RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0028

Cross-border Data Transfer Regulation in China

Yuan Li

With the growing participation of emerging countries in the global data governance, the traditional legislative paradigm dominated by the European Union and the United States is constantly being disintegrated and reshaped. It is of particular importance for China to establish the regulatory framework of cross-border data transfer, for not only it involves the rights of Chinese citizens and entities, but also the cyber sovereignty and national security, as well as the framing of global cyberspace rules. China keeps leveraging the data sovereignty to fasten the law-makings to support the development of critical technology in digital domains and infrastructure construction. This paper aims to systematise Chinese regulations for cross-border data exchange following the chronological order. The enacted and draft provisions as well as binding and non-binding regulatory rules are studied, and various positive dynamic developments in the framing of China's cross-border data regulation are shown. Despite certain limitations, the Cybersecurity Law, together with Civil Code and Personal Information Protection Law, demonstrates great willingness towards a stronger data protection regime and more flexible regulatory mechanism.

China – Cross-border data flow – Cybersecurity

Sommario: *1. Introduction – 1.1. Global Data Transfer – 1.2. Problem Statement – 2. The Evolution of China's Personal Data Protection Laws – 2.1. Cybersecurity Law – 2.2. Enforcement and Authorities – 3. Data Export Regulations – 3.1. Critical Information Infrastructure Data Export – 3.2. Personal Information Export – 4. Conclusion*

1. Introduction

The regulation of cross-border data transfers represents one of the greatest challenges that data protection experts and legislators are facing around the world[1]. The global data protection law regime is fragmented by the divergence among various data protection standards. The potential negative effects shall not be undermined. From the perspective of countries, the adoption of the "adequate level of protection" approach *de facto* restricts the less developed regions, especially those that have not enacted data protection laws, from entering the global data flows. It further leads to the elimination of such countries from participating in global digital trade and exacerbates the polarization of the world economy. From the perspectives of entities, particularly those in the Information Communication Technology (ICT) sector, the legal requirements set out in different jurisdictions are likely to impose additional administrative and technical burdens when conducting business internationally. The overlapping jurisdictions over various countries, cumbersome transfer assessment rules, and excessive discretionary powers of supervisory authorities have led to increased compliance costs while reducing the transaction efficiency of multinational businesses. From the perspective of data subjects, individuals' rights and

Y. Li is Early Stage Researcher in the framework of the HEART project (*HEalth related Activity Recognition system based on IoT – an interdisciplinary training program for young researchers*), at the University of Macerata (Italy). The HEART project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 766139. This article reflects only the author's view and the REA – Research Executive Agency is not responsible for any use that may be made of the information it contains. This essay is part of the monographic section *Ubi data, ibi imperium: public law facing data localization* edited by Simone Calzolaio.

responsibilities vary from nationality, residence, or information collection region. It is, however, contrary to the original purpose of protecting personal data while promoting data sharing.

1.1. Global Data Transfer

The benefits that can be derived from cross-border data flows are growing, while the ability of countries to reap such benefits may vary[2]. Although it is widely recognized that countries should have a common interest in facilitating cross-border data flows and reconciling different policy objectives in this field, the implementation of the free flow of cross-border data remains vague. Due to the differences lay in digital economic development, legal systems, and data sovereignty objectives, it is difficult for countries to impose effective regulations on cross-border data transfer through one's own. In contemporary legislations, a trend of preference for establishing one data flow model inside a region within a given group of countries is emerging.

Multilateral international agreement

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) adopted by the Council of Europe in 1981 is the first and up-to-date only binding multilateral international agreement to set standards for the transborder data flows. The early version of Convention 108 provides general principles that require signatory countries not to restrict or impose any special authorisations to prevent the flow of personal data among the member states and aims to achieve greater unity between its members[3]. The Convention 108 was further developed in the Additional Protocol in 2001 to introduce the concept of an "adequate level of protection" for the intended data recipient countries that are not the signatories to Convention 108[4]. Such exporting party is also subject to exceptions where the transfer is in the need of individual's legitimate interests and public interest, or is based on authority-approved contractual clauses.

The Convention 108 is the result of the implementation of the European Convention on Human Rights with regard to privacy protection. It attempts to build consistent data protection principles to safeguard individual's rights while keeping active exchanges of such personal information across the borders. Be great as it may, the significance of Convention 108 is limited[5]. Although international agreement as an instrument for dealing with modern societal and legal topics is advantageous in terms applicable scope of the rules, enforcement and guidance, its complex and lengthy establishment procedures have slowed down the reaction time to the emerging issues in international community, especially in areas where international consensus has not yet been reached.

Bilateral international agreement

In view of the latency of the international community's cooperation in the field of cross-border personal data transfer, multiple emerging countries in digital economy have actively launched bilateral negotiations based on their own development needs. By reaching the bilateral agreement, it is provided with a legal basis for the personal data exchanges between the signatory countries. The EU-U.S. Privacy Shield Framework is an example. In 2014, being the direct response to the Snowden revelations, *Schrems I* case led to the revocation of the Safe Harbor as a valid mechanism for transfers between the EU and the U.S. by the Court of Justice of European Union (CJEU)[6]. The EU and the U.S. successfully reached the Privacy Shield Framework as the alternative, putting forward more stringent and descriptive data transfer requirements for data controllers[7]. After receiving wide critics, the EU Commission's adequacy determination for the Privacy Shield was rendered[8]. American companies may be permitted to acquire personal data from a total of 28 European countries after being registered under the Privacy Shield program and demonstrated that they fulfil the "adequacy protection" requirement by self-certify procedures. Privacy Shield Framework additionally includes verification, assessment and supervision mechanisms, as well as special rules related to arbitration procedures[9]. The bilateral agreement allows two countries to make more detailed arrangements for cross-border data transfer issues. It is advantageous in terms of negotiation efficiency and enforcement, as well as the flexibility of contents. Yet, its scope of application is limited to the jurisdictions of the two countries. For the establishment of a regional framework of personal data cross-border transfer, bilateral agreement has very limited effect on bridging different legal standards.

Soft laws

Soft laws often play important roles in encouraging reluctant states to consider and eventually agree upon policies and strategies in areas where serious differences exist. Many international organisations have issued soft laws to regulate cross-border transfer of personal data, which has given certain guidance to the national legislation and implementation. The OECD Privacy Guidelines released in 1980 serve as the first internationally agreed upon set of personal

information protection principles and focus on balancing between the needs for digital economy and the protection of individual's rights. It addressed the needs for greater efforts to tackle the global dimension of privacy through improved interoperability and provided the member states a basic framework of free flow of personal data for further negotiations. The APEC framework, published by the Asia-Pacific Economic Cooperation in 2004, is a framework to protect privacy while enable regional personal information transfers to promote consumer trust and business confidence, to lighten compliance burdens and booster digital economy. The data controllers' obligations are particularly emphasised as data subject's consent is mandatory prior to the transfer of the personal information, and the adequate level of data protection shall be guaranteed. This framework is used as a basis for the APEC Cross-Border Privacy Rules ("CBPR"). The U.S.-led CBPR system comprises Privacy Enforcement Authority, privacy certification institutions and recognized entities operating upon nine general privacy principles and a bundle of practical requirements. A joint APEC-EU working team attempts to discover more opportunities for "double compliance" via EU BCR and APEC CBPR referential[10]. Additionally, the Southern African Development Community (SADC) developed the Model Law on Data Protection in 2010 containing general data protection principles for cross-border data transfer. Notwithstanding the efforts, many African countries are still struggling with enacting laws to regulate the collecting and processing of personal information. The organisations' practices stopped at proposing a broad framework of guidance. Further discussions over effective solutions to the conflicts of applicable laws of personal data transborder regulation are needed. However, the international negotiations and corporations are worthy of recognition.

1.2. Problem Statement

China is imminently in need for a strong and more coherent data transborder flow regulatory framework, backed by transparent enforcement and legal certainty. As the world's second largest economy, China's demand for data exchange across borders has grown significantly. On one hand, cross-border e-commerce transactions reached 134.7 billion RMB (approximately 17.7 billion Euro) and is expected to reach one trillion Euro by the year 2020, accounting for 37.6% of China's total imports and exports[11]. On the other hand, technical innovations have brought unprecedented threats to privacy and data security. Furthermore, global trade and political tensions are rising. Against this background, China needs to carefully assess domestic and international economic and legal situations to create a quality strategy for cross-border data flow regulation.

China's cross-border data transfer regulation is an evolving project that still under development, with various administrative regulations and department rules mushrooming. The Personal Information Protection Law has been incorporated into the law-making plan of the 13th Standing Committee of National People's Congress, and was released with the draft for public comment on October 21, 2020. The legislators especially emphasised the protection of public interest and state security, taking into account the needs of the protection of data subject's rights, and took a reluctant position on the regulation of cross-border data transfer. *The Cybersecurity Law* (enacted in 2017) for the first time addressed data localisation and security assessment of data export requirement for Critical Information Infrastructure providers[12]. *The Civil Code of China* (adopted May 28, 2020) newly introduced greater protection of privacy rights and personal information[13]. It clarified that (i) the rights and interests of natural persons over their personal information are civil rights and private rights; (ii) the natural persons' rights to their personal information belong to personality rights; and (iii) the distinction is made between privacy and personal information. These three pieces of legislations constitute the foundation of China's personal information protection laws.

The Measures on Personal Information and Important Data Export Security Assessment (draft for comments) was released on 2017 by the Cyberspace Administration of China (CAC). It was planned to contain elements in the scope of the security assessment, such as the consent of data subject, the security protection status of data recipient, and risk of data leaving China. Upon receiving constructive criticism, the CAC updated its second version of *The Measures on Personal Information Export Security Export* (draft for comments) in 2019. One essential element – the important data – was removed while one important element – the standard contractual clauses – was introduced.

This paper aims to provide a comprehensive analysis of China's cross-border data transfer regulation. The rest of the paper is organised as follows. Section 2 demonstrates how the personal data protections laws have evolved owing to transitions in the Chinese economy with a focus on the objectives and characteristics of cybersecurity law followed by how the Cybersecurity Law (CSL) is enforced and authorities responsible for the same. Section 3 highlights

the Data Export Regulations in China, broadly classified into Critical Information Infrastructure Data Export and Personal Data Export and how the approaches vary in terms of the measures and assessments. This section is followed by the conclusion derived from this study. Notably, this paper includes important drafts of laws and regulations to demonstrate the possible future developments in China.

2. The Evolution of China's Personal Data Protection Laws

Chinese concepts of privacy and personal data protection vary through different historical periods. Most of them are rooted from Chinese traditional ethics or moral standards, and partially integrated with socialism ideology[14]. Since the economic transmission from central planned market to free market in the 1990s, Chinese communities began to experience greater variety of roles in participating economic, societal and political activities. Although traditional predominant values still hold a deep influence on people's behaviours, individualism and subjectivity have dramatically been promoted in their social life. Scrutiny and concerns over the importance of individual's privacy and protection of emerging personal data processing are ever growing. Baidu, the largest Chinese search engine provider, was sued by a consumer rights protection association for illegally collecting user data without consent[15]. Alibaba, another internet giant, was challenged by Chinese users for the misuse of their digital transaction records and social media presence on Zhima Credit (an online credit service that offers loans based on users' digital activities)[16]. The consciousness of privacy in contemporary China has been gradually expanded and individuals have raised their expectations for the right to be let alone.

Prior to the CSL, China's personal data protection policy was integrated in a number of laws and administrative rules through the protection of personal dignity and reputation. Article 28 of the Chinese Constitution provides citizens an inviolable personal dignity from "insult, defamation or false charge." Article 252 of Criminal Law (1997) prohibits any violation to the freedom of citizen's communication rights by hiding, destructing or illegally opening other's letters. Article 101 of General Principles of Civil Law (1986) confers natural person and legal person the right of reputation. The Supreme People's Court in 2001 for the first time confirmed the legal ground for claiming remedies for the damages caused by the violation of one's privacy or other personal rights.

Personal Information was firstly defined in the Notice concerning Punishing Criminal Activities of Infringement of Citizen's Personal Information in 2013, stating that "personal information includes any information that can identify the citizen's personal identity or information and data involving the citizen's personal privacy, such as name, age, ID number, and so on." In response to the rapid development of technology, Chinese authorities released over 200 pieces of laws, administrative regulations and sector-specific rules regulating the collecting and processing of personal information across domains like banking, healthcare, medical record or disease control[17]. A comprehensive framework for personal data protection laws is urgently in need.

2.1. Cybersecurity Law

In November 2016, the final legislation of Cybersecurity Law was passed by the Standing Committee of National People's Congress imposing new cybersecurity requirements on *network operators* that "own or manage networks, or provide network services." It applies to any activities related to the "construction, administration, maintenance and use of networks."[18] The CSL is up to date the highest-level legal instrument concerning personal information protection in China. Be broad as it is, three pillars constitute the substantive provisions of the Law: multi-level protection scheme, critical information infrastructure protection, and personal information protection.

2.1.1. Objectives

Article 1 of the CSL sets multiple objectives aiming to "safeguard cyberspace security, to guarantee cyberspace sovereignty, state security and social public interests, to protect legitimate interests of citizens, legal persons and other organisations, to promote the health development of informationalisation of economic society"[19]. This is aligned with the special aspect in terms of multiple objectives in Chinese law makings, particularly those areas where face most of the challenges brought by emerging issues. As this provision suggests, the objectives are to govern everything within the country's cyberspace infrastructure, ranging from internet activities to data export.

The downside is, however, observable. It is not unusual that such generality and flexibility, sometimes excessive omissions, can be found in Chinese law drafting. Coupled with a wide discretionary power conferred on lower-level competent authorities in order to implement the law, predictability and certainty of law often are compromised. Furthermore, in order to identify a complete set of independent objectives and to prioritize them, the law makers are re-

quired to hold clear concepts, logical foundations and thought-provoking procedures[20]. In China, most of the data protection rules were made in the response to an existing problem. Despite insufficient experiences in data protection law makings and "rent-seeking" among various authorities, one essential aspect is the missing of a unified value for the protection of personal information. It is yet not crystal clear in other jurisdictions as technology and law in this regime are significantly inter-dependent. Without the clear value set ahead, multiple objectives would affect the fundamental principles as well as the conceptual framework of data protection. The immediate consequence is the vague defining of rights and obligations for stakeholders involved. This echoes the lack of legal predictability and certainty.

2.1.2. Multi-level Protection Scheme

Article 21 of the CSL requires all network operators to be obliged with different security measures according to the *cyberspace Multi-level Protection Scheme* (MLPS). Under the MLPS, network operators shall safeguard the cyberspace from interference, destruction or unauthorised access, and to protect the internet data from leak or fraud. Security obligations include but not limited to (i) the establishment of the internal security management protocol; (ii) the appointment of a person in charge of security affairs; (iii) the deployment of technical measures for cyber attacks; (iv) the record of internet operation activities no shorter than six months and the response plan for security incidence; and (v) the classification of data and the backup and encryption of the important data.

The MLPS was born from the demands of the national computer system security in 1994 and thus falls under the competence scope of the Ministry of Public Security (MPS). After a series development of administrative regulations, the updated draft of *Regulation on Cybersecurity Multi-level Protection Scheme* as a milestone was released in 2018. Together with a bundle of supplementary national technical standards, the so-called MLPS 2.0 framework of cybersecurity in China is finalised[21]. The MLPS Regulation as a supporting document of Article 21 CSL defines descriptive obligations and requirements for the network operators fell under different levels of MLPS. Eleven general obligations are listed to clearly allocate the liability and to set technical and organizational security measures. Specific obligations need to be met according to the level of the network operator's activities that would affect the state and public security, scaled from 1 the least risky to 5 the most risky[22]. After being classified, which is based upon a self-assessment, the network operators are required to deploy special security measures such as personnel management, datasets backup and encryption to protect important data.

The compliance with the MLPS 2.0 will be essential for understanding the personal data export regulation in China. Not only because such compliance is mandatory, but also the second pillar of the CSL, critical information infrastructure protection, is based on the classification within MLPS.

2.1.3. Critical Information Infrastructure

Critical Information Infrastructure (CII) is a major challenge in implementing China's cybersecurity strategy and had been recurred at top-level national cybersecurity meetings. On the basis of the cybersecurity MLPS, the state implements key protections to CII which, «if destroyed, suffering a loss of function, or experiencing leakage of data, might seriously damage national security, social welfare, and public interests.» A non-exhaustive example list (including public telecommunication and information service, energy, transportation, water resources, finance, public service and e-governmental information) is given in Article 31 CSL showing the broad scope of the application of CII requirement. In principle, any network operators that being graded above level III (including level III) under the MLPS shall be regarded as CII operators.

CII operators are imposed stricter security requirements due to the nature of the data being processed. More importantly, Article 37 CSL rules that:

«Personal information or important data that CII operator collected or generated during its operations within the territory of the People's Republic of China shall be stored within the territory of China.»

Transferring CII information outside of China is only allowed under exceptional circumstances where actual needs for business are in place and a security assessment is approved by competent authorities. Under the CSL, CII operator is the only subject-matter that is required to comply with the data localisation policy and security assessment for cross-border data transfer. However, the definitions of CII and other key concepts such as important data remain unclear.

CII is in essence a network facility, information system, digital asset, or a collection of such elements[23]. In the early stages of informationalisation, CII was considered to be part of Critical Information (CI) that was scoped clearly. With the changing of the technical landscape, sources of risks are far beyond the scope of CI, such as the attacks coming from

virtual entities, i.e. ICT or Operation Technology domain[24]. At present, large-scale network destruction of CII is a high-risk yet low-probability incident that very limited examples of CII being damaged from cyber-attacks or data leakage can be provided. Therefore, the assessment of security and risks of CII mainly reply on the experts in the domain, instead of evidences or case studies. This brought inconsistency in determining the scope of CII and eventually made it difficult to implement relevant policies. Generally, all ICT service providers fall within the scope of CII operators according to the laws, which is not efficient in the digital economic community.

2.1.4. Personal Information Protection

There is no chapter entitled "personal information protection" in the CSL, yet provisions related to the protection of personal information are scattered through this law. Chapter 4 Network Information Security covered most of the personal information protection provisions. Network operator is the core subject-matter that most of the obligations imposed upon. Data subject's rights have been conferred passively through the legal obligations for network operators, i.e. network operator shall correct or delete on the request of the data subject when the personal information are incorrect or wrongly processed.

The structure comprises basic principles for processing, legal grounds for processing and a non-exhaustive example list of prohibited conduct. Personal information can only be collected when data subject is informed and agree to the purpose and scope of the collection. The processing of personal information must follow basic principles listed in Articles 40-42, 47, 49 which share substantive similarities with the APEC privacy framework. Consent is the ONLY legal ground for processing of the personal information[25]. This is to ensure that data subject has sufficient autonomy to decide the way his or her personal data will be collected, processed and distributed. Such autonomy is endorsed by the sufficient informing requirement, meaning that only after data subject is informed of the purpose, scope and means of processing of the personal data can he or she be capable of giving the genuine consent. The network operator has to perform the information obligation before collecting the individual's personal data.

2.2. Enforcement and Authorities

The CSL's provisions relating to data privacy formed the most comprehensive and broadly applicable set of privacy rules. It acts as an umbrella that covers a bundle of administrative regulations and numerous normative texts scattered across most of the industries. To date there is no independent authority for data protection. Multiple competent authorities or supervisory authorities are in charge of the implementation and enforcement of the rules.

2.2.1. Regulatory Framework

Various types of documents have the force of law in China. Among all the legal instruments, the Constitution Law enjoys the highest primacy yet is rarely applied directly. The law made by the National People's Congress or the Standing Committee of NPC has the highest legal effect in the respective regime, such as the Cybersecurity Law.

Administrative regulations are rules promulgated by the State Council. Its legal effect is lower than the Law but higher than the Department rules. To date, two administrative regulations were issued: the *Regulation on Critical Information Infrastructure Security Protection and the Regulation on Cybersecurity Multi-level Protection Scheme*. Additionally, sector-specific administrative regulations also affect China's personal data export study, such as the *Regulation on Computer Information Security Protection and the Regulation on Human Genetic Resources Information Management*.

Department Rules are legal documents issued by the ministries and commissions under the State Council, along with other agencies with administrative functions directly under the State Council. The applicable scope is determined by the competence of the issuing government department. For example, the aforementioned *Measures on Personal Information Export Security Assessment* is a department rule issued by the CAC. To date, around 30 department rules were issued by various authorities in the field of security, data protection and export.

Judicial interpretations are the explanations to specific legal questions made by the State Supreme judicial institutions during the application of the laws. Both the Supreme People's Court and the Supreme People's Procuratorate had released interpretations relating to cases that infringe personal information.

Standards (no legal effect) are mandatory or voluntary technical standards published by the Standardisation Association of China (SAC). In Cybersecurity and Data protection fields, TC260 group under the SAC is responsible for a series of standards titled Information Security Technology that covers methodologies, definitions or scopes of the norms. Within China, national standards play an important role in implementing laws and regulations. Despite the non-compulsory nature, they are better understood as a quasi-regulation rather than a technical specification typically presented in Western context.

Since 2010, over 240 national standards in this field have been published. It is remained debatable with the necessity of such a big amount of technical standards in force.

Additionally, local regulations are directly applied within the scope of the provinces, autonomous regions and municipalities directly under the Central Government.

2.2.2. Competent Authorities

Under the CSL, different parties are in charge of specific area of works. The *State* is to (i) make cybersecurity strategies; (ii) clarify fundamental requirements and objectives of cybersecurity; (iii) guide key area cybersecurity policies and measures. Additionally, the State shall adopt measures to guarantee the cyberspace free from attacks, interferences and crimes. The *network-related industrial associations* shall provide guidance for entities' self-regulation and promote the healthy development of the industries. The *network operators* are required to fulfil obligations addressed in the CSL and to uphold societal responsibilities.

Respectively, the *Congress* is responsible for determining the scope of CII and key areas. The *Cyberspace Administration of China*, an administrative agency directly under the State Council, is in charge of the coordination and management of all cybersecurity related issues. The MIIT and MPS are responsible for supervising and managing affairs within the scope of their competence[26]. The SAC publishes national and sectoral technical standards.

The CAC, also framed as an agency directly under the Chinese Communist Party, inherently carries a heavy stroke of political colour. It is the most important supervisory authority of cybersecurity and directly reports to the State Council for managing Internet information and contents. It works independently from the Ministries of information, public security or commerce. The CAC also leads the drafting of department rules implementing the CSL. Its branches at the province level are the main enforcement institutions that supervise, investigate, and impose administrative fines.

2.2.3. Enforcement

Enforcement of the CSL and related rules in China follows a typical bottom-top approach. Supervisory authorities have broad discretionary powers as well as the competence to impose administrative fines upon entities. Overlapping areas of jurisdictions often pop up among different authorities. The CAC is responsible to coordinate all issues arise through the enforcement. Although not legally binding, the competent authorities often refer to the Information Security Technology standards when performing assessments or issuing certifications.

The supervisory authorities are actively performing their duties since the year 2015. Means of enforcement include communication with the operator, supervising the modification of business, or administrative fines and termination of the operation. A special operation targeting at illegally collecting and processing personal information through mobile applications is jointly conducted by the CAC, MIIT (Ministry of Industry and Information Technology of the People's Republic of China) and SPS.

It is rebuttable that the CAC has the competence in imposing administrative fines. According to the Organic Law of the State Council, the CAC is not one of the departments under the State Council. The legal ground for the CAC should be Article 11 of the Organic Law of the State Council ruling that "the State Council can establish agencies directly under the Council for managing specific affairs or assisting the Primer to handle specific affairs". However, it is not explicitly informed that which agency the CAC is established for. The official documents issued by the later agencies are categorised as "other kind of administrative documents" which cannot be enforced as the basis for administrative fines[27].

According to the CSL, it is clear that the responsibilities of the CAC is coordination and supervision. Therefore, the rules and measures issued for imposing fines might not be legitimate, even their legal effect could be challenged (emphasis mine). Such gap originated from the boost of cybersecurity legislations, and shall be bridged in the future law makings. With the working-in-progress Personal Information Protection Law, the CAC is expected to (i) remain as an agency under the CCP for supervising the Internet affairs, and the national independent Data Protection Authority is formed for data protection regulation; or (ii) be conferred the legitimacy under the new law.

3. Data Export Regulations

3.1. Critical Information Infrastructure Data Export

The starting point for the study of personal data export is to define the CII operator. Quoting the data localisation requirement discussed in 2.2.3, any personal information or important data that are involved in CII shall not be transferred abroad unless a security assessment is conducted with the supervisory authorities' approval.

Defining CII

On 11 July 2017, the CAC released the draft for comments *Regulation on Critical Information Infrastructure Security Protection* (CII Regulation). Aligned with the CSL, the scope of the CII shall be determined by a two-step test: (i) if business falls within the industry or sector listed in the Regulation; and (ii) if the business is graded security level 3 or above as demonstrated in Table 1.

Table 1: Security levels under the Regulation on Cybersecurity Multi-level Protection Scheme

Subject-matter of the infringement	Severity of damage		
	Harm	Serious Harm	Particularly serious harm
Legitimate interests of citizens, legal persons or other organisations	I	II	III
Social order and/or public interest	II	III	IV
State security	III	IV	V

Additionally, the CAC's Guidelines on State Cybersecurity Inspection (no legal effect) proposed three aspects to help self-evaluating the CII:

1. key business domain, e.g., data centre cloud service, domain name resolution service, or voice data internet basic network and hub in Telecommunication sector;
2. information system or industrial control system that supports the key business, e.g., generator set control system or information management system;
3. quantity of CII device, e.g., registered users above 10 million, or active users above 1 million, or daily transaction exceeds 10 million RMB for a platform service.

Defining CII operator

The rules apply to registered entities operating inside the territory of the PRC, as well as those which do not register inside China but offer business and services to Chinese customers. The criteria to determine whether the entity provides business or service in China include: (i) using RMB as currency; (ii) using Chinese as the language; and (iii) delivering goods to China. Any of the abovementioned criteria is sufficient to lead multinational companies to store the collected personal information and important data inside China.

3.2. Personal Information Export

3.2.1. Personal Information

Personal Information is defined as "any information that is recorded, electronically or by other means, can be used or in combination with other information to identify the identity of a natural person" (Art. 76(5) CSL; Art. 4 Personal Information Protection Law (draft)). It is a commonly adopted "capacity to identity" methodology.

In the Information Security Technology – Personal Information Security Specification 2017, based on the definition given in the CSL, this standard enlarged the scope by using a very expansive wording: "any information recorded electronically or by other means". This targets all operators from both public and private sector, as well as all collecting and processing activities of personal data they conduct. Furthermore, the standard added that "personal information is ... or any information that can reflect a specific natural person's activities". This may be consistent with the broad interpretation of personal data held by the CJEU.

Important Data has been repeatedly addressed in the CSL. It is of crucial importance for assessing CII and CII data export requirement, yet surprisingly not defined in the law. The draft of Information Security Technology – Data Export Security Assessment Guidelines (the Guidelines) defines important data as "raw data and inferred data collected or generated by entities, organisations and individuals inside of China, that do not involve national secrecy, but are closely related to state security, economic development or public interests". Publicly accessible government information is excluded from the scope of important data. An index for determining important data is attached with this standard, comprising of 27 main categories and 223 sub-categories. The categorisation is similar to the U.S. Controlled Unclassified Information (CUI) system.

3.2.2. Measures on Personal Information and Important Data Export Security Assessment 2017

On 11 April 2017, the CAC circulated the draft for public comments entitled "Measures on Personal Information and Important Data Export Security Assessment" (the 2017 Measures). Unlike the CSL, the 2017 Measures expand the subject-matter of Article 37 CSL from "CII providers" to "network operators". Under the CSL, any owners or managers of networks and network service providers are defined as network operators. It is disappointing since the main issue

that practitioners were expecting from the 2017 Measures is to distinguish between the CII operator and the ordinary network operators. A clear definition of important data is also missing, only stated that "data closely related to state security, economic development and societal public interests." It further cited the Guidelines as the reference.

Being the first legislation concerning data export regulation of China, the 2017 Measures provided guidance to assess the necessity of the export and data that are prohibited from exporting. Security assessment is classified into self-conducted and authority conducted. Data that do not exceed the benchmark (500,000 pieces of personal information/1,000 GB data/important domains) can be exempted from administrative procedures of approval. Unfortunately, all essential issues were kept untouched, or otherwise worded vaguely, making it very difficult to comment.

3.2.3. Measures on Personal Information Export Security Assessment 2019

After receiving a large number of public comments, the CAC published the second draft titled "Measures on Personal Information Export Security Assessment" (the 2019 Measures). As its name suggests, the 2019 Measures only apply to personal information. The legal requirements set out in the 2019 Measures are significantly more onerous than the 2017 Measures. Within two-year considerations, the legislators demonstrated observable preference in data export regulation approach.

Data localisation

The 2019 Measures require all personal information to be stored domestically for security assessment before being provided to recipients outside of China[28]. Two aspects are implied: all personal information need to be locally stored; and all personal information exports need to go through security assessment.

While data localisation is gradually adopted in international data regulation standards, one shall notice that data localisation does not necessarily mean the restrictions over cross-border data flows. Either the EU GDPR or the U.S. CUI system both emphasise that data localisation, backed with transparent regulatory rules, can reconcile the objectives of safeguard state security and personal rights and free flow of data across borders, which are of equal importance. The 2019 Measures itself aims to functioning as a precise and predictable mechanism for cross-border personal data transfer.

Security assessment

Network operators shall submit the applications for a clearance for the personal information export to the province-level Cyberspace Administrations after a transfer contract is signed with the recipient. The supervisory authority after received the application shall conduct security assessment based on the submitted documents, and to complete it within 15 working days, with the possibility of extensions depending on the complexity of the export.

The security assessment focuses on (i) legal compliance; (ii) protection of data subject's rights; (iii) enforceability of the transfer contract; and (iv) the recipient's record on whether it had infringed data subject's rights or had security incidence. When serious data leakage or data misuses occur, the data subjects are unable to protect their legitimate interests, or the parties are unable to provide protection of the personal information, the authority can request the network operator to pause or terminate the transfer. The security assessment shall be performed at least once per two years. When the substantive factors, such as the purpose of transfer or the retention period, have changed, a new application of assessment shall be submitted.

Standard contractual clauses

The requirement of the legally-binding contractual agreement between the network operator and the recipient is probably the biggest surprise in the 2019 Measures. This so-called transfer contract is the EU Standard Contractual Clauses alike, taking into consideration the limitation of territorial jurisdiction, recognises *inter partes* autonomy.

The contractual clauses are required to include: (i) the purpose, type and retention period of the personal information export; (ii) the data subject is the beneficiary of the clauses involving data subject's interests; (iii) the legal ground for the data subject to claim for remedies when infringement occurs; (iv) when the recipient is unable to perform the contract due to its state's legal environment changed, the contract shall be terminated or re-assessed; and (v) the termination of the contract shall not exempt the obligations involving the legislative interests of the data subject, unless the personal information is destroyed or anonymised. The 2019 Measures further clarifies the contractual obligations of network operator and recipient, respectively.

The adoption of standard contractual clauses integrates the regulatory requirements into contract autonomy. It is expected to indirectly abide offshore entities by the China's standard. This approach largely depends on the supervision of the

post-transfer performance of the parties. Considering that China is still waiting for her own Personal Information Protection Law, it is more likely that China's personal data protection and cross-border transfer regulation will be tilted towards the European standard. On the other hand, there is no clear line between personal information and important data. Important data naturally could contain a large amount of personal information. The regulation on important data and important data export is waiting for the other boot to drop.

3.2.4. Personal Information Protection Law (draft)

On 21 October 2020 the Legislative Affairs Commission of the Standing Committee of the National People's Congress released the draft of Personal Information Protection Law (the PIPL) and invited for public comments. Different from the 2019 Measures, the PIPL draft does not require all kinds of personal information transborder activities to be examined through the security assessment.

Derogations

Cross-border transfer of personal information is by default not allowed, unless at least one of the derogations is granted:

1. Where the amount of personal information being processed reaches the threshold for CAC security assessment, the personal information processor shall firstly store the personal information inside China. Such personal information can only be transferred outside of China after the security assessment being conducted and approved by the CAC[29].
2. Prior to the cross-border transfer, the processor shall provide the data subject with information including the identify and contact of the recipient, purpose and means of processing, types of personal information, and means for data subject to implement the rights. The transfer is allowed when the individual's consent is obtained[30].
3. A personal information protection certificate issued by a CAC-recognised organisation[31].
4. Contractual obligations over the recipient with regard to the personal information protection[32] (similar to the contractual clauses described in Sec. 3.2.2).

Restrictions

For the concerns of the protection of China's data subjects and data sovereignty in the global data governance, as well as to achieve a delicate balance in international relations, the PIPL draft for the first time introduced restrictions and countermeasure clauses over personal data. The measures embodied a "black list", on which the subjects to the restrictions or countermeasures will be included in the list that personal information transfer is restricted or prohibited. The applicable conditions of restrictions and countermeasures have also been strictly limited. The subjects to the restrictions include foreign institutions or individuals engaged in personal information processing activities that (i) damage the rights of Chinese data subjects; and (ii) endanger China's national security and public interests[33]. The subjects to the countermeasures are countries or regions that impose discriminatory restrictions, prohibitions or similar measures on China[34].

DPIA requirement

Data protection impact assessment (DPIA) is one of the most important means for the continuous and autonomous operation of the compliance operations that personal information processors shall demonstrate and/or self-certify. Prior to the Personal Information Protection Law, DPIA is recommended via non-mandatory technic standards. For the first time DPIA is ruled as a legal compliance that more stringent requirements have been put forward for the establishment of an organisation's internal compliance system. Specifically, the DPIA is required when personal information are transferred to a recipient that is located outside of China. A period of minimum three years has been proposed as the retention time for keeping the result of the DPIA and the record of the processing[35].

Transfer by national agencies

The access and transfer of personal information are possible based on the request for international judicial assistance. Where national agencies need to transfer personal information abroad, special laws and regulations shall be complied with[36].

4. Conclusion

With the increasing participation of emerging countries in the global data governance, the traditional legislative paradigm dominated by the European Union and the United States is constantly being broken and reshaped. It is particularly important for China to establish the regulatory framework of cross-border data transfer, for not only it involves the rights of Chinese citizens and entities, but also the cyber sovereignty and national security, as well as the framing of global cyberspace rules.

China keeps leveraging the data sovereignty to fasten the law makings to support the develop-

ment of critical technology in digital domains and the infrastructure construction. The cross-border data transfer regulation prefers a strict unidirectional data flow administration that focuses on controlling the flow of the data being transferred outside of China. The regulation is largely orientated by the CAC agencies, which weakens the autonomy for individuals and entities in terms of self-governance and enforcement. It is better to objectively value the importance of efficiency in digital economy and to avoid the excessive rigid adherence to traditional sovereignty, of which, the data localisation requirement as the strongest manifestation of data sovereignty is imposed.

In practice, either the "common European data space" proposed by the European Data Strategy, or the "certified governments" recognized by APEC CBPR system are both an attempt to establish cross-border judicial corporation frameworks among trusted entities for the application of rules and efficient enforcement. However, China has not established a mutual trusted mechanism for transborder data flow with other countries. The proposed initiatives largely remain at the conceptual level without practical operability.

Despite the limitations, there are various positive dynamic developments in the framing of China's cross-border data regulation. The CSL, together with Civil Code and Personal Information Protection Law demonstrate great willingness towards a stronger data protection regime and more flexible regulatory mechanism. By introducing contractual obligations and statutory derogations while strengthening domestic personal data protection standard, it is observable that China's legislation is continually moving towards the European approach. Given the fact that countries are unlikely to form a corporation framework in a short period, cross-border data transfer between China and the EU would be profoundly rooted in bilateral and multilateral trade and investment negotiations.

Notes

[1]There is a lack of clarity as to the meaning of the term "cross-border data transfer" even inside one jurisdiction, and often regulatory instruments use different definitions to apply the measures. The EU General Data Protection Regulation (GDPR) refers to "transfer to a third country of personal data" (recital 153) without defining "data transfer"; the APEC Privacy Framework variously uses the terms "international transfer", "information flows across borders", cross-border information flow" and "cross-border data transfer" interchangeably to refer to the movement of personal data across national borders. The OECD Privacy Guidelines refer to "transborder data flows", defining the term as "movements of personal data across national borders" (Section 1(c)), while the Convention 108 refers to "transborder flows of personal data", defined as "the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed" (Article 12(1)). It is also unclear whether merely making personal data accessible should be considered to result in such a transfer, or whether this requires some active or automatic transmission of the data (see Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971). In this article, cross-border data flow and transborder data flow are interchangeable, based on the context as well as the specific document it is referred to.

[2]See OECD, *Declaration on Transborder Data Flows*, 1985.

[3]See Council of Europe, *Details of Treaty No.108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1985.

[4]See Council of Europe, *Details of Treaty No.181. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*, 2004.

[5]Limited signatory countries, overbroad content and free applicable scope eliminate the practical performance of the Convention 108. Additionally, International Law Commission listed "protection of personal data in the transborder flow of information" in its long-term working programs as early as 2006, yet fruitless so far. See *Report of the International Law Commission Fifty-eighth session (1 May-9 June and 3 July-11August 2006)*, p. 489.

[6]The CJEU found that the U.S. government permitted generalized access to electronic information and failed to provide redress mechanisms. Therefore, the CJEU determined that the U.S. law did not provide an adequate level of protection essentially equivalent to EU laws. See *Schrems v. Data Protection Commissioner*.

[7] Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM/2015/0566 final.

[8]Digital Rights Ireland brought the first challenge on 2016, seeking the annulment of the determination on the basis that the Shield failed to provide sufficient substantive changes from the Safe Harbor Framework. This challenge was dismissed for lack of admissibility. French advocacy group La Quadrature du Net also challenged the Commission's decision arguing that the Shield not only continues to violate the Charter, but also fails to provide effective redress mechanisms. This case remains pending.

[9]Similarly, the U.S. also reached Swiss-U.S. Privacy Shield Framework with Switzerland.

[10] The Referential for Requirements for Binding Corporate Rules (BCR) and APEC Cross Border Privacy Rules system serves as an informal checklist for companies to apply certifications under the BCR and CBPR system. The referential outlines common compliance requirements and ad hoc requirements for each of the systems. Although the referential was superseded after the enactment of the GDPR in 2018, EU representatives have continued to express a strong interest in developing a work plan for future efforts. See Article 29 Data Protection Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents.

[11]See Ministry of Commerce of PRC, *Report on E-Commerce in China*, 2018.

[12]The *Cybersecurity Law*, 2017.

[13]«The personal information of a natural person shall be protected by law. Any organization or individual that needs to acquire the personal information of an individual shall obtain such information in accordance with law and guarantee the safety of such information. Any illegal collection, usage, processing, and transfer of the individual's personal information, or illegal trade, making available or disclosure of other's personal information is the violation of law.» Article 111 Civil Code of the People's Republic of China.

[14]See B.S. McDougall, A. Hanson (eds.), *Chinese Concepts of Privacy*, Brill, 2002, p. 8.

[15]See M. Jing, *China consumer group accuses Baidu of snooping on users of its smartphone apps*, 2018.

[16]See X. Wang, *Zhima Credit apologizes for its annual report's "mistake"*, 2018.

[17]China provides direct protection of personal information through The Seventh Amendment of Criminal Law, Tort Law, Telecommunication Law, Junior Protection Law, Consumer Protection Law, etc. Indirect protection of personal information is provided though Constitution Law and Civil Law. For example, the Ministry of Industry and Information Technology is in charge of regulating the ISPs via *Measures on Protecting Personal Information of Telecommunication and Internet Users, Measures on SMS service management*, etc.

[18]*Cybersecurity Law* (n12), Article 2.

[19]*Ivi*, Article 1.

[20]See R.L. Keeney, *Identifying, prioritizing, and using multiple objectives*, in "EURO J Decis Process", 2013, n. 1, p. 45-67.

[21]The three newly released national standards are: (1) GB/T 22239-2019 *Information Security Technology-Basic Requirements for the Multi-level Protection*, (2) GB/T 25070-2019 *Information Security Technology- Cybersecurity Multi-level Protection Security Design Technical Requirements*, and (3) GB/T 28448-2019 *Information Security Technology-Cybersecurity Multi-level Protection Assessment Requirements*, which was into force on 1 December 2019. Another national standard titled GB/T 25058-2019 *Information Security Technology-Implementation Guide for Cybersecurity Classified Protection* comes into effect on 1 March 2020.

[22]For the description of the security levels, see Table 1.

[23]CAC, *National Cyberspace Security Strategy*, 2016 (unofficial English translation). See also, Title VII, the USA PATRIOT Act, 2001; M.P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, National Institute of Standards and Technology of the U.S., 2018.

[24]For example, some malware target industrial operation system in electricity, gas, or chemical plants, while some cyber attacks target the control or tampering of information and data.

[25]*Cybersecurity Law* (n12), Article 41.

[26]*Ivi*, Article 8.

[27]*Law of the People's Republic of China on Administrative Penalty*, 2018, Article 14.

[28]*2019 Measures*, Article 2.

[29]*Personal Information Protection Law* (draft), Article 38(1) and Article 40.

[30]*Ivi*, Article 39.

[31]*Ivi*, Article 38(2).

[32]*Ivi*, Article 38(3).

[33]*Ivi*, Article 42.

[34]*Ivi*, Article 43.

[35]*Ivi*, Article 54.

[36]*Ivi*, Article 41.

* * *

La disciplina cinese del trasferimento transfrontaliero dei dati

Riassunto: In virtù della crescente partecipazione dei paesi emergenti alla governance globale dei dati, il paradigma normativo tradizionale dominato dall'Unione Europea e dagli Stati Uniti viene costantemente disintegrato e rimodellato. È di particolare importanza per la Cina stabilire il quadro normativo del trasferimento transfrontaliero dei dati, poiché non solo coinvolge i diritti dei cittadini e delle istituzioni cinesi, ma anche la sovranità digitale e la sicurezza nazionale, nonché la definizione delle regole globali del cyberspazio. La Cina continua a far leva sulla sovranità dei dati per consolidare i processi di produzione di norme a sostegno dello sviluppo di tecnologie critiche in domini digitali e della costruzione di infrastrutture. Questo articolo mira a fornire una analisi sistematica delle normative cinesi relative allo scambio transfrontaliero dei dati. Vengono analizzate sia le disposizioni già adottate sia quelle in corso di adozione, come anche le norme vincolanti e quelle non vincolanti; vengono inoltre evidenziati gli sviluppi positivi verso la definizione in Cina di un quadro regolatorio del flusso transfrontaliero dei dati. Nonostante alcune limitazioni, la legge sulla sicurezza informatica, insieme al codice civile e alla legge sulla protezione dei dati personali, dimostra un forte orientamento verso un regime di protezione dei dati più forte e un meccanismo di regolamentazione più flessibile.

Parole chiave: Cina – Circolazione transfrontaliera dei dati – Sicurezza informatica