# CHINA LAW UPDATE

# CYBER PROTECTION OF PERSONAL INFORMATION IN A MULTI-LAYERED SYSTEM

Zhou Yuexin*

Table of Contents

I. INTRODUCTION ..... 160
II. THE REGULATORY TREND IN CYBER PROTECTION OF PERSONAL INFORMATION ..... 160
A. Information Security Technology – Personal Information Security Specification ..... 161
B. Guideline for Internet Personal Information Security Protection ..... 163
C. Draft Measures on Administration of Data Security ..... 165
III. DATA PROTECTION IN A "MULTI-LAYERED" SYSTEM ..... 166
A. Overview of Cyber Protection of Personal Information ..... 166
B. A Multi-Layered System: Better or Worse.? ..... 167
1. The Understanding of the System: Lessons from Practice ..... 167
2. The Tension between Innovation and Privacy Protection ..... 168
IV. CONCLUSION ..... 169

* ZHOU Yuexin, LL.B. candidate at Tsinghua University School of Law. Many thanks to Lin Meng, Song Jinyang and Lin Ziyu for their thoughtful feedback at various stages of this article, and the TCLR staff for careful editing. All errors are my own.

# CYBER PROTECTION OF PERSONAL INFORMATION IN A MULTI-LAYERED SYSTEM

Zhou Yuexin

## I. INTRODUCTION

In the past two years, to ensure the cyber data security and the legitimate rights of citizens, China has issued a series of regulatory documents to set the benchmark of data use. With the global focus on legislation of cyber data protection, the regulatory process manifested China's attempt to establish its own cyber data protection system.

This note will briefly introduce the development and status quo of cyber data protection in China. Part I introduces the regulatory development on cyber data protection driven by the three regulations. Part II, in the following, concludes the regulatory trend manifested by the three documents and discusses the multi-layered system established by them, including the reason to establish this system and how it works, and the tension between innovation and privacy protection underlying this system. This note concludes that there are problems when carrying out this system. Suggestions will also be given to address the problems.

## II. THE REGULATORY TREND IN CYBER PROTECTION OF PERSONAL INFORMATION

On May 1, 2018, *Information Security Technology-Personal Information Security Specification* (hereinafter referred to as the "*Specification*") issued by the Standardization Administration of China entered into force.[1] On April 19, 2019, China's Ministry of Public Security released the final version of *Guideline for Internet Personal Information Security Protection* (hereinafter referred to as the "*Guideline*") as a restatement and confirmation of the Standard. On May 28, 2019, Draft *Measures on Administration of Data Security* (hereinafter referred to as the "*Measures*") were issued by the Cyberspace Administration of China, along with a public

[1] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018).

consultation.[2] After being formally issued, the *Measures*, unlike the *Specification* and the *Guideline*, would become a binding regulation.

### *A. Information Security Technology – Personal Information Security Specification*

As a recommended national standard, the *Specification* is mainly a voluntary framework, not legally binding to courts nor mandatory to undertakings. However, it sets forth the benchmark for data collection under the 2016 *Cybersecurity Law of the People's Republic of China* (hereinafter referred to as 'Cybersecurity Law').[3]

It should also be noted that the *Specification* is never merely a practical and detailed version of *Cybersecurity Law*. It steps further, raising stricter requirements upon data collection. This progressive development mainly characterizes the following points.

Firstly, compared with *Cybersecurity Law*, the scope of personal information is expanded in *Specification* due to a different defining method. Article 76 of *Cybersecurity Law* defines personal information as all kinds of information recorded in electronic or other forms, which can be used to identify a natural person's personal identity.[4] Personal information under this definition includes but is not limited to name, date of birth, identity certificate number, biometric information, address and telephone number. Even though it is stated that the above list is inexhaustive, the scope of personal information, however, is undoubtedly narrowed down to a limited scope by the way it defines. The *Specification*, in contrast, defines personal information as including information reflective of both a natural person's identity as well as his activities.[5] In this regard, information like IP address is included and protected.[6] Additionally, the *Specification* adds a new category of personal sensitive information, including but not limited to ID number, transaction information and information of children under 14. Personal sensitive information is prescribed to enjoy a higher level of protection.[7]

---

[2] Shuju Anquan Guanli Banfa Zhengqiu Yijian Gao (数据安全管理办法征求意见稿) [Draft Measures for the Administration of Data Security] (promulgated by the Cyberspace Administration, May. 28, 2019), (CHINALAWINFO).

[3] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat' l People's Cong., Nov. 7, 2016, effective Jan. 1, 2017), art. 76(5) (CHINALAWINFO).

[4] *Id*. art. 76(5).

[5] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018), art. 3.1.

[6] *Id*. app. § A.

[7] *Id*. sec. 5.5, sec. 6.3.

Secondly, the rules of prior consent from individuals are detailed in the *Specification.* Article 41 of *Cybersecurity Law* mandated Internet companies to acquire prior consent to any collection of information.[8] Based upon this setting, the *Specification* further categorize requirements for different types of information collection. As to direct collection, where the data collector is the direct user of data, the collecting entity must notify the individuals of the type of information being collected and the detailed way of using it. Express consent of collection from the individual is required after the notification.[9] As to indirect collection, where the collector collects personal data from other data collectors, the collector should confirm the legitimacy of the original collection of information. And the individual's express consent to the share of information is also compulsory.[10] What is more, when collecting information from minors under 14, the explicit consent of their parents is required.[11] As to the collection of personal sensitive information, prior detailed, voluntary and explicit consent is a must.[12] If the users refuse to voluntarily provide such information, they could not be denied to access the "core business functions" provided by the collecting entity, which protects users from being forced to provide important information. It should be noted that, individual name is not categorized as sensitive information.[13] This leaves room for the real-name registration mandated by *Cybersecurity Law*, which stipulates that if an individual fails to provide a real name, the individual cannot get access to all the services.[14] But why individual name is not prescribed a higher level of protection requires justification since the misuse of individual name would cause identity risk, which satisfies the definition of personal sensitive information.[15] The reason for the preclusion of individual name is unclear in the *Specification*. And this could trigger the confusion that whether this is just to be in accordance with the real-name registration requirement set forth in *Cybersecurity Law*.

[8] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat' l People's Cong., Nov. 7, 2016, effective Jan. 1, 2017), art. 41 (CHINALAWINFO).

[9] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018), art. 5.3.

[10] *Id*.

[11] *Id*. art. 5.5 (c).

[12] *Id*. art. 5.5 (a), art. 5.5 (b).

[13] *Id*. app. § B.

[14] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat' l People's Cong., Nov. 7, 2016, effective Jan. 1, 2017), art. 24 (CHINALAWINFO).

[15] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018), app. § B.

Thirdly, the *Specification* establishes the principle of minimization. This is a clarification of the principle of necessity in the Article 41 of *Cybersecurity Law*. While the principle of necessity prohibits only irrelevant collection to the services provided by the network operators,[16] the minimization principle permits only personal information which is directly related to the realization of business functions of the products or services that cannot be otherwise achieved. By saying "minimization", the *Specification* looks not only at the features of the information, but also at the quantity and frequency of collections. should also be the minimum to realize the operational functions of the products or service.[17]

It could be concluded that, the *Specification* is aimed at promoting the implementation of *Cybersecurity Law*. But it also makes its own evolution on the basis of *Cybersecurity Law*, which marks a more detailed and rigid control on information collection.

### *B. Guideline for Internet Personal Information Security Protection*

After the launching of the *Specification* almost one year later, the *Guideline* was subsequently issued by the Ministry of Public Security, which is the main law-executor to crack down on cybercrimes and protect cybersecurity. The *Guideline* is important and referential to network operators when implementing *Cybersecurity law*.

Referring to the *Specification* as its "indispensable source",[18] the *Guideline* overlaps with the *Specification* in the use of terms and certain basic rules, for instance, *inter alia*, the principle of minimization.

But the *Specification* also makes its own progress, for example, by setting down the basic framework of the regulation in technical measures, which is not included in the previous normative documents. Under *Cybersecurity Law*, network operators shall take technical measures and other necessary measures to ensure the security of personal information collected by them, and prevent information leakage, damage and loss.[19] This general requirement indeed provides undertaking with leeway to a certain extent. But in

[16] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat' l People's Cong., Nov. 7, 2016, effective Jan. 1, 2017), art. 41 (CHINALAWINFO).

[17] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018), art. 5.2.

[18] Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Guideline for Internet Personal Information Security Protection] (promulgated by the Ministry of Public Security, Apr. 10, 2019, effective Apr. 10, 2019), sec.2 (CHINALAWINFO).

[19] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat' l People's Cong., Nov. 7, 2016, effective Jan. 1, 2017), art. 42 (CHINALAWINFO).

Section 5 of the *Guideline*, a whole system to safeguard data security is established.[20] Detailed stipulations targeting at different stages of data transmission, including the safeguard of telecommunications and network security, perimeter security, computing environment security and application and data security, ensure the confidentiality of data to a large extent. This is definitely an extension of *Cybersecurity Law*, and covers what is still left blank under the *Specification*.

It should be noted that, even though the concept of "personal sensitive information" is not raised in the *Guideline*, the *Guideline* also sets up a rigid standard to the collection and use of personal sensitive information. Particularly, network operators should not collect or process such sensitive information as race, ethnicity, political views or religious beliefs on a large scale. Collection of personal biometric information in its original form should also be avoided.[21] This new requirement is raised by the *Guideline* for the first time.

In view of all this, a comprehensive protection system is established under *Specification* and *Guideline*. The general clauses and principles in *Cybersecurity Law* are more practical with the supplementation of these two normative documents. However, differences still exist within them which may poses some obstacles when implementation. An obvious example is the setting of different exceptions to the mandatory consent of information collection. Eleven types of exceptions are listed as exceptions to user consent in *Specification*,[22] but only three in *Guideline*, two of which overlaps with the *Specification* [23] and fully automatic user profiling technology for precision marketing, search results ranking, personalized push news, targeted advertising and other value-added applications is a new exception set in the *Guideline*.[24] Even though the *Guideline* includes fewer exception clauses, the general permission of data use without consent, under the context of automatic user profiling technology in valued added applications,

[20] Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Guideline for Internet Personal Information Security Protection] (promulgated by the Ministry of Public Security, Apr. 10, 2019, effective Apr. 10, 2019), sec. 5 (CHINALAWINFO).

[21] Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Guideline for Internet Personal Information Security Protection] (promulgated by the Ministry of Public Security, Apr. 10, 2019, effective Apr. 10, 2019), sec. 6.1 (CHINALAWINFO).

[22] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018), art. 5.4.

[23] Hulianwang Geren Xinxi Baou Zhinan (互联网个人信息保护指南) [Guideline for Internet Personal Information Security Protection] (promulgated by the Ministry of Public Security, Apr. 10, 2019, effective Apr. 10, 2019), sec. 6.6(b), 6.7(b) (CHINALAWINFO).

[24] *Id.* Sec. 6.3(c).

does give undertakings the space to carry out a certain part of business. Other differences of the two documents center on the category of personal information and the requirement of technical measures. The inconsistency of the two documents raise confusion as to which to follow. This problem will be further discussed in the next section of this note.

### *C. Draft* Measures on Administration of Data Security

Issued by Cyberspace Administration of China on May 28, 2019, the Draft *Measures* just ended its open comment period and are about to release officially, after which they will gain legal force to the extent as departmental rules. The *Measures,* crystalizing the lessons acquired from the implementation of the previous normative documents, overlap with the *Specification* to a certain extent as well, thus giving legal effect to the previous voluntary framework. The release of Draft *Measures* could be viewed as confirmation of the continuing efforts to gain experience in implementing cyber data protection.

The *Measures* introduce similar regulations on notice and consent, data subject rights, personalized recommendations and target advertising, sharing of personal information and incident response.[25]

However, the *Measures* also introduce new requirements as to "important data", which is defined as "data that may directly affect national security, economic security, social stability, public health and safety once leaked". An inexhaustive list of important data includes unpublished government information, information related to a large population, genetic health, geography and mineral resources. Both the collection and processing of important data are rigidly controlled. Prior to data collection for business use, network operators are required to file their data collection practice to local cyberspace administration office.[26] And after the collection, measures including classification, backup and encryption should be taken to strengthen the protection of important data.[27] When publishing, sharing or trading with important data, in addition to evaluating the security risk, the undertakings are also required to ask for the permission of industry supervisor.[28]

---

[25] *China Releases Draft Measures for Data Security Management*, INSIDE PRIVACY NET (May 28, 2019), https://www.insideprivacy.com/uncategorized/china-releases-draft-measures-for-the-administration-of-data-security/.

[26] Shuju Anquan Guanli Banfa Zhengqiu Yijian Gao (数据安全管理办法征求意见稿) [Draft Measures for the Administration of Data Security] (promulgated by the Cyberspace Administration, May. 28, 2019), art.15 (CHINALAWINFO).

[27] *Id*. art. 19.

[28] *Id*. art. 28.

The *Measures*, in all, succeed from the *Specification* and is thus also closely related to the *Cybersecurity Law*. The guidance it provides throw light on the undertakings compliance with legal order.

## III. DATA PROTECTION IN A "MULTI-LAYERED" SYSTEM

### *A. Overview of Cyber Protection of Personal Information*

In accordance with from the above discussion, China has been devoted to accomplishing and improving its own system of data protection. With *Cybersecurity Law* as a general framework, the three normative documents offer more detailed benchmarks from the perspectives of different regulators. Since the *Specification* and the *Guideline* are lacking in legal force, they mainly formulate a voluntary framework as reference for undertakings, while the *Measures* may serve as a more important guideline to supplement the enforcement of *Cybersecurity Law*.

But as all these documents are made by regulators on network operators, there is actually a strong incentive for compliance because of the investigatory powers of these authorities over the infringements on personal data, which could lead to administrative sanctions. For example, in 2019, the Ministry of Public Security, the issuer of the *Guideline*, initiated the "Network Clearing 2019" campaign, which targeted at governing the applications misusing personal data. Administrative penalty and fine would be imposed on the offending undertakings. The normative documents made by them could be reflective of the standard of their action under Cybersecurity Law.

Therefore, it is not difficult to conclude that this system gives undertakings more instructions for compliance. As *Cybersecurity Law* is aimed at safeguarding the overall network sovereignty, it is not a conclusive and complete regulation of individuals' rights, namely data protection and privacy.[29] The supplementary system will definitely benefit the implementation of *Cybersecurity Law*, and inevitably, however, bring about a certain inconsistency and confusion as which to follow. As different documents categorize personal information in different ways and stipulate different level of protection, undertakings may have difficulty in following all the instructions at the same time. And just as mentioned above, the exception clauses also differ in each document. This could be hard for undertakings when they need legal justification. And if they need

[29] Sarah Wang Han; Abu Bakar Munir, *Information Security Technology – Personal Information Security Specification: China's Version of the GDPR*, 4 Eur. Data Prot. L. Rev. 535, 538 (2018).

to follow all the instructions, it seems necessary to have a single overall regulation instead of scattered ones.

Therefore, by making several normative documents supplementary to the *Cybersecurity Law*, China has established its unique multi-layered data protection system. The documents, issued in different stages, could be experimental tool adapting to the rapidly changing Internet. But it also raises other problems. Further discussion focuses on this unique system.

### *B. A Multi-Layered System: Better or Worse.?*

As illustrated above, China uses a multi-layered system on cyber regulation. This part will focus on why China establishes this particular system in data regulation and how it could work smoothly and effectively.

#### 1. The Understanding of the System: Lessons from Practice

The *Cybersecurity Law* was issued at the end of 2016, during exactly the period when China entered into the era of "4G+",[30] and the Internet is starting to play a more fundamental role in citizens' daily life. What's more, 2016 also witnesses the birth of a new generation of information and communication technology, represented by big data, intelligence, mobile Internet and cloud computing, which just began to fully and deeply integrated into all fields of the economy and society. This triggers the concern of how privacy could be invaded by the spread of technology.

Given this context, the *Cybersecurity Law* was deemed as important and necessary. However, standing at that point, the policy maker could hardly foresee the future with the rapid development of technology. Consequently, the word use in *Cybersecurity Law* is quite general so as to include as many likelihoods as possible, so that it can be able to respond to future conditions. By offering basic principles for the healthy Internet environment rather than detailed guidance for enterprises, the *Cybersecurity Law* gives the court more flexible space for discretion.

With the launching of European General Data Protection Regulation (hereinafter referred as "GDPR") issued in May, 2018, regulators all over the world accelerated the process of data regulation. In this regard, the *Specification*, which is also renowned as Chinese version of GDPR, came into birth. In this initial stage, the *Specification* offered network operators with a reasonable

[30] *2016 Nian Zhonguo Hulianwang Chanye Zongshu Yu 2017 Nian Fazhan Qushi* (2016年中国互联网产业综述与2017年发展趋势) [*China's Internet Industry Overview in 2016 and Development Trends in 2017*], XINHUA NET (Jan. 06, 2017), http://www.xinhuanet.com//info/2017-01/06/c_135961249.htm.

expectation and instructions to follow. It also makes sense why the *Specification* is only a recommended standard, since it serves as an experimental benchmark and practice model for enterprises. The result under this framework could be important and referential for the later normative documents. Too rigid compulsory obligations for network operators could hinder the process of innovation.

Therefore, when addressing the problems in the rapidly changing Chinese Internet market, regulators need more experimental experience and flexible framework instead of discretionary policy-making. The experience gained from the implementation of the *Specification* and the following normative documents filled the gap between policy and the reality, and could be the basis for the making of a guideline with legal force.

2. The Tension between Innovation and Privacy Protection

The tension between innovation and privacy protection also triggers the development of this multi-layered system.

The Internet industry is dynamic. Therefore, the rule-making process is always accompanied by the balancing test of national security, privacy and innovation. Such struggles could be clearly observed from the provisions. For example, article 7.4 of the *Specification* reads, when a personal information subject, the data of whom is collected, requests access to information which they have not voluntarily provided, personal information controllers can consider the request in a comprehensive manner, taking into account risk or harm to the subject's lawful rights and interests that could arise from not responding to the request, technical feasibility, cost, and other factors in carrying out the request. And after the decision is made, an explanation of the decision should be provided.[31] This is a compromise between undertaking interests and personal privacy. As in GDPR, the operators must provide the data users request though they could charge on that. This is an important part of right to access. Similarly, in *Guideline*, sensitive information as race, ethnicity, political views or religious beliefs should not be collected or processed on a large scale, but this is notably loose compared to GDPR, which bans the processing of sensitive data as a whole.[32]

It is not hard to conclude that personal data regulations are full of balancing test based on the goal of government. The details of a rule

[31] Xinxi Anquan Jishu Geren Xinxi Anquan Guifan (信息安全技术 个人信息安全规范) [Information Security Technology - Personal Information Security Specification] (promulgated by the Standardization Administration, Dec. 29, 2017, effective May.1 2018), art. 7.4.

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 9, 2016 O.J. (L 119) 1, 38.

might be the interest game between information collector and data subject. The multi-layered system indeed helps the accomplishment of the balancing. Lacking in the experience accumulated from case law and industry understanding, it's hard for our domestic courts to further explain and clarify the general rules set in *Cybersecurity Law*. For example, to interpret "business ethics", "good faith" and "social responsibilities",[33] a comprehensive observation and understanding of the industry ecology is undoubtedly required.

However, if the role of gap filling ultimately falls on the courts, who lacks the actual experience of this developing industry, the balancing might not be perfect. Therefore, the rule-making process of detailed rules could take this role. With rounds and rounds of discussion for *Specification*, *Measures* and *Guideline*, experts from all areas could be gathered together to find out the solution. The process of implementing these documents could also be a good chance for domestic courts to observe outcome and gain understanding. Only in this way could the judgements, especially those regarding the general clauses in *Cybersecurity Law*, accomplish the goal of protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization as set in Article 1 of *Cybersecurity Law*.[34]

## IV. CONCLUSION

This article basically focuses on the development of China's regulation on personal data protection under the context of *Cybersecurity Law*. Except for the regulatory innovations and a more rigid standard for data collection, this process characterizes the establishment of a multi-layered system of data protection.

This system brings about the benefits of experimenting and experience gaining; however, it also suffers from an inevitable inner inconsistency. The mixed and unclear system could negatively affect the realization of the goal in setting these documents. Because if enterprises are not willing to follow the rules, no experience could be gained at all. Therefore, to set up an integrated overall system of personal information is urgent. The multi-layered system could only be relied on temporarily. Therefore, the article asks for a reconciliation of the system and an integrated single legislation, which could benefit the undertakings from their undue burden of compliance.

---

[33] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law] (promulgated by the Standing Comm. Nat' l People's Cong., Nov. 7, 2016, effective Jan. 1, 2017), art. 9 (CHINALAWINFO).

[34] *Id.* art. 1.