Vol.5 Iss.3 2024
https://doi.org/10.37420/j.mlr.2024.026
Modern Law Research

The Comparison and Conflicts of the Cross-border Criminal Data Retrieval between Europe and China

Ruoxue Ma[1*]
[1]**Law Faculty, University of Barcelona, Barcelona, Spain**
[*]**Corresponding author,E-mail: maruoxue20011225@163.com**

Abstract
With the background of the generalization of the concept of cybercrime, the high demand for cross-border data retrieval, and the poor operation of the traditional cross-border electronic evidence collection system, China and Europe changed the system of cross-border data retrieval. Currently, the forensic models of the two have institutional similarities, but they are fundamentally different. Besides, the European model conflicts with China's exit data protection rules such as the Data Security Law and the Personal Information Protection Law, and Chinese companies are facing a data compliance dilemma as a result. For this reason, this paper intends to adopt the research method of normative research and comparative research to explore the fundamental reasons for the existence of legal conflicts by combing and comparing the cross-border data retrieval legislation and practices of China and Europe, and to analyze the impacts of the two different forensic modes on the data compliance of Chinese enterprises. This paper suggests that enterprises build a dynamic compliance management system with full process coverage, and construct a long-term strategy for compliance-oriented to specific issues.

Keywords
Data retrieval, Electronic criminal evidence, Forensic, Corporate Compliance

1 Introduction

While facilitating human daily lives, digital and Internet technologies are also being utilized by criminals to evade law enforcement activities. In this context, cybercrime no longer refers only to crimes committed against electronic information systems and crimes that disrupt network business activities and disorderly conduct on the Internet. More and more traditional crimes are also gradually characterized by the use of electronic information system technology, such as fraud, dissemination of pornographic material and terrorist activities. It makes law enforcement and juridical for such crimes increasingly dependent on data retrieval when collecting evidence.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

The fact that traditional international mutual legal assistance in criminal matters could no longer meet the practical demands of the efficient fight against criminality, which had triggered a worldwide legal revolution in the data retrieval model. For example, China has begun legislative attempts to implement new forensic measures since 2016 under the basic view of data security, cybersecurity and data sovereignty. Regrettably, these new rules are low-ranking and fragmented and this makes their application confusing. By contrast, Europe already established the cross-border data retrieval rules earlier, such as the Second Additional Protocol to the Cybercrime Convention on enhanced cooperation and disclosure of electronic evidence (Protocol II) introduced by the Council of Europe, as well as a regulation about European Production and Preservation Orders introduced by the European Union (EU).

This legal evolution, or the source of this legal change, includes not only the dramatic impact of advances in technology but also the clash of cultures. It seems to serve as an example of a simultaneous refutation of both evolutionary and diffusionist theories [8]. In this evolution, China and Europe both have large data markets, while the United States (US) controls most of the large corporations. The legal developments in China and Europe are clearly colored by a response to the US Cloud Act, but at the same time adhere to their unique positions. Therefore, this paper focuses on China and Europe and expects to summarize the different strategies adopted by them in the face of similar dilemmas and analyze the reasons for the differences through a comparative study of their legislation of data retrieval, especially by conducting more micro-comparisons. In addition, this paper expects to carry out some macro-comparative analyses to analyze the characteristics of them as well as their advantages. Ultimately, this paper will explore the reasons for the emergence of auxiliary law conflicts and the impact on enterprises through these comparisons, and put forward recommendations for business.

2 Overview of the Cross-Border Criminal Data Retrieval System in China

Currently, in China, four main models of cross-border criminal data retrieval system exist in judicial practice, which include international mutual legal assistance (MLA) in criminal matters, the direct collection of evidence by investigating authorities on their own initiative, bilateral or multilateral cooperation, and the retrieval of data by competent authorities from service providers aboard or from the third party. The first two can be found separately in Chapter 4 of the Law on International Mutual Legal Assistance in Criminal Matters (LIMLACM) and Article 9 of the Provisions on Several Issues Concerning the Collection, Extraction, Examination and Judgement of Electronic Data in Handling Criminal Cases (hereinafter referred to as the Provisions 2016). bilateral or multilateral cooperation is also mostly based on bilateral or multilateral agreements and treaties signed with other entities. However, the taking of data from the third party has not yet been formally established by legislation. Furthermore, the traditional way of criminal data retrieval as well as direct collection of evidence by investigating authorities on their own initiative in the operation of the system also have more or less problems.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

2.1 Limited Application of Traditional Legal Assistance in Criminal Matters

China's domestic legal basis for cross-border criminal data retrieval through international mutual legal assistance in criminal matters is mainly the LIMLACM. According to the LIMLACM, countries with which China has signed treaties on mutual legal assistance in criminal matters may carry out cross-border forensics following the procedures stipulated in the treaties. Until now, China has signed bilateral treaties on mutual legal assistance in criminal matters with 58 countries. [*]Generally, in China, the construction of the international criminal MLA system, which is mainly used to combat traditional crimes, has become increasingly mature. The MLA system can achieve the goal of realizing legal assistance on the basis of respect for the sovereignty of other countries without relying on diplomacy. However, with the development of technology, it has become more and more difficult to determine the location and attribution of data in cyberspace, with the generation of the cybercrime concept, the reduction of the cost of crime, the more complex relationship between the location of crime subject, the place of crime commission and the place of harmful result occurrence. All these problems cause the application of the traditional system of MLA in criminal matters under cross-border data retrieval limited.

Firstly, the traditional system of international MLA in criminal matters is time-consuming and inefficient. It adopts an "inverted U-shaped" structure. Taking the procedures stipulated in China's LIMLACM as an example. From the time that a request is made by a Chinese law enforcement agency to the reception by the requested State, a total of four procedures need to be followed: according to article 25 of LIMLACM, when requesting a foreign State to conduct an investigation and obtain evidence, a) the authorities in charge of the case should make a request and submit the request and related materials to the competent authorities for examination; b) the competent authorities give the consent and the authorities in charge of the external contact request the foreign State; c) the request reaches the requested country, the competent authorities of receptor also examine the request; d) after passing the examination, the law enforcement agency of receptor executes the request. For example, in the case of making a request to US, the process takes an average of 10 months, and that 10 months does not include the time between the execution of the request by the US law enforcement agency and the eventual receipt of the required data by the law enforcement agency of the requesting country [17]. Besides, data are easy to modify and delete, which makes it difficult to ensure the integrity of their preservation during the lengthy examination process. In general, the longer the request period demands, the more difficult it is to locate and collect the required data. It can be seen that the traditional "inverted U-shaped" international criminal MLA procedure is not only complex and inefficient, but may also greatly reduce the effectiveness of evidence due to its excessively time-consuming character.

Secondly, not all criminal data retrieval demands can be met through the international criminal MLA process. The prerequisite for the application of the international criminal MLA system is the ability to determine the storage location of the required data, and only by determining the storage location of the required evidence can it be determined to whom the request for evidence should be addressed. The application of cloud computing, blockchain, darknet, deepnet and other technologies makes the storage location of data

* Data Source: People's Republic of China - Treaty Database. Available online: http://treaty.mfa.gov.cn/Treaty/web/list.jsp (Accessed on 5 January 2024).

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

uncertain. The distributed storage method of cloud computing and blockchain decentralized distributed storage and anonymity will scatter the data in different geographic locations for storage, and even the user itself or the service provider cannot determine where those data are located. While the first two may be able to identify the internet service provider (ISP), the highly covert, encrypted and anonymous nature of the darknet and deepnet makes it quite difficult for law enforcement agencies to locate the data, let alone trace it back to the desired data after a lengthy examination process.

2.2 The Construction of the Direct Collection of Evidence by Investigating Authorities on Their Own Initiative and the Emergence of New Problems

In earlier years, China realized that traditional international criminal MLA could not satisfy the needs of law enforcement authorities for cross-border data retrieval. As early as 2005, Rules for the Investigation of Computer Crime Scenes and the Examination of Electronic Evidence published by the Ministry of Public Security proposed, for the first time, forensic measures that could be carried out through the network on remote target systems by article 3, and stipulated procedural matters for the implementation of remote investigation. Then Provisions 2016 directly clarified that data stored outside the country can be obtained by online extraction through online remote inspections: online remote inspections can be carried out when necessary to further ascertain the situation, and the process of investigation requires the adoption of technical investigation to be subject to strict authorization procedures. In 2019, Rules for Public Security Organs to Handle Electronic Data Forensics in Criminal Cases (Rules 2019) further stipulates 6 applicable circumstances for online remote inspection.

As mentioned above, Chinese law explicitly provides for a total of three methods for direct collection of evidence by investigative authorities on their own initiative, which includes online extraction, online remote inspections and remote technical investigation, and the taking of such activities does not require the consent of the competent authorities of the country in which the data are located. Online extraction mainly focuses on the extraction of electronic data from web pages, online videos and files on online disks, i.e., downloading files from the Internet [10]. Online remote inspections focus on inspecting computer information systems located abroad through the Internet, searching for and extracting crime-related electronic data stored in the system and recording the status of the computer system, thereby providing clues for the investigation of cases [11]. Remote technical investigation requires the use of specialized software or technical means to break through computer security barriers and enter the system for forensics, or implant software to monitor and extract data in real time [15]. Although Chinese rules provide detailed procedures for the use of the forensic measures described above, but fail to specify the scope of scenarios to which it applies or the types of data that can be involved.

While these three data retrieval measures have enhanced the ability of Chinese investigative authorities to obtain evidence, they have also breached the boundaries of law enforcement jurisdiction of other countries. Criminal evidence-gathering jurisdiction is a subordinate concept to criminal law enforcement jurisdiction, which has strong territorial limitations, and the foregoing evidence-gathering measures are undoubtedly an evasion or breach of the boundaries of criminal law enforcement jurisdiction [7]. Unless the investigators are extracting publicly accessible data from the territory of another State, because such forensic acts are

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

arbitrary investigative acts and do not involve infringement of the sovereignty of another State [9]. Therefore, in principle, the consent of the country located the data should be obtained for cross-border criminal forensic acts which are related to the sovereignty of other countries. Even though the provisions of Chinese law provide a clear basis in domestic law for investigative organs to implement the above-mentioned investigative measures, in the absence of the necessary theoretical or international rules to support them, the collection of electronic data stored in non-public cyberspace and located abroad carries the possibility of infringing on the sovereignty of other States and triggering international disputes.

2.3 Judicial Practice Breaks with Legislation: Limiting the Effectiveness of Taking Data from the Third Party Abroad

Taking data from the third party mainly refers to taking directly or requesting assistance in data retrieval from ISPs or individuals who control or possess the required data. Compared with law enforcement authorities, ISPs have technical advantages and data resource advantages, and investigating authorities are also happy to request third parties to take evidence on their behalf or with their assistance. The high efficiency and convenience of obtaining evidence by this way make it common in judicial practice, especially for domestic forensics. Provisions 2016 gives law enforcement agencies the power to collect and retrieve data from third parties, and provides for the third party the cooperation duty with the data retrieval. However, it does not specify whether law enforcement authorities may retrieve data from third parties located abroad.

The reason why China has not yet explicitly the authorities could collect data from the third party abroad is that such forensic method faces many obstacles in theory and practice. First, similar to the direct collection of data by investigating authorities on their own initiative, explicitly providing for the taking of evidence from third parties abroad in the legislation is an expansion of law enforcement jurisdiction, which also would cause a conflict of sovereignty. Second, Chinese law definitely has the right to attach an obligation to cooperate with law enforcement measures to ISPs and individuals in China, but not ipso facto enjoys the right to regulate ISPs and individuals abroad. Those ISP and individuals are entirely voluntary to provide the data under their control. Lastly, even if Chinese law provides a basis in domestic law for the application of the measure of taking data from the third party, this measure may still be in conflict with other countries' data access, data collection, data collection, data collection, data access and data collection. Finally, even if Chinese law provides a domestic legal basis for the application of evidence collection from third parties, the regulation may conflict with prohibitions or restrictions on data access or acquisition in other countries. In other words, its true effectiveness of this method of evidence collection is uncertain. Taking ISPs of the US as an example, as shown in Tables 1 and 2, in 2021 the rate of responding to the requests for customer data access from the Chinese government to Apple achieved 92%; whereas in the first half of 2022, China filed a total of 13 law enforcement requests to Microsoft, but all of them were denied with the reason of that the requests fail to comply with US legal requirements.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Table 1. Microsoft H1 2022 Law Enforcement Request Report (excerpt).[*]

Law Enforcement Requests Report 2022										
	Total Requests		Some Customer Data Disclosed				No Customer Data Disclosed			
	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests	Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)	
	#	#	%	#	%	#	%	#	%	#
China	13	0	0.00%	0	0.00%	0	0.00%	0	100.00%	13

Table 2. Apple 2021 Government Data Access Requests in Mainland China [**]

China Mainland 2021 Government Requirement for Customer Data					
Request Type	Device	Financial Identifier	Account	Emergency	
Number of Requests	2628	456	122	0	2862
Number of responses	2456	213	93	0	2637
Rate of responses	94%	71%	76%	-	92%

Overall, the practical effect of taking data from the third party in judicial practice often depends on the third party itself. If ISPs can provide standards for cross-border data retrieval and review electronic evidence according to the law before taking actions, it will not only enable ISPs to avoid penalties arising from legal conflicts, but also could maximize the need to assist in judicial law enforcement and the fight against crime.

* Data Source: Microsoft Law Enforcement Request Report. Available online: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (accessed on 4 December 2023).

** Data Source: Apple Transparency Report for Mainland China. Available online: https://www.apple.com/legal/transparency/cn.html (Accessed on 21 April 2023).

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

3 Overview of the European Regime for Cross-border Criminal Data Retrieval

3.1 International MLA System in Criminal Matters Represented by the Protocol II

The Convention on Cybercrime (Budapest Convention), signed by 26 member States of the Council of Europe and 30 other countries, including the US, Canada, Japan and South Africa, is the world's first international convention to address cybercrime. Different from its Additional Protocol I, the Protocol II focuses on procedural matters, mainly related to MLA among member States for criminal justice purposes and issues related to the disclosure of electronic data, in order to address the limitations of traditional assistance mechanisms, strengthen international cooperation in terms of both depth and breadth, and build a new order for combating cybercrime.

The Protocol II mainly stimulates procedures for direct cooperation with providers and entities in the territory of another party, procedures for international cooperation between authorities about data disclosure, mutual assistance in emergencies, procedures for international cooperation without an applicable international agreement, and conditions and guarantees for the functioning of these procedures. According to article 2 of the Protocol II, the Protocol applies to criminal offences relating to computer systems and data, as well as to offences of racist and xenophobic acts committed through computer systems, as established in Protocol I.

Among the aforementioned data retrieval measures, international cooperation between official agencies of the two Parties on data disclosure, mutual assistance in emergencies and international cooperation without applicable international agreements are essentially optimizations and improvements of the forensic regime of international MLA in criminal matters. The most noteworthy data retrieval measures regulated in the Protocol II is the direct cooperation between the authorities of one Party and the providers or entities of another party, which contains legal provisions for direct data disclosure with a strong unilateral dimension. Article 7, paragraph 8, of the Protocol II allows States parties to set the highest applicable priority for this mode of data retrieval. It authorizes the judiciary to order the disclosure of user information stored in the territory of another Party directly from its ISPs before seeking cooperation with its authorities, in the absence of reasonable grounds of the ordering party. The user information consists mainly of the registrant's details and its Internet Protocol address (IP address). This forensic measure is designed to provide a faster way for the judiciary to access data stored abroad directly.

3.2 Improvements and Innovations with the European Production and Preservation Order

On April 17, 2018, the European Commission formally launched the (Draft) Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (EU E-evidence Regulation) with a consensual text in early 2023. Specifically, the European Production Orders (EPO) and the European Preservation Orders (EPO) constitute the two core regimes of the EU E-evidence Regulation. The regulation

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

also provides for defenses and legal consequences for refusal to comply with relevant judicial orders. The main function of the Regulation is to facilitate easy and efficient cross-border data retrieval among European countries, among EU Member States and between Member States and third countries outside the EU. In terms of the institutional tenor, the draft intends to shift the voluntary disclosure of data by ISPs to mandatory operation at the legal level through legislation. At the same time, this shift is also a response to the impact of the kind of design such as "long-arm jurisdiction" in the US Cloud Act.

3.2.1 The European Production Orders

The European Production Orders are essentially judicial decisions issued by a judicial authority of an EU Member State for the purpose of accessing data, which will be directly enforced by an ISP. According to its design, the judicial authorities of the EU Member States can compel the provision of electronic data by ISPs operating in the EU. The ISPs must respond in accordance with the directive whether the data is actually stored inside the EU or not. The data subject to the European Production Orders includes, in particular, textual content, messages, e-mails and information identifying suspected criminals. In order to ensure its fast functioning, ISPs are required to respond within 10 days, and in the event of an emergency, the corresponding response time is reduced to no more than six hours [5]. The response time requirement of the European Production Orders in terms of is obviously stricter than the 120-day response time of the previous European Investigation Order. It will undoubtedly accelerate the response time for cross-border data retrieval and greatly enhance the efficiency of the fight against cybercrime.

3.2.2 The European Preservation Order

The European Preservation Order is a judicial decision issued by the judicial authorities of the EU Member States in criminal proceedings, following an assessment of individual cases in accordance with the principles of proportionality and necessity. The judicial authorities of the EU Member States may compel ISPs in the EU to store certain electronic data, so that the corresponding data can be subsequently accessed through legal procedures such as MLA procedures, European Investigation Orders, European data submission orders, etc. Similarly to the European Production Orders, the European Preservation Order is only for offences that have actually been committed and requires ISPs to retain data generated before the time node that issued the order, and has no legal effect on data generated at a future time after the receipt of the order.

4 Comparison of Institutional Improvement Programs in China and Europe

4.1 Common Land for Data Retrieval Regimen in China and Europe

In general, both China and Europe have begun to improve their systems after recognizing the limitations of the traditional international MLA procedure in criminal matters as an evidence-gathering measure in judicial practice. On the one hand, they have optimized the MLA procedure itself, while on the other hand, both of them are attempting to develop other more efficient and applicable measures.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

First, both have attempted to optimize the forensic measure MLA itself to some extent. For Europe, Article 8 of Protocol II to the Budapest Convention sets a time limit for the requested party to serve a request to an ISP and for the service provider to return the results. Article 9 establishes a 24/7 network point of contact in case of an emergency and Article 10 regulates the procedure for 24/7 emergency mutual assistance. Articles 11 and 12 supplement the possibility of taking evidence through videoconferencing and joint investigations in the absence of an international agreement; although both measures slightly diminish the probative value of the evidence. Articles 11 and 12 add the possibility of discovery through videoconferencing and joint investigations without any applicable international agreement, although both measures slightly diminish the probative value of the evidence. For China, the LIMLACM was enacted late, passed in 2018, and there is no amendments have been made to it. However, there is almost a consensus in the academic discussion that the current MLA procedures need to be optimized, and various scholars are exploring optimization options. For example, Wang proposed three options to simplify procedures and improve efficiency: legalizing direct cooperation between domestic and foreign law enforcers, dispatching officers to investigate and collect evidence, and establishing a case-by-case e-discovery assistance mechanism [12]. Feng proposed that different MLA evidence should be differentiated and promoted a "three-level" judgment method that shall be applied in order to improve the admissibility of the evidence obtained [2].

Secondly, both sides have created more efficient and broadly applicable new direct evidence collection by investigative authorities in addition to the traditional data retrieval measures, which have been specifically analyzed in the previous two chapters. China has provided for the direct collection of evidence by investigating authorities on their own initiative in its legislation. For Europe, Protocol II to the Budapest Convention introduced the spillover effect of direct cooperation between the authorities of one State and the providers or entities of the other Party. The subsequent European Production Orders and the European Preservation Orders further strengthened and consolidated the implementation of the same type of collection of evidence measures.

4.2 Differences of Data Retrieval Regimen between China and Europe

Although, from the perspective of the classification of data retrieval measures, those measures taken by China and Europe in judicial practice appeared to be relatively similar, with criminal judicial assistance, taking of data from the third party that includes ISPs or individuals, and direct access to data by the investigating authorities. However, whether in terms of the overall pattern or the details, the difference in the design of the two systems of data retrieval is quite obvious.

First, just from the perspective of legislative techniques, the relevant rules in China are more fragmented than those in Europe. China's provisions on evidentiary measures are dispersed in laws, legislative interpretations and departmental regulations of different levels, while the European rules are more centralized. This has already created problems for businesses to fully understand the rules in order to cooperate with enforcement investigations.

Second, they have distinct jurisdictional models. Generally, the jurisdictional model of cross-border data retrieval can be categorized into the model of data storage location and the model of data controllers [4].

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

The model of data storage location implies that a state's jurisdiction for criminal forensics is based on the physical location where the data is actually stored, similar to territorial jurisdiction in criminal law. The model of data controllers refers to obtaining access to data under the control of an ISP by seeking its cooperation or issuing instructions to it. That is, under the model of data storage location, a state has undisputed criminal forensic jurisdiction over data stored in electronic media located in its territory, but the procedure for accessing data stored outside its territory needs to be legal. Under the model of data controllers, the data controller becomes the medium for law enforcement agencies to access data, breaking through the jurisdictional limitation of the physical location of data storage; whether it is through foreign ISPs without a local physical presence or foreign ISPs with a physical presence to obtain data outside of the country belongs to this model. Thus, according to the previous analysis, Europe has provided for a large number of forensic measures relying on ISPs, which is typical of the model of data controllers. While the design of China's data retrieval system is more conservative, and although the judicial practice breaks through the system design, it is more in favor of the model of the place of data storage in general.

Finally, Europe has established more additional procedural safeguards measures. For example, Article 14 of Protocol II to the Budapest Convention provides for a total of 15 safeguards on scope of application, purpose and use, data accuracy and integrity, safeguards for the processing of sensitive data, retention periods for personal data, automated processing, prevention and handling of security incidents, record-keeping, data sharing and transfer, transparency and notification, data access and rectification, remedies, supervisory authorities and functions, and consultations on non-compliance. The European Production Orders and Preservation Orders also stipulate the corresponding scope of application and set up a defense procedure for ISPs. If an ISP finds that it is unable to comply with the relevant order, it may activate the response communication mechanism as required. ISP shall give a full explanation of the circumstances under which it is unable to comply with the order, then the order-issuing authority will decide whether or not to withdraw the order after assessing its explanation. However, China's provisions on evidentiary measures other than international criminal MLA are quite rough, lacking detailed provisions on the scope of application and clear safeguards for legal rights such as personal privacy and data security, which is also a major problem often criticized by domestic scholars [2].

4.3 Reasons for Different Data Retrieval Models in China and Europe: Chinese View of Data Sovereignty

Overall, the pattern of data retrieval adopted by China is quite conservative, while in details, the design of the relevant legal system in China is quite rough, and this is widely recognized. However, China has so far not made any institutional changes or faced huge difficulty in making changes, mainly because of its fundamental position of data sovereignty. The concept of cyberspace sovereignty and data sovereignty has been mentioned many times not only in laws but also in some national policies. To summarize, China has always adhered to the basic idea of data sovereignty, and based on this view of sovereignty, China basically upholds the position of the data storage place model for cross-border data retrieval. However, the forensic measures stipulated in China's current legislation are obviously contradictory to this basic position. Therefore, how to carry out institutional reforms on the basis of not violating data sovereignty and designing

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

more efficient and more widely applicable forensic measures is the primary issue at present. However, this issue has not yet been resolved, and as a result, China's relevant institutional reform legislation has stagnated, remaining only at the stage of theoretical discussion.

5 Path for Corporate Compliance under the Perspective of Cross-border Data Retrieval

Although the taking of evidence from third parties has not yet been incorporated into the legislation in China, it has been widely used around the world. Under these complex and numerous data access rules, enterprises are often most likely to be involved in the vortex of legal conflicts, and become the "dilemmas in the cracks". In this context, data compliance is not only a social responsibility and legal obligation for enterprises, but also a safeguard measure to enhance their core competitiveness, reduce their cross-border business risks, and prevent them from being penalized for non-compliance as much as possible [1].

5.1 The Impact of the European Data Retrieval Model on the Corporate Compliance in China

Both Protocol II to the Budapest Convention and the draft EU E-evidence Regulation has established measures to obtain evidence from network service providers with extraterritorial spillover benefits, regardless of where the data is stored. However, the essence of taking evidence from ISP is to hand over the work of taking evidence to data controllers, and does not essentially resolve the conflict of laws, while the governance of cyberspace inherently involves a variety of legal relationships and legal roles, and Chinese ISPs are bound to face a variety of dilemmas if they want to achieve compliance under these conflicting rules [6].

A.Corporations become the real bearers of the consequences of legal conflicts.

In order to cope with the revolution of "expansive" data retrieval mode outside China to safeguard data security and even national security, on the basis of the provision of localized data storage, Article 36 of China's Data Security Law (DSL) and Article 41 of the Personal Information Protection Law (PIPL) also restrict the data outbound transfer for the purpose of assisting in the administration of justice and law enforcement, i.e., data stored in China shall not be disclosed outbound unless approved by the competent authorities of China. Data stored in China may not be disclosed outside China without the approval of the competent authorities. Therefore, Chinese companies that transfer data outboard without approval are bound to be penalized by Chinese regulators, but they still face the risk of enforcement or penalties if they refuse to provide required data to foreign judicial and law enforcement agencies on this basis. In addition to conflicting with data outbound transfer restrictions, the cross-border data retrieval model may also conflict with China's personal information protection rules. As a result, the original gaming of the forensic system among states is finally assumed by enterprises, which brings considerable difficulty to the data compliance of Chinese corporations.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

B.High compliance costs for enterprises

At present, some data regulations in China are not yet fully operational, which makes it necessary for enterprises to figure out how to manage data compliance on their own. In addition, compliance management of the data processed is inherently costly for enterprises on top of their normal operations, and is a significant investment in terms of technology, personnel and time. Some of them may also need to set up additional data storage centers inside the territories of countries where they operate in order to comply with localized data storage requirements. In addition, the aforementioned risk of penalties for conflict of laws can also be factored into the cost of compliance. These data compliance costs are not inputs that can be directly converted into revenues. In this case, especially for SMEs, some of the compliance costs can be unaffordable.

5.2 Creating a Dynamic Compliance Management System for the Entire Process

From the current situation, strengthening data regulation is bound to become the future regulatory trend. With the continuous introduction of various subordinate laws and the frequent joint enforcement actions of various regulatory authorities, enterprises also have recognized the importance and necessity of accelerating the construction of compliance management. In order to improve their risk response capability and maximize the effect of compliance construction, enterprises should take the initiative to build a full-process, targeted and dynamic compliance management system. Although data compliance construction will inevitably lead to an increase in operating costs, enterprises should also note the social and economic benefits of active compliance [16].

First, from the perspective of cross-border data retrieval, data compliance management should not be limited to the prior risk prevention stage, risk assessment in actions and posterior risk response are equally important with the prior risk prevention. For example, the International Organization for Standardization developed the ISO series of standards that adopts Deming Cycle (also known as PDCA Cycle) management concepts, to provide the compliance management program with a set of pre-programming (Plan), implementation (Do), post-checking (Check) and summarize or deal with the results (Action). This dynamic and comprehensive management program is not only applicable to the regular compliance management of enterprises, but also applicable to specific issues and business scenarios, and can also improve the fault tolerance and correction mechanism of compliance.

Secondly, enterprises should implement the data localization required by law, strengthen the management of data classification and grading, and make timely declarations on data outbound transfer reviews. In order to cope with the expansion of cross-border data retrieval rules in other countries and to ensure the cybersecurity and data security of China, China's legislation attaches considerable importance to data classification and grading management, and requires the l localization of certain data, establishes a system of data security assessment and review, and even prohibits the exit of some types of data from the country. In this case, especially critical infrastructure operators and special industry operators, such as enterprises in the fields of finance, insurance, medical care, and automobiles, should localize key data, personal information, and other data locally under the guidance of laws, regulations and standards within the scope of each field. Be-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

sides, they may even divide a product into two versions, one for the domestic and one for the offshore, after comprehensively considering the cost, risk, and other factors [3]. Also, it is recommended that enterprises begin to take measures to assess their own business and manage data classification from the perspectives of importance, sensitivity, confidentiality and availability for the purpose of data classification, with particular emphasis on the storage and protection of key data, national core data and personal information. Finally, before assisting in foreign judicial and law enforcement agencies and disclosing data outbound, enterprises should conduct security self-assessments, take the initiative to declare to the authorities and provide data outbound only after they have passed the security review.

5.3 Establish a Long-term, Decisive Compliance Strategy

First, under the current framework of cross-border data retrieval rules, whether from the perspective of cost or workload, data compliance for enterprises is inevitably a long-term regulatory task. Therefore, it is recommended that corporates take into account the cost of corporate compliance as well as the direction and goals of development at this stage, establish a long-term compliance strategy oriented to specific issues, and gradually complete the data compliance work in phases. For SMEs that can hardly afford high costs, they can only perform necessary, low-level compliance work after considering the target orientation of the enterprise, and gradually raise the level of data compliance management in the course of their development.

Second, pay attention to domestic and overseas legislation and law enforcement developments, and constantly update and adjust the compliance management system according to the characteristics of the industry. Currently, we are still in the peak period of legislation and amendment of data regulation around the world, and after the United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (UN Convention against Cybercrime) is formally introduced, China's legislation will certainly be adjusted. In addition, in the past two years, more operational new regulations and industry-specific regulations have been introduced almost every year. The EU also continues to introduce new legislation on cross-border data transfer. Therefore, it is recommended that enterprises continue to pay attention to the relevant legislation and regulatory developments at home and abroad, and adjust their compliance strategies in accordance with the changes in the system and the regulatory developments in the industry. Enterprises can also participate in the rule-making process through various means, so that they can fully understand the background, purpose and value orientation of each rule, but also can provide feedback from the perspective of their own interests [16].

Third, give full play to the leading and autonomous role of industry associations. The research, development and construction of a complete compliance management system, without the assistance of others such as government or large-scale enterprises, will inevitably consume a lot of effort and material and financial resources of enterprises. While the Chinese enterprise group is still dominated by SMEs [13]. They may not be able to bear the relevant costs, nor have sufficient reserves of professional talents. In this case, it is more feasible to rely on the resources and expertise of industry associations to assist enterprises in compliance building.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Industry associations can become standard-setters, and can first work with large enterprises to discuss and practice the optimal solution for data compliance management, in order to introduce industry uniform standards such as the compatibility board and data classification and grading guidelines that are more in line with the current situation of the industry. In addition, some scholars have proposed that industry associations can replace enterprises to build standardized application data access assistance templates, and become the medium of data access application between investigating authorities and enterprises as a rule controller and norm enforcer. The assistance template needs to clarify the reason for access, practice, content of access, applicable scenarios, list of evidence, confidentiality and other contents [14].

6 Conclusions

In comparison, China and Europe have expanded the same types of data retrieval actions on the basis of traditional measures, but in details, Europe has contributed more effort to procedural safeguards and human rights protection. Overall, the two are fundamentally different in their ideas for improvement, choosing different jurisdictional models and holding different views on data sovereignty. As a result, the European forensic model conflicts with the Chinese view of data sovereignty and corresponding protection legal standards, and it has become a challenge for enterprises to complete the construction of data compliance under many standards.

To solve this problem, this paper suggests that enterprises take the initiative to build a whole-process, specific and dynamic compliance management system, carry out data classification and grading management and data outbound transfer declaration in accordance with the law, and rely on industry associations to carry out standard setting and supervision within the industry. However, in any case, due to the existence of the sovereignty issue, these initiatives cannot fundamentally resolve the institutional dilemma, and it is hoped that the draft of the UN Convention against Cybercrime may provide some substantial help in resolving this problem in the future.

Reference

[1] Chen, B. (2023). Legalization of Compliance Governance in Cross-border Data Flow of Digital Enterprises. Research on Rule of Law, 02, 34-44.

[2] Feng, J. (2017). Review of the Admissibility of Evidence Obtained through Mutual Legal Assistance in Criminal Matters: Principles and Methods. Criminal Science, 06, 68-84.

[3] Hong, Y. (2021). Cross-border Access to Data for Law Enforcement Purposes in the Context of Conflicts of Laws: Case Studies on the U.S., EU and China. Global Law Review, 43(01), 38-51.

[4] Liang, K. (2019a). Data Sovereignty-based Mode of National Jurisdiction over the Collection of Criminal Evidence. Chinese Journal of Law, 41(02), 188-208.

[5] Liang, K. (2019b). Development Trends of the EU's Cross-Border Rapid E-Discovery Regime and its Implications. Journal of People's Public Security University of China (Social Sciences Edition), 35(01), 33-43.

[6] Pei, W. (2021a). Access to Data from Internet Service Providers: The Origins, Obstacles and Construc-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

tion of the New Model of Cross-Border Digital Investigation. Hebei Law Science, 39(04), 56-81.
[7] Pei, W. (2021b). The Enforcement Jurisdiction in Cross-Border Obtainment of Evidence against Cybercrimes. Journal of Comparative Law, 06, 30-45.
[8] Somma, A. (2015). Introducción al Derecho comparado. Universidad Carlos III de Madrid.
[9] Tang, B. (2020). Research on Cross-border Data Collection in Criminal Justice. The Jurist, 2020(04), 156-170+196.
[10] Wan, C., Wang, J., Wu, M., & Gao, Y. (2016). Understanding and Application of the Provisions on Several Issues Concerning the Collection, Extraction and Examination and Judgement of Electronic Data in Handling Criminal Cases. Prosecutorial research and mentoring, 06, 1-22.
[11] Wan, C., Wang, J., Wu, M., & Gao, Y. (2017). Understanding and Application of the Provisions on Several Issues Concerning the Collection, Extraction and Examination and Judgement of Electronic Data in Handling Criminal Cases. People's Procuratorial Semimonthly, 01, 1-22.
[12] Wang, L. (2020). The Construction of Summary Procedure of Judicial Assistance of Cross Border Electronic Evidence. Law Science Magazine, 41(03), 82-92.
[13] Wang, Z. (2022). The Number of Micro, Small and Medium-sized Enterprises in the Country Reached 48 million. People's Daily, 010.
[13] Yao, H. (2023). Analysis of the Dilemma of Network Service Providers in Cross-border Electronic Forensics—Taking the Chinese Bank Case as an Example. Journal of Hebei Vocational College of Public Security Police, 23(01), 17-21.
[14] Ye, Y. (2020). Building An Electronic Forensics System of Cross-Border Diversified. Journal of People's Public Security University of China (Social Sciences Edition), 36(4), 48-58.
[15] Zheng, Z. (2021). Spotlight on Cross-border Data Disclosure and National Security Reviews. China Forex, 16, 11-13.
[16] A New UK – US Data Sharing Agreement: A Tremendous Opportunity, If Done Right. Available online: https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/ (accessed on 8 January 2024).

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)