

Legal Commentary

June 28, 2019



Mission and Boundaries: Thoughts on the Recent Personal Information and Data Security Rules

Authors: Min ZHU | Kemeng CAI

Recently, a series of personal information and data security rules and standards have been issued, including the *Measures for Cybersecurity Reviews (Draft for Comment)*, *Measures for Administration of Data Security (Draft for Comment)* (“**Data Security Measures**”), *Provisions on Online Protection of Personal Information of Children (Draft for Comment)* (“**CI Provisions**”) and *Specification for Essential Information for Basic Business Functions of Mobile Internet Applications*, there are also several key regulatory documents awaiting promulgation.

The recent acceleration in the issuance of draft rules in the area of data protection may be attributed to multiple factors, in particular the need to strengthen regulations in the context of U.S.-China trade frictions and to exert pressure on trade talks. In this article, we wish to express our views on data protection regulations in China in light of the recent draft rules, which we hope can also serve as our feedback to the draft rules during their public comment periods. As our preliminary analysis and thoughts, this article will discuss the recent drafts from the perspectives of the boundaries of regulatory authorities’ power, regulatory approaches and methods and coordination of regulatory rules. We will further sort out and analyze specific provisions in the future.

I. Mission of the Data Security Measures

Judging from the content, the Data Security Measures can be regarded as a summation of the early stage of implementation of *the Personal Information Security Specification* (“**Specification**”) and *Guidelines for Self-assessment of Violations of Laws and Regulations by Apps Collecting and Using Personal Information*, since the Data Security Measures, in the form of departmental rules, elevate the legislative level of mature supervisory rules, practices and issues of general concern and provide confirmation and clarification. Issuance of the Data Security Measures is also consistent with general rules for administrative rulemaking, i.e., to give compulsory legal and regulatory effect to regulatory guidance once it is appropriate to do so. This practice helps to reduce resistance encountered during implementation and enforcement.

Objectively speaking, the Specification, a voluntary national standard, has far exceeded expectations in terms of its pervasive influence and applicable scope in practice, which is rare compared with other voluntary national standards. Considering the Specification has become a “soft law,”¹ and most provisions on protection of personal information under the Specification coincide with those of the Data Security Measures, the promulgation of the Data Security Measures would appear unnecessary. Therefore, it seems that the Data Security Measures should have more objectives and “ambition,” especially in terms of data security.

The Data Security Measures clarify issues related to network data scraping, targeted push, manuscript drafting, cross-border transfer approval, and presumptive fault liability of platform operators for third-party apps. Besides these provisions, another reasonable interpretation of the Data Security Measures should be that they elevate provisions of the Specification to the level of departmental rules which allows for the imposition of penalties in accordance with provisions of the Legislation Law. This will help to fix the issue of the Specification’s lack of enforceability as a voluntary national standard and finally give “teeth” to supervisory rules which have been validated and effective in practice.

The recently promulgated CI Provisions represent a breakthrough as standalone rules for the protection of personal information of children, and are also important in providing administrative enforcement power. The CI Provisions source a majority of their content from existing provisions (especially the Specification), but differ significantly in respect of administrative measures and penalties specified under Articles 24, 25 and 26, which could not be realized by the Specification.

II. Coordination between Rules Systems

Since the promulgation of the Cybersecurity Law, different administrative departments have promulgated a series of documents of different levels of effectiveness in relation to cybersecurity, personal information protection and data compliance. These documents include regulatory documents such as rules and guidelines promulgated by the Cyberspace Administration of China and other departments and commissions, judicial interpretations promulgated by Supreme People's Court and Supreme People's Procuratorate, industry standards and guidelines and enforcement action documents. Many of the issues involved in the Data Security Measures had already been stipulated in these documents. Therefore, it is becoming increasingly difficult to resolve how to coordinate the relationship between these rules systems, to provide clear guidance for industry practitioners and to resolve confusion and even conflict in the application of the different systems.²

¹ For the operation and application of the Specification in practice, you may refer to *The Effectiveness and Function of “Personal Information Security Specification”*, China Information Security, Issue 4, 2019

² A legislative case that can be referenced is the Measures for Supervision and Administration of Internet Food and Drugs (Draft for Comment) issued by the former State Food and Drug Administration in May 2014, which attempted to develop a “five-in-one” unified legislation for food (including edible agricultural products and food additives), health foods, medicines, cosmetics and medical devices. This attempt posed great challenges in legislative skills, and the implementation effects of the draft measures were also seriously questioned due to the obvious differences between these product categories, the diversity of regulatory policies applicable to these product categories, especially the regulation of drugs, and a controversy over whether or not to lift the ban on online sales of prescription drugs. The draft

It is noticeable that data security and personal information protection have been identified as two independent legislative topics, according to legislation work plans. Two separate laws are being formulated in in this respect, the Data Security Law and the Personal Information Protection Law. In addition, the legislative focus for data security (or cybersecurity) law and personal information protection are not entirely the same. Data security focuses on the protection of data confidentiality, integrity and availability, while the personal information protection focuses on the protection of individual autonomy, individual's control of personal information, and the use of personal information in conformity with the subjects' anticipated uses. The Data Security Measures mix these two topics, which poses technical legislative issues, such as the need to link with past and future legislation and the same rules which cover different subjects.

As mentioned above, if the Data Security Measures are a summation of an early stage of supervisory practice, we also believe another role of Data Security Measures is to link legislative and regulatory planning. On the basis of the mission of this completed stage, more extensive supervisory experience and legislative materials may be prepared for the drafting and promulgation of the forthcoming Data Security Law and Personal Information Protection Law.

III. Enforcement Power of Regulatory Authorities

The Data Security Measures grant broad powers to law enforcement authorities in respect of obtaining access to personal information. According to Article 27 of Data Security Measures: "Before providing personal information to others, network operators shall assess the possible security risks and obtain the consent of the information subject." A notable exception to this rule is where such information is "necessary for law enforcement authorities to perform their duties in accordance with law." Article 36 further stipulates that "[w]here the relevant competent authorities of the State Council, in order to fulfill their duties of safeguarding national security, social management, economic regulation and other duties, in accordance with the provisions of laws and regulations, require network operators to provide relevant data, the network operators shall so provide."

The foregoing provisions of the Data Security Measures are clearly too principled relative to actual circumstances³. "[N]ecessary for law enforcement authorities to perform their duties in accordance with law" and "fulfill ... duties of safeguarding national security, social management, economic regulation and other duties" are both very broad statements. Although the latter provision restricts the authorities to "relevant competent authorities of the State Council," in general, the provision still gives regulatory authorities relatively broad discretionary power. We recommend that the procedures and rights of the authorities to obtain corporate data and personal information be regulated in subsequent finalized standards or relevant regulations and rules, in

measures were not adopted after several deliberations, and the former State Food and Drug Administration finally chose to promulgate separate rules for different products categories.

³ Section 5.4 of effective version of the Specification and Article 7 of the recently issued draft for comment of the Specification. Moreover, in addition to the purpose for protection of the national security and public interests, the Specification specifies that a regulatory department may request the disclosure of personal information for purposes "directly related to criminal investigations, prosecutions, trials and execution of judgments" in the judicial process, rather than "law enforcement agencies to perform their duties in accordance with law" in the Data Security Measures.

order to realize the benefits of national security and social management while safeguarding due process and protecting the legal rights and interests of data subjects and enterprises which collect data.

IV. The Legislative Authority of Departmental Rules

Article 28 of the Data Security Measures is a particularly eye-catching clause, which stipulates that “[b]efore a network operator publishes, shares, trades or provides important data cross-border, it shall assess the possible security risks and report to the competent industry supervisory department for approval; if the competent supervisory department of the industry is unclear, it shall proceed to the provincial cyberspace department for approval. The cross-border provision of personal information is carried out in accordance with relevant provisions.”

According to Article 37 of the Cybersecurity Law, “[p]ersonal information and important data collected and generated by operators of critical information infrastructure within the territory of the People’s Republic of China shall be stored within the territory. Where it is necessary to provide cross-border, [the operator] shall conduct a security assessment in accordance with methods formulated by the competent departments of the State Council; where laws and administrative regulations stipulate otherwise, in accordance with such provisions.”

Strictly speaking, Article 37 of the Cybersecurity Law only applies to operators of critical information infrastructure, and merely requires the operators to conduct a security assessment, but does not require them to report to the “competent industry supervisory department” or “provincial cyberspace department” for approval. Does this development ultimately exceed the authority of the higher-level law to create an “administrative license,” or increase obligations on subject enterprises, or are the administrative measures refined in the form of departmental rules within the scope of authority set by the higher-level law? This is indeed a topic worthy of discussion. Of course, another explanation is that the specific reporting procedures will be clarified in the assessment methods jointly developed by the Cyberspace Administration of China and the relevant departments of the State Council in accordance with authorization granted by the Cybersecurity Law.

V. Regulatory Activities

In the field of cybersecurity, personal information protection and data compliance legislation will impose new obligations and requirements on business entities in relevant industries with each new set of rules, and lead to an increase in corporate compliance costs. In the wild west of unfettered growth, many industry practices do require regulation through the establishment of new regulatory systems, but it is a very challenging and unavoidable reality that there are trade-offs between the conflicting demands of innovation and restraint, development and regulation, self-interest and public welfare.

Compared to the traditional law enforcement and supervision methods such as supervision and inspection, regular reporting and review and approval, there is a consensus that has been formed

in recent years to apply social co-governance and government-enterprise cooperative governance in the administrative regulation of social and economic activities, which is also a concept that has been reflected in many legislative and law enforcement activities. For example, big data is of substantial potential use and value in the era of the data economy, but its use is restricted due to the high compliance requirements of personal information and data privacy protection. The cooperative governance and incentive compatibility⁴ administrative model may best resolve this conflict. It is exciting to see that the Specification has played a very positive role in mobilizing enterprises to establish internal control compliance systems for personal information protection, offering incentives to encourage voluntary legal compliance and reducing the cost of law enforcement.

This legislative concept is also reflected in Article 34 of the Data Security Measures, which stipulates: “The State encourages network operators to voluntarily pass data security management certifications and application security certifications, and encourages search engines, app stores, etc., to clearly identify and prioritize apps which have passed such certifications. The Cyberspace Administration of China, together with the State Council market supervision and regulatory department, will guide national cybersecurity review and certification organizations, and organize data security management certification and application security certification work.”

We have every reason to expect a better personal information protection and data security governance environment under the co-governance model in China if more similar rules and policies are promulgated in the future and play a positive role in encouraging the government and enterprises to perform their respective duties.

VI. Connection between Rules and Basic Legal Theory

Laws are rules, the legal system comprises foundational legal theories and specific rules. In Europe, an integrated legal framework governing personal data processing activities dominated by the General Data Protection Regulation has been formed based on a basic human rights theory. The United States is supported by the Fair Information Practice Principles (FIPP), and takes a sectoral approach, which specifically includes the Federal Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA, also known as the Financial Modernization Act of 1999).

In China, however, the pace of establishment of a foundational theory for personal information and privacy data protection appears to be relatively slow. The Tort Liability Law in 2009 clarified

⁴ For a discussion of incentive-compatibility governance models, please see “*Exploring Personal Data Governance under Incentive-Compatibility Model*,” by Hanhua Zhou, Chinese Journal of Law, Issue 2, 2018. The author believes that under the traditional legal theory, the law is the order of the sovereign that must be observed, and the strict enforcement is its basic features. Therefore, the traditional legislative system is subject to mandatory enforcement, which is achieved in the form of prohibitive rules or obligatory rules, which require the governing subjects to or not to conduct the certain behaviors. This kind of rules has many drawbacks, including: the order will be generally ignored unless strong law enforcement is in place; the order may not match the market rules and curb market participants’ ability to innovate and legal compliance incentives due to information asymmetry; too extensive enforcement power may lead to issues including selective law enforcement or “law enforcement capture,” etc.

for the first time the legal status of privacy rights and the 2017 General Provisions of the Civil Law for the first time adopted a “dualistic” protection model for privacy and personal information. In general, however, a series of rules and regulatory documents that have been successively launched since the introduction of the 2017 effectiveness of the Cybersecurity Law, including the Data Security Measures and the CI Provisions, are basically a set of rules established under a principle of pragmatism that seeks to regulate the existing Internet ecosystem. With the completion of the personal rights section of the General Provisions of Civil Law, and the successive introduction of Personal Information Protection Law and the Data Security Law, the basic concepts and theoretical frameworks of personal information, privacy and data assets, etc. will become increasingly improved. We further believe that the government will establish a complete supervision system with theory and rules which coordinate effectively with each other.

The road is long, but the pace is firm and clear.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Min ZHU

Tel: +86-21-6080 0955

Email: min.zhu@hankunlaw.com