and failure to provide technical support and assistance to the police or a state security authority; Article 48 of the Data Security Law provides sanctions for failure to cooperate with the police or a state security authority when investigating crimes or maintaining national security. The sanctions are similar to those in the aforementioned Article 61 of the Cybersecurity Law.

Article 84 of the Counterterrorism Law encompasses sanctions for failure to provide technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by the police or a national security authority as required; or failure to cease the transmission and deletion of information with any terrorist or extremist content, preserve the relevant records, shut down the relevant website or terminate provision of the relevant services according to the requirements of the competent department; or failure to implement network security, information content supervision rules or technical measures for security prevention, which causes the dissemination of information with any terrorist or extremist content and the circumstances are serious. The competent department shall impose a fine of not less than 200,000 CNY but not more than 500,000 CNY on the violator, and impose a fine of not more than 100,000 CNY on its directly responsible persons in charge and other directly liable persons; if the circumstances are serious, it shall impose a fine of not less than 500,000 CNY on the violator, and impose a fine of not less than 100,000 CNY but not more than 500,000 CNY on its directly responsible persons in charge and other directly liable persons, and the public security authority may detain its directly responsible persons in charge and other directly liable persons for not less than five days but not more than fifteen days.

Before deciding to impose sanctions, the competent administrative department usually has a disciplinary interview with non-cooperative service providers. This disciplinary interview works as a soft method to promote service providers' cooperation. Indeed, it is an essential tool of the Chinese government to supervise and control the internet before formal sanctioning, helping to make up for the lack of law enforcement resources, to clarify service providers' obligations case by case and to urge service providers to meet their obligations.[75]

17.4.4.2 Criminal Liability for Failure to Fulfil Cooperation Obligations

In addition to the aforementioned administrative sanctions, failure to fulfil cooperation obligations may also result in criminal liability. In case of non-cooperation, service providers can be prosecuted for the crime of 'refusing to perform the information network security management

[75] Lu Chao, 'The Research on Administrative Negotiation Tool in China's Internet Content Regulation' (2019) 2 *Chinese Public Administration* 42–44 (in Chinese).

obligation' provided in Article 286-1 of the Criminal Law as amended in 2015. A conviction of this crime requires all of the following elements:

(1) the service provider has 'obligations for security management of information networks' as prescribed by laws and administrative regulations, but fails to meet these obligations;
(2) it refuses to correct its acts as ordered by the competent authorities; and
(3) the refusal causes serious consequences, such as spread of a large amount of illegal information, serious loss of evidence for a criminal case or leakages of users' information that lead to serious results.

Whoever is guilty of this crime shall be sentenced to a fixed-term imprisonment of not more than three years, criminal detention or public surveillance and concurrently or separately fined. Where an entity[76] commits the crime, it shall be fined. The director and other responsible personnel shall also be punished.

In the above offence definition, the wording of 'security management obligations regarding information networks' caused broad discussions about the source of these obligations, but the Cybersecurity Law is without doubt considered one such source.[77] Since Article 28 of the Cybersecurity Law imposes a cooperation obligation for service providers in criminal investigations (explained in Section 17.4.1), failure to cooperate may lead to the application of Article 286-1 of the Criminal Law.

Given that security management obligations regarding information networks cover a rather wide range, Article 286-1 of the Criminal Law has been criticised for being overly broad. Scholars suggest that this legislative wording should be interpreted more strictly to avoid overcriminalisation.[78] On the other hand, in judicial practice, convictions for the crime of Article 286-1 turn out to be surprisingly rare.[79] From 2015 to 2020, there were only two criminal cases of this crime,[80] neither of which resulted in a conviction. This crime is punishable only when the service providers refuse to correct when they receive the correction order from the administrative agencies. Typically, service providers opt to correct in order to avoid possible criminal prosecution and punishment. That is why, in judicial practice, very few service providers are prosecuted.[81]

One of the most recent and remarkable cases is the *Didi* case in Yueqing City (located in Zhejiang Province), in which non-cooperation of the service provider caused a victim's death

[76] 'Entity' here refers to a company, enterprise, institution, organisation or group which commits an act endangering society that is considered a crime under the law and shall bear criminal responsibility as a whole. See, e.g., Criminal Law, Art. 30.

[77] Some experts suggest that the source could include some, but not all, administrative regulations that impose obligations on service providers, but others focus purely on the Cybersecurity Law. See, e.g., Chen Hongbing, 'On the Application Space of the Crime of Failure to Perform the Information Network Security Management Obligation' (2017) 12 *Political Science and Law* 39–42 (in Chinese); Zhou Hongbo and Yue Xiangyang, 'How the Network Security Law Relates to the Criminal Law' (2018) 6 *Journal of Capital Normal University* 49–51 (in Chinese); Yang Xinlv, 'On the Legal Interests of Refusing to Fulfil the Obligation of Information Network Security Management Crime' (2019) 6 *Northern Legal Science* 46–47 (in Chinese); Pi Yong, 'On Service Providers' Management Obligations and Criminal Responsibilities' (2017) 5 *Studies in Law and Business* 23 (in Chinese).

[78] Pi, 'On Service Providers' Management Obligations', 24.

[79] Tong Dehua and Ma Jiayang, 'Justification and Research on the Types of the Obligations in Refusing to Fulfil the Obligation of Information Network Security Management Crime' (2020) 21 *Journal of Law Application* 80 (in Chinese).

[80] Ma Chaoyang and Ren Pengbin, 'Refusing to Fulfil the Obligation of Information Network Security Management Crime: Plight in Practice, Lawful Connotation and Thoughts of Responses', in *Theory and Practice of Cyberspace Crime Governance to Optimize Criminal Procuratorial Supervision: Collected Works of the 16th National Senior Prosecutors Forum* (Beijing: China Procuratorial Press, 11 November 2020) 2 (in Chinese).

[81] Xiong Bo, 'On the Negativity of "Prior Administrative Procedure" for Criminal Liability of Network Service Providers and Its Solutions' (2019) 5 *Political Science and Law* 50 (in Chinese).

but did not constitute the crime of Article 286-1. Didi is the largest online ride-hailing platform in China. On 25 August 2018, the victim, a twenty-year-old girl, hitched a ride through Didi in the city of Yueqing. After getting into the car, she sent a text message to her friends asking for help. Her friends soon called the police. At 16:41 the police required Didi to provide more detailed information about the driver and his car twice, alleging that its security expert would intervene. Only an hour and a half later, at 18:13, did Didi send the car number and other information about the driver to the police.[82] But it was too late, the girl had already been raped and killed by the driver.

Requiring to provide information is an investigative method in criminal procedure. Failing to provide the police with the requested information in time and thus failing to fulfil its cooperation obligation in the criminal investigation, Didi was punished administratively. Soon after the *Didi* case in 2018, the Ministry of Transport, the Ministry of Public Security and related agencies in Tianjin, Zhejiang and Beijing summoned senior executives of Didi for a disciplinary interview and ordered the company to rectify the problems with its online ride-hitching services. Didi was required to fulfil its security responsibility and cooperate with the public security agencies in future criminal cases.[83] Didi's Hitch Service was suspended for 435 days, the time taken for the company to modify and improve 330 functions of its service.[84]

Since the Didi company did not refuse to make corrections, it did not commit an offence. This case clearly shows the limitations of Article 286-1 of the Criminal Law, which puts too much weight on administrative orders to make corrections. It only requires service providers to fulfil their obligations, correct illegal behaviours, eliminate adverse effects and restore property to its original condition. But obviously the right to life and health cannot always be restored.[85]

17.4.5 *Legal Remedies and Protection of Fundamental Rights*

Legal remedies and protection of fundamental rights which relate to criminal investigations, especially the collection of electronic evidence, can be found in the following areas: notification of data collection; limited usage of data obtained; application procedure of data collection and complaints against unreasonable search and seizure; exclusion of illegally obtained evidence; and state compensation for the damages caused by improper investigative measures. Some of these remedies and protections are quite successful, but others are still rather vague and their effects are limited in practice.

17.4.5.1 Notification of Data Collection

Articles 17 and 18 of the PIP Law impose general notification obligations on service providers: before processing personal information, service providers must notify individuals of, among other matters, the purposes and methods of processing of personal information, the categories of

[82] Public Security Bureau of Wenzhou City, 'A Report about the Work of Police after the Alarm Received in the Homicide Case of Didi Driver in Yueqing City', *Safe Wenzhou*, 25 August 2018, https://mp.weixin.qq.com/s?__biz=MjM5ODE2NDAzMw==&mid=2652325164&idx=1&sn=0acdb748b810c6710521cd9f43ebb67c (in Chinese).

[83] Zhao Wenjun and Qi Zhongxi, 'The Ministry of Transport, the Ministry of Public Security and Related Agencies Summoned Didi for Face-to-Face Meeting', *Xinhua News*, 26 August 2018, www.gov.cn/xinwen/2018-08/26/content_5316759.htm (in Chinese).

[84] Qin Jing and Du Gang, 'Didi's Hitch Service Coming Back to Seven Cities, Can Passengers Travel at Ease?', *Xinhua News*, 8 November 2019, http://travel.people.com.cn/n1/2019/1108/c41570-31444346.html (in Chinese).

[85] Xiong, 'On the Negativity', 55.

personal information to be processed and the retention periods, unless laws or regulations provide that such processing shall be kept confidential or that notification is not necessary.

However, there is no explicit provision on notification to suspects when the police collect data from a service provider, which often takes place without suspects' knowledge. Thus, a suspect's right to be notified about the information collection and its procedure is not guaranteed. On the contrary, in many cases the processing is kept confidential.

17.4.5.2 Limitation on the Usage of Collected Data

According to Article 152 of the CPL, investigators must promptly destroy any information and materials obtained using technical investigative measures that are irrelevant to the case. Moreover, materials obtained through technical investigative measures must be used only for the investigation, prosecution and trial of specific cases, not for any other purposes. Relevant entities and individuals must cooperate with public security agencies in their application of technical investigative measures in accordance with the law and must keep confidential all relevant information.

The Joint Provisions and the Rules MPS also require that the original storage media that have been sealed up or seized, or the frozen electronic data, must be freed within three days after they are found to be irrelevant to the particular case under investigation (Article 12 of the Joint Provisions, Articles 22 and 38 of the Rules MPS).

17.4.5.3 Data Collection Approval and Complaint Procedures

As was explained in Section 17.4.2, to protect fundamental rights, some electronic evidence collection methods that are particularly intrusive must be approved by a higher level of public security organisation.[86] Employment of technical investigative measures must be approved by public security agencies at or above the municipal level, and freezing of electronic data and seizure of email must be approved by public security agencies at or above the county level, whereas the director of the case-handling department has the power to approve requesting relevant entities and persons to provide electronic data. For other electronic data collection methods, the laws and regulations do not specifically provide the authority to approve, even though some of the methods also interfere with fundamental rights. It is important to highlight that there is no judicial warrant requirement for investigative measures (not even for the most intrusive ones) in criminal investigations in China. Therefore, the requirement to be approved by the principal of the public security organisation at the municipal or county level or above is already the highest-level protection available.

If suspects or service providers, as well as other interested parties, are of the opinion that the seal, seizure or freeze of property is irrelevant to the case at hand, or should have been terminated, they are entitled to file a petition or complaint to the police, the prosecution office or the judge, depending on which stage the case is at (Article 117 of the CPL). The organisation that accepted the petition or complaint must make a decision within thirty days and rectify the illegal sealing, seizure or freezing (Article 196 of the Provisions PSA). All aforementioned petitions and complaints apply to all kinds of property under sealing, seizure or freezing, not specifically electronic evidence.

[86] See, e.g., Jiang Yong, 'Procedural Law Turn of Electronic Investigation Regulation in China from the Perspective of Personal Information Protection' (2019) 6 *Journal of Xi'an Jiaotong University (Social Sciences)* 143–144 (in Chinese).

17.4.5.4 Exclusion of Illegally Obtained Evidence

Article 56 of the CPL establishes exclusionary rules of illegally obtained evidence. However, there is an absolute exclusion when it comes to testimonial evidence, including confessions extorted from a criminal suspect or defendant by illegal means such as torture, as well as the testimony of witnesses and statements of victims that are collected by violent means, threat or other unlawful means. The CPL does not preclude all of the illegally obtained physical or documentary evidence. Such evidence is admissible if it is not likely to cause substantial damage to due process and if the irregularity can be corrected in a reasonable way or can be justified by reasonable explanation. However, it is not clear whether the exclusionary rules can be applied to electronic evidence that is illegally collected.[87]

Even if the judge accepts that the exclusionary rules can be applied to electronic evidence, there are only a few standards to apply when examining the legitimacy of the collection of electronic evidence. The Interpretation by the Supreme People's Court Regarding the Application of the Criminal Procedure Law (ICPL)[88] provides standards to apply when examining electronic data collected in criminal procedures,[89] including: whether the collection of electronic data is performed by two or more investigators; whether the collection methods are in compliance with relevant technical standards; and whether strict approval formalities are completed (Article 112 of the ICPL). But these standards focus more on guaranteeing the authenticity of electronic data, rather than the legality of its collection.[90] When electronic data is collected without the signatures or seals of investigators, it is not admissible unless it can be reasonably explained with a rectification of signature by the holders, the providers of the electronic data or eyewitnesses on transcripts or lists. Other than this, there are no provisions concerning the admissibility of illegally obtained electronic evidence in the ICPL.

17.4.5.5 State Compensation

Article 18(1) of the Law on State Compensation[91] allows service providers whose original storage media are unlawfully sealed or seized during criminal investigations to apply for state compensation. The organisation liable for compensation is the authority in charge of the criminal investigation (Article 21 of the Law on State Compensation). To claim compensation, a service provider must first apply to the public security organisation responsible for the criminal investigation (Article 22 of the Law on State Compensation). The service provider may apply for reconsideration of the organisation's decision to the public security organisation at the next higher level or seek a decision from the compensation committee of the court (Articles 24 and 25 of the Law on State Compensation). If the original storage media can be returned or its original condition can be restored when damaged, this will be done. If the media cannot be returned to their original condition or are missing, compensation will be paid (Articles 32 and 36 of the Law on State Compensation).

87 Zhang He, 'Study on the Rules of Illegal Electronic Data Examination in Criminal Procedure' (2021) 2 *BFSU Legal Science* 57 (in Chinese).

88 Interpretation by the Supreme People's Court Regarding the Application of the Criminal Procedure Law (ICPL), 26 January 2021, www.court.gov.cn/fabu-xiangqing-286491.html (in Chinese).

89 Joint Provisions also provide the standard to examine electronic data for legitimation in Article 24, and the provision has been absorbed into Article 112 of ICPL, so here we discuss only Article 112.

90 Xie Dengke, 'On the Protection for Rights in Electronic Data Collection' (2020) 12 *Lanzhou Academic Journal* 44 (in Chinese).

91 Law on State Compensation, 26 October 2012, Art. 18(1), www.spp.gov.cn/sscx/201404/t20140424_71280.shtml (in Chinese).

17.5 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

17.5.1 *Introduction*

In 2020, during the Internet Development Forum of the World Internet Conference, the Ministry of Foreign Affairs launched the Global Initiative on Data Security,[92] relating data security and governance of data to the issue of sovereignty, national security and jurisdiction of the state. In the initiative, China calls on all states to join forces in forging a community with a shared future in cyberspace, featuring peace, security, openness, cooperation and order. Therefore, states should neither request their own domestic companies to gather data generated and obtained overseas nor obtain data located in other states through companies or individuals without the other states' permission. Instead, they should obtain overseas data through mutual legal assistance. The initiative was considered a response to the Clean Network program put forward by the Trump administration in the United States.[93]

In 2022, China submitted *Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Conventions on Countering the Use of Information and Communications Technologies for Criminal Purposes*[94] to the Ad Hoc Committee in the first session to elaborate the Convention as decided in Resolution 75/282 of the General Assembly of the United Nations in 2021. In these *Suggestions*, China reasserted its position as shown in the Global Initiative on Data Security, calling on the member states to respect the sovereignty of the state where the evidence is located, to abide by due process, to respect the legitimate rights of relevant individuals and entities and to take no invasive and destructive technical investigation means in cross-border electronic evidence collection.

Based on cyberspace sovereignty and data sovereignty, China has adopted a data localisation approach in deciding jurisdiction. Data localisation means that a state has the power to control and use electronic data stored within its territory. In Article 25 of the ICJA Law, electronic data is handled in the same manner as physical evidence. This illustrates that electronic data will be obtained similarly to physical evidence, and a territorial approach should be applied to decide its jurisdiction.[95]

On the other hand, the PIP Law draws on the experience from the EU General Data Protection Regulation[96] and, for the first time, extends its application to personal information processing activities outside the territory of China on the principle of territoriality and personality.[97] Article 3 of the PIP Law states it applies to natural personal information processing activities within the territory of China as well as those outside the territory if they are for the purpose of providing products or services to natural persons located within China, or for

[92] Ministry of Foreign Affairs, 'Global Data Security Initiative', 29 October 2020, www.mfa.gov.cn/wjb_673085/zfxxgk_674865/gknrlb/tywj/zcwj/202010/t20201029_9869292.shtml (in Chinese).

[93] Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative"', Digichina, 31 March 2022, https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/.

[94] *China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, submitted by China as a member state of the United Nations on 5 November 2021, www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

[95] See Liang Kun, 'The Mode of Jurisdiction over Criminal Evidence Collection at the National Level Based on the Data Sovereignty' (2019) 2 *Chinese Journal of Law* 200 (in Chinese).

[96] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ L 119, 4 May 2016.

[97] Xu Yunfei, 'Interpretation of the Key Points in the Personal Information Protection Law', Weixin, 24 August 2021, https://mp.weixin.qq.com/s/KHDOXKRF5TPs_7tXR2KRVg (in Chinese).

the purpose of analysing or assessing the conduct of natural persons located within. Article 53 of the PIP Law further requires that personal information processors outside the territory of China shall establish special institutions or designate representatives within the territory of China to handle affairs relating to personal information protection, including cooperation with LEAs.

17.5.2 *Mandatory Data Localisation Requirements*

To guarantee data sovereignty and territorial jurisdiction, it is required that certain operators or service providers store certain types of data domestically. For now, there are mainly three types of operators and three types of data under the domestic storage obligation, as provided in the Cybersecurity Law, the PIP Law and the Data Security Law.

First, critical information infrastructure operators[98] shall store domestically the personal information or important data that is collected or generated during domestic operations (Article 37 of the Cybersecurity Law and Article 31 of the Data Security Law). 'Domestic operations' is defined as conducting business or providing products or services in the territory of China. Those service providers that do not register in China shall nevertheless be deemed to be conducting 'domestic operations' if they use the Chinese language or use the Chinese yuan (CNY) as currency or deliver goods or services to China.[99] In contrast, Chinese service providers that conduct business with or provide products or services solely to institutes, agencies or individuals outside of the territory of China shall not be deemed to be conducting 'domestic operations'.[100] This type of data comprises only a small part of the data generated in the course of electronic commerce in China.[101]

Second, the PIP Law also provides that the personal information processors that process the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity, as well as critical information infrastructure operators, shall store domestically the personal information collected and generated within the territory of China (Article 40 of the PIP Law). Despite the aforementioned strict data localisation requirement, it is still possible for certain data collected and generated domestically to be transferred across the border. If the data is deemed to be important, its cross-border transfer shall observe measures for security management developed by the national cyberspace authority in conjunction with the relevant departments of the State Council (Article 31 of the Data Security Law). For example, automobile data processors shall store important data domestically (Article 11). In this example, important data refers to data that may endanger national security, public interests or the lawful rights and

[98] Critical information infrastructures include public communication and information services, power, traffic, water resources, finance, public service, e-government and other critical information infrastructure which, if destroyed, suffering a loss of function or experiencing leakage of data, might seriously endanger national security, national welfare, the people's livelihood or the public interest (Cybersecurity Law, Art. 31).

[99] Let's take the example of Tesla Inc, an American multinational automotive and clean energy company that sells electric cars and provides services in China. In May 2021, Tesla set up a data centre in China to localise data storage; later that year, in September, the chief executive officer of Tesla promised at the World Internet Conference Wuzhen Summit that the personal identity information of the company's Chinese clients would not be transferred abroad and that important data would be transferred abroad only after obtaining the approval of the competent authority in accordance with the Several Provisions on the Management of Automobile Data Security (see footnote 102). See, e.g., Xu Xu, 'Tesla Promises No Cross-Border Transfer of Personal Identity Information', China Economic Net, 26 September 2021, www.ce.cn/xwzx/gnsz/gdxw/202109/26/t20210926_36948364.shtml (in Chinese).

[100] Draft Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (draft for comments), 25 August 2017, Art. 3.2, www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&recode_id=23883 (in Chinese) (still has not been adopted).

[101] Zhao Haile, 'Data Localization in China's Legislation and Its Reconciliation with FTA Conclusion' (2022) 2 *Journal of International Economic Law* 30 (in Chinese).

interests of individuals or agencies when tampered with, destroyed, leaked or illegally obtained or used (Article 3).[102]

Since the provisions that require domestic storage came into force, a number of high-tech companies and multinational corporations have already reacted. For instance, since 28 February 2018, Apple Incorporated has cancelled its cross-border storage for its iCloud services and built the first data centre in Guizhou Province, and now stores all the data of Chinese users in this data centre. Additionally, Apple has cooperated with the Guizhou-Cloud Big Data Industry Development Company to provide iCloud services to users in mainland China.[103]

The domestic storage of data aims at protecting the data security of domestic users and it does help resolve some of the problems arising in the area of cross-border collection of electronic evidence.[104] On the other hand, it cannot resolve all of the problems, especially the problems of collecting data that is not covered by the requirement of domestic storage. It could also lead to an isolated information island, preventing timely and efficient collection of cross-border electronic data and development of an international mechanism for cross-border electronic data collection.[105]

17.5.3 *Cooperation of National LEAs with Foreign Service Providers*

17.5.3.1 Legal Framework

As mentioned in Section 17.5.1, China's position is that collection of data located in other states through companies or individuals must be conducted with the permission of the state where the data is located. Therefore, the formal way to collect cross-border electronic data from international service providers still lies in mutual legal assistance.

This indirect cooperation (i.e. cooperation through mutual legal assistance) has long been criticised for low efficiency and incapacity to deal with changeable electronic data. An analysis shows that indirect cooperation is also rare. Research was conducted on a sample of thirty-five criminal cases that involved foreign servers, and illustrated that not a single piece of electronic evidence in these thirty-five cases was collected through mutual legal assistance. This is because the traditional mutual legal assistance approach is complex, slow and bureaucratic. Under such a procedure, it is difficult to respond efficiently to the flow of criminal data. Twenty-nine out of the thirty-five cases included the extraction of electronic evidence from foreign servers via open websites or via entering user name and password, while the collection method of the other six cases was not explicitly mentioned in the research report.[106]

The Chinese police forces are seeking ways to promote the efficiency of traditional mutual legal assistance by simplifying the judicial assistance process and building sharing platforms for cross-border collection of criminal electronic evidence.[107] In 2019, the Office of Cooperation

[102] Several Provisions on the Management of Automobile Data Security, issued by the Cyberspace Administration, the National Development and Reform Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security and the Ministry of Transport (for Trial Implementation), No. 7, 16 August 2021, Art. 3, www.cac.gov.cn/2021-08/20/c_1631049984897667.htm (in Chinese).

[103] See Ren Xiaoyuan, 'The Apple Users' iCloud Will Move Back to Guizhou with Users' Privacy Promised by Apple', *Beijing Youth Daily*, 11 January 2018 (in Chinese).

[104] Feng Junwei, 'Development and Reflection of Cross-Border Obtaining Electronic Evidence' (2019) 6 *Law Science Magazine* 28(in Chinese).

[105] See ibid., 28.

[106] See Ye Yuanbo, 'Practical Investigation and Improvement of Cross-Border Electronic Forensics System in China' (2019) 11 *Hebei Law Science* 108 (in Chinese).

[107] Wang Zhigang and Zhang Xue, 'The Dilemma and Outlet of Cross-Border Electronic Data Forensics' (2021) 5 *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)* 51 (in Chinese).

and Coordination between China and Cambodia was founded in Phnom Penh, in which police and experts from the two countries work together and share electronic evidence collected.[108] This mechanism has proven successful in fighting crimes such as cross-border online gambling and telecom and online fraud.[109]

Apart from mutual legal assistance between countries, there also exist attempts for LEAs to seek assistance directly from foreign service providers. However, an interview with the police revealed that it is difficult for national LEAs to directly obtain electronic evidence from foreign service providers, which are frequently unwilling to cooperate.[110]

17.5.3.2 Nature of the Cooperation

In accordance with Article 9 of the ICJA Law, where the case-handling organisation needs to request a foreign country to provide mutual legal assistance, it must prepare a written request for assistance with the relevant materials attached. After being examined and approved by the competent authority[111] to which the handling authority is subordinated, this request must be filed by the foreign affairs liaison authority in China with the foreign country in a timely manner.

The 'foreign affairs liaison authority in China' mostly refers to the Ministry of Justice, as provided in most treaties,[112] while the rest of the treaties designate the National Oversight Commission, the Supreme People's Court, the Supreme People's Procuratorate or the Ministry of Public Security as the foreign affairs liaison authority in China.[113]

17.5.3.3 Legal Remedies and Protection of Human Rights

For now, notwithstanding mutual legal assistance is slow and not very efficient, it is still the most common way for cooperation between national LEAs and foreign service providers to take place, in accordance with mutual legal assistance treaties between the states involved or through diplomatic channels. The treaties fully respect foreign countries' sovereignty, and usually the gathering of evidence based on mutual legal assistance turns into a domestic issue on whether and how service providers need to cooperate with their national LEAs. In this sense, legal remedies and protection of human rights will strongly rely on the domestic laws of the service providers.

[108] Mao Pengfei, 'The Office of Cooperation and Coordination between China and Cambodia Officially Founded in Phnom Penh', Xinhua Net, 28 September 2019, www.gov.cn/xinwen/2019-09/28/content_5434513.htm.

[109] Ministry of the Public Security, 'The Sum-Up Meeting for the Year of Legal Enforcement Cooperation between China and Cambodia Held', National Immigration Administration, 4 June 2021, www.nia.gov.cn/n897453/c1415848/content.html.

[110] See Feng, 'The Collection of Internet Evidence', 37.

[111] 'Competent authority' refers to the highest rank of the case-handling organisations which enjoy investigative powers on criminal cases, namely the National Supervisory Commission, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security and some other relevant government departments (ICJA Law, Art. 6).

[112] For example, Treaty on Judicial Assistance in Civil and Criminal Matters between the People's Republic of China and the Russian Federation, signed 19 June 1992, www.mfa.gov.cn/web/ziliao_674904/tytj_674911/200804/t20080408_7948028.shtml (in Chinese); Agreement on Mutual Legal Assistance in Criminal Matters between the People's Republic of China and the United States of America, signed 19 June 2000, www.mfa.gov.cn/web/wjb_673085/zfxxgk_674865/gknrlb/tywj/tyqk/200912/t20091204_9277065.shtml (in Chinese); and Treaty on Judicial Assistance in Criminal Matters between the People's Republic of China and Australia, signed 3 April 2006, www.mfa.gov.cn/web/ziliao_674904/tytj_674911/tyfg_674913/200804/t20080408_9867450.shtml (in Chinese).

[113] Wang Aili (ed.), *The Interpretation of the Law of International Criminal Judicial Assistance of the People's Republic of China* (Beijing: Law Press China, 2019), 34 (in Chinese).

17.5.4 *Cooperation of National Service Providers with Foreign LEAs*

As mentioned in Section 17.5.2, service providers must store domestically certain data collected within the territory of China. Furthermore, direct cross-border data transfer from national service providers to foreign LEAs is prohibited.

The ICJA Law, adopted in 2018, prohibits institutions, agencies or individuals within the territory of China from providing evidentiary material and assistance prescribed by this Law to foreign countries without the approval of the competent authority of China (paragraph 3 of Article 4 of the ICJA Law). The PIP Law and the Data Security Law, both adopted in 2021, follow this position and specify that without the approval of the competent authority, a personal information processor or any domestic organisation or individual shall not provide personal information stored within the territory of China to any foreign judicial or law enforcement authority. All requests for data from a foreign judicial or law enforcement authority will be processed by the competent authority of China in accordance with the relevant laws and international treaties and agreements entered into or acceded to by China, or under the principle of equality and reciprocity (Article 41 of the PIP Law and Article 36 of the Data Security Law).

Where foreign LEAs need the cooperation of national service providers in China, they must make a request for mutual legal assistance, handing it to the foreign affairs liaison authority of China (Article 13 of the ICJA Law). The foreign affairs liaison authority will examine the written request and the attached materials, and forward them to the competent authority[114] according to the division of functions (Article 15 of the ICJA Law). The competent authority will then examine the request. Where the competent authority deems that it may assist in the execution in accordance with the provisions of this Law and the mutual legal assistance treaty, it will make a decision and proceed to execution of the request by the relevant case-handling organisation (Article 16 of the ICJA Law). When executing a request, the case-handling organisation must protect the lawful rights and interests of the parties and other relevant persons, and protect personal information (Article 17 of the ICJA Law).

As the cooperation of national service providers with foreign LEAs follows the traditional mutual legal assistance method, it encounters the same problems of slowness and low efficiency as the cooperation of foreign service providers with Chinese LEAs. Another problem has arisen for multinational service providers. In March 2018, the US enacted the CLOUD Act, compelling US-based technology companies to produce requested data regardless of whether it is stored within or outside the US. To some extent, the prohibition of national service providers from providing evidence and assistance to foreign countries as regulated in paragraph 3 of Article 4 of the ICJA Law is China's response to the CLOUD Act.[115] These laws are trapping service providers in a dilemma: when the US LEAs require US service providers that provide services within the territory of China or Chinese service providers that have branch offices in the US to provide electronic data, the service providers will have to follow the US LEAs' request or face punishment, while the Chinese Laws may prohibit them from doing so.[116]

[114] According to Article 6 of ICJA Law, the National Oversight Commission, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security and other departments are the competent authorities in charge of international criminal judicial assistance. With regard to the collection of electronic evidence, it should be the agencies with investigative powers, including the National Oversight Commission, the Ministry of Public Security and the Ministry of State Security.

[115] Hu Wenhua, 'The Impact of American CLOUD Act on China and Its Counter Measures' (2019) 7 *Information Security and Communications Privacy* 35 (in Chinese).

[116] See, e.g., Liang, 'The Mode of jurisdiction', 206.

The cooperation between Chinese LEAs and foreign service providers, on the one hand, and between foreign LEAs and Chinese service providers, on the other, depends on traditional judicial assistance between both countries. Given its low efficiency and the aforementioned dilemma, China is now reflecting on adjusting its original data localisation position and clarifying electronic data jurisdiction boundaries. In the meantime, it is trying to strengthen the dialogue mechanisms with other countries to reach bilateral and multilateral agreements on the issue of cross-border data collection.[117]

China has firmly held the opinion that it is necessary to establish a universal or global legal instrument on cybercrime within the framework of the United Nations.[118] In 2019 and 2021, the United Nations adopted Resolutions 74/247 and 75/282 to elaborate an international Convention on countering the use of information and communications technologies for criminal purposes. Supporting the elaboration on the Convention, China will 'take a constructive part in the negotiation, and work closely with all parties to jointly push for an authoritative and universal convention at an early date, so as to provide a practical and effective solution for the international community to cope with the challenges of cyber crimes'.[119]

[117] See Hu, 'The Impact of American CLOUD Act', 36; Liang Kun, 'On the Change Logic of Terrorism Development Trend and Enlightenment of EU Cross-Border Fast Electronic Evidence System' (2019) 1 *Journal of People's Public Security University of China (Social Sciences Edition)* 40–42 (in Chinese).

[118] Hu Jiansheng and Huang Zhixiong, 'The Problems and Prospects of the International Legal Regimes in Combating Cybercrimes – From the Perspective of Council of Europe's Convention on Cybercrime' (2016) 6 *Chinese Review of International Law* 22 (in Chinese).

[119] Ministry of Foreign Affairs of the People's Republic of China, 'Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on May 28, 2021', 28 May 2021, www.mfa.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202105/t20210528_9170754.html.