JUNHE
SPECIAL REPORT

February 23, 2021

2021 FORECAST: THE TOP TEN NOTEWORTHY TRENDS AND ISSUES REGARDING DATA PROTECTION LAWS IN CHINA

Information technology has become increasingly involved in our business and daily lives. It supports economic growth and enhances the quality of our lives, but it also brings new challenges regarding compliance and security. The phrases "personal information", "data security" and "data production factors" are hot topics and are frequently used when describing economic growth and society. This article intends to review the major events related to data protection in 2020, analyze the trends of legislation and regulation regarding information protection and cybersecurity, and summarize the top ten noteworthy trends and issues forecast for 2021 in China.

I. Legislation will be fast tracked regarding the new Personal Information Protection Law and Data Security Law

On July 3, 2020, the *Data Security Law (Draft)* was released for public comment. On October 21, 2020, the *Personal Information Protection Law (Draft)* was released for public comment after being reviewed at the 22nd Session of the 13th NPC Standing Committee. The cutoff for public comment has now passed for both of these drafts. As the fundamental law in the field of data security, the *Data Security Law* will establish the basic rules and regulations governing data security protection. As the first law dedicated to governing personal information protection, the *Personal Information Protection Law* will establish a more solid, complete and systematic legal framework to protect personal information.

On December 21, 2020, when answering journalists' questions on the NPC's major legislative efforts in 2021, the spokesperson for the Legislative Affairs Commission of the NPC's Standing Committee said that the annual legislation plan for 2021 has been preliminarily adopted, and the Standing Committee will further review the drafts of the *Data Security Law* and the *Personal Information Protection Law* in 2021 and endeavor to promulgate them as soon as possible. [1] These two laws together with *Cybersecurity Law* will constitute the basic laws in the field of information and data in China. We suggest enterprises closely follow the legislative progress and development of these laws and their subsequent influence on enterprises.

II. Implementation of the Civil Code will provide solutions for personal information protection

The *Civil Code* came into force on January 1, 2021. It sets forth the definitions, protection requirements, civil liabilities and individuals' rights with respect to privacy and personal information protection in eight articles in Book Four - Personality Rights, as well as some other new

[1] See http://www.china.com.cn/zhibo/content_77033450.htm。

injunctions relating to personality rights. In order to further implement the *Civil Code*, the Supreme People's Court issued the first series of seven judicial interpretations of the *Civil Code* on December 30, 2020 and indicated that their next focus is the guidance of the research on the new additions and major revisions brought about by the *Civil Code*. In addition to the relevant content of the foregoing judicial interpretations, the Supreme People's Court will conduct thorough investigations and research on the new provisions and cases under the *Civil Code*, such as those regarding the judicial protection of personality rights including the individuals' voice, the individuals' privacy right and personal information, and then officially promulgate the relevant judicial interpretations.[2] The Supreme People's Court also issued the *Decision to Revise the Provisions on Causes of Action for Civil Cases*, adding cause of action for "personal information protection disputes" under "Personality Right Disputes"[3].

In recent years, several lawsuits regarding personal information protection have occurred. When the *Civil Code* had not yet come into force, and in the absence of the *Personal Information Protection Law*, it was difficult to bring civil lawsuits over infringements on personal information rights which do not constitute "privacy" due to difficulties in the application of the laws. Nowadays, given that the *Civil Code* has come into force and civil awareness for protection of personal information has aroused, and the judicial interpretations on personal information protection will be promulgated in the future, the number of lawsuits is expected to significantly increase. Enterprises will need to re-evaluate the risk of lawsuits regarding personal information protection alongside such development.

III. The regulation of online apps' personal information protection is constantly being strengthened

In recent years, the competent authorities have made thorough efforts in the regulation and enforcement of apps' personal information protection. We envisage that the regulation of online apps' personal information protection in 2021 will have the following features:

A combination of both central and local regulations. After the special rectification of online apps' illegal collection and use of personal information in 2019, the Cyberspace Administration of China ("**CAC**"), the Ministry of Industry and Information Technology ("**MIIT**"), the Ministry of Public Security ("**MPS**") and the State Administration for Market Regulations ("**SAMR**") ("**Four Ministries**") together launched the 2020 rectification inspection on July 22 last year. Meanwhile, provincial and municipal regulators have also gradually launched rectifications regarding personal information protection of apps based on their local situations and plans.[4]

Joint efforts of various regulators. The illegal collection and use of personal information by apps will still be mainly regulated by the Four Ministries. MIIT, MPS, SAMR and the Personal Information Protection Task Force on Apps (an organization established by the Four Ministries) will mainly focus on the regulation of the illegal collection and use of personal information by apps[5], while CAC will mainly focus on special rectification of non-

[2] See http://www.court.gov.cn/zixun-zhuanti-aHR0cDovL3d3dy5jaGluYWNvdXJ0Lm9yZy9hcnRpY2xlL3N1YmplY3RkZXRhaWwvaWQvTXpBd05NZ3RNSUFCQUEuc2h0bWw.html。

[3] See http://www.court.gov.cn/fabu-xiangqing-282031.html。

[4] In April 2020, the provincial counterparts of MIIT, MPS and SAMR and the provincial administration of communication in Jiangsu Province jointly issued a circular concerning special rectification of the illegal collection and use of citizens' personal information by apps through the entire territory of Jiangsu Province.

[5] In 2020, MIIT announced several batches of apps that had infringed upon the users' rights and interests and ordered the non-conforming enterprises to make corrections, and further ordered the removal of those apps that had not been corrected as required. The Personal Information Protection Task Force on Apps also issued circulars concerning the illegal collection and use of personal information by apps.

conforming content in an app's information.[6]

Further regulations in special industries and sectors. Regulators in various industries and sectors regulate an app's personal information protection based on the characteristics of their respective industries and sectors. For example, in the financial sector, the People's Bank of China ("**PBOC**") issued the *Notice concerning the Promulgation of Financial Sector Standards for Improving Financial User-End Apps Security Management* in 2019, requiring the National Internet Finance Association of China ("**NIFAC**") to implement the filing and registration of financial apps on a real name basis. As of December 2020, NIFAC had announced five batches of the filed apps. In the education sector, the Ministry of Education promulgated the *Regulations on the Filing of Education-Related Mobile Internet Apps*, requiring entities to complete the filing of their existing education-related mobile apps from December 1, 2019 to January 1, 2020 and then make the filed information available to the public.

Reasonably extending the scope of regulation. Presently, in addition to the fight against the illegal collection and use of personal information by apps, regulators have extended the application of apps' rules and regulations to mini-programs and Quick App and incorporated mini-programs and Quick App into their scope of regulations. In accordance with the *Guidelines for Cybersecurity Standard Practice - Guidelines for Self-Evaluation of Mobile Internet Application (App) on Personal Information Collection and Use*, app operators and operators of mini-programs and Quick App may also conduct self-evaluation by reference to the applicable provisions of these guidelines. MIIT's rectification also involves the evaluation of mini-programs and Quick App. Therefore, mini-programs and Quick App are likely to be gradually incorporated into the scope of regulation.

IV. Pilot implementation of localized data protection rules

More rules and regulations are being localized based on local demands. In 2020, local governments made exploratory and innovative efforts in the legislation of information protection laws and formulated more specific guidelines or regulations to the extent permitted by law. For example, on July 15, 2020, the Justice Bureau of Shenzhen Municipality promulgated the *Data Regulations of Shenzhen Special Economic Region (Draft for Comment)*, raising the concept of "data rights" for the first time. It emphasized that individuals are entitled to rights in their personal data and set forth a series of rules on personal information collection and use. On July 30, 2020, the local office of CAC in Tianjin Municipality issued the *Interim Regulations of Tianjin Municipality on Data Trading (Draft for Comment)*, setting forth the obligations of data traders and data trade service agencies in data trading activities. The *Social Credit Regulations of Tianjin Municipality* were officially adopted on December 1, 2020 and implemented as of January 1, 2021. These regulations prohibit enterprises, public institutions, industrial associations and chambers of commerce from collecting facial images, fingerprints, voices and other biological identification data.

In the future, local governments may promulgate advanced policies and regulations on data protection. Therefore, enterprises need to keep abreast of local regulations in addition to national laws and regulations.

V. More thorough and detailed rules regarding data protection will be promulgated

[6] For example, as of November 5, 2020, OCCA organized and carried out special rectification of non-conforming content in mobile applications, and 105 illegal apps were rectified.

in various sectors

The regulators of various sectors and industries, especially strictly regulated ones, will further establish personal information protection regulations that are particularly relevant to their own sectors and industries. For example, in the financial sector, Chen Yulu, the vice president of PBOC, said at the regular briefing on the State Council's policies on December 25, 2020 that PBOC will promulgate *Interim Regulations on Personal Financial Information Protection* in accordance with *Personal Information Protection Law*, *Data Security Law* and other new national laws to be issued, so as to reinforce the regulation of personal information use in the financial sector.[7] In the field of facial recognition, the use and development of facial recognition technology has brought a lot of new changes to personal information protection, but so far the *Personal Information Protection Law (Draft)* has only roughly set forth the requirements on the collection of images and the use of personal identification devices. The Legislative Affairs Commission of the NPC's Standing Committee indicated at a press conference that they will further consider public comments and carry out thorough research on the relevant issues. Given this, as well as the fact that the first facial recognition case in China is still pending, we cannot rule out the possibility that legislators will promulgate special regulations to govern the use of facial recognition technology and set forth requirements regarding personal information collection and use with such technology in the future.

VI. Standards and guidelines will become systematic

As the relevant legislations are accelerated, the national, industrial and organizational standards and guidelines have gradually become systematic and may be used as a reference by enterprises for the purpose of compliance.

When discussing the developments in national cybersecurity policies and standardizations, Guan Xiaoli, the deputy general secretary of the National Information Security Standardization Technology Committee ("**TC260**"), said that TC260 issued 53 national standards and initiated 64 different research and promulgations with respect to cybersecurity in 2020. These involved biometric recognition of faces, genes, gait, voiceprints, as well as other important areas of concern such as online shopping, instant messaging, online payments, and online car-hailing.[8] Moreover, TC260 promulgated several guidelines for cybersecurity standards in practice, such as the *Guidelines for Apps Self-Assessment on Collection and Use of Personal Information* and the *Common Issues on Mobile Internet Application (App) Personal Information Protection and Guidelines for Response to These Issues*. These guidelines are standards-related technical documents, intended to provide guidelines for standards in practice based on cybersecurity laws, rules, policies, standards, hot topics and events. On December 25, 2020, MIIT promulgated the *Guidelines for Building Data Security Standards System for Telecommunications and Internet Sectors*, proposing to issue more than 20 data security standards in 2021 to preliminarily establish a data security standards system for the telecommunications and internet sector.

Therefore, more standards and guidelines for information protection and data security are expected to be promulgated in the future. This means that the regulatory requirements and regulations on data protection are inclined to be more detailed and more practical on the one hand but will lead to more difficulty for enterprises for

[7] See http://www.gov.cn/xinwen/2020zccfh/49/index.htm。

[8] See https://mp.weixin.qq.com/s/1xs0s9Devx9V1H_xTD5XOg。

the purpose of compliance in practice.

VII. Regulatory requirements on cross-border data transfers will become more certain and clearer

Cross-border data transfer has become a focus in business development and the data compliance of domestic and foreign enterprises. The *Personal Information Protection Law (Draft)* establishes a complete regulatory system for the cross-border transfer of personal information. Compared with the security assessment requirements under the previous draft, this draft law sets out the different requirements for legal basis for the cross-border transfer of personal information (including a security assessment) upon full consideration of an enterprises' needs for cross-border data transfers in their business operations. Therefore, the regulatory requirements on cross-border data transfer becomes more certain and clearer. But how to interpret and implement these statutory provisions in practice, such as how to understand the necessary requirements and how to conduct personal information protection certification, are still subject to further observation.

Regulators first conducted pilot regulations of cross-border data transfers in some regions in 2020. For example, the *General Pilot Plan for Full and Thorough Innovation and Development of Service Trade* promulgated by the Ministry of Commerce on August 14, 2020 contemplated conducting a full and thorough innovation and development of the service trade in 28 provinces and cities, including exploring modes to regulate cross-border data transfer on a classified basis in some pilot regions, so as to carry out pilot cross-border data transfer security regulation. The Shanghai Free Trade Zone and the Beijing Free Trade Zone also promulgated documents with respect to pilot cross-border data transfer regulation. Whether and how these pilots will be implemented in 2021 are noteworthy in the regulatory practice of cross-border data transfer.

VIII. "MLPS" and "CII Protection" requirements will be gradually implemented

On July 22, 2020, the MPS promulgated the *Guidelines for the Implementation of Cybersecurity Classified Protection System and Critical Information Infrastructure Security Protection System* ("**Guidelines**"), emphasizing the implementation of a cybersecurity classified protection system (or the multi-level protection system, "**MLPS**") and a critical information infrastructure security protection system ("**CII Protection**"). So far five national standards for MLPS 2.0 have come into force. Also, on August 10, 2020, the *Information Security Technology – Method to Identify Critical Information Infrastructure (Draft for Comment)* was released, providing a reference for critical information infrastructure operators. The Guidelines expressly state that regulators and supervisors of public communication and information services, energy, transportation, water resources, finance and other important sectors and industries shall promulgate critical information infrastructure identification rules for their own sectors and industries and then have such rules filed with the MPS. They shall also be responsible for the identifications thereunder.

As stated by the MPS at the "2020 Cybersecurity Standards Forum" on December 28, 2020, the *Regulations on Critical Information Infrastructure Security Protection* referred to in the legislation plan for 2020 will be promulgated, and the *Regulations on Classified Protection of Cybersecurity* will also be further researched and promulgated as soon as possible.[9] This means that the relevant regulations on MLPS and CII Protection are expected to be duly promulgated

[9] See https://mp.weixin.qq.com/s/1xs0s9Devx9V1H_xTD5XOg。

and implemented in the upcoming year. Meanwhile, regulators will further enforce the regulation of enterprises in practice. We suggest enterprises closely follow the progress of the relevant developments.

IX. Data leakage may occur more frequently and more enterprises will be affected

In the past year, various cases of data leakage have occurred due to failures of internal management, protection measures and other issues and have attracted much negative public attention. This should remind enterprises of the importance of data security and the prevention of data leakage for the purpose of data compliance.

We found when reviewing typical data leakage cases in 2020 that some enterprises leaked their users' information without authorization due to improper management or a failure to strictly implement relevant personal information protection regulations. For example, China CITIC Bank was condemned by the public and was investigated by the China Banking and Insurance Regulatory Commission due to its disclosure of the account transaction information of a talk show host to their former employer without their authorization.[10] In another example, an employee of YTO Express leased an employee's internal account to criminals, so that the criminals stole the users' personal information and further sold it on.[11] Some enterprises were maliciously attacked and their personal information was stolen due to their failure to take proper technical measures for security protection. For example, Weibo admitted in March 2020 that personal information uploaded by their app users was leaked [12] due to a malicious call by the users' query interface. As a result, Weibo was investigated and ordered by MIIT to take effective protective measures to eliminate future potential data security risks.

It is a basic responsibility of the network operators to perform cybersecurity protection obligations and prevent the occurrence of data leakage and other cybersecurity accidents. Given that the regulators have become increasingly strict in law enforcement with respect to the performance of cybersecurity protection obligations by network operators, and further given various data security accidents occurred last year, we suggest that enterprises take heed of such accidents and fully perform cybersecurity protection obligations and prevent data leakage.

X. Data monopoly

"Data monopoly" will be a hot new topic in the upcoming year. On November 10, 2020, SAMR issued the *Guidelines for Antitrust in the Field of Platform Economy (Draft for Comment)* ("**Antitrust Guidelines**").

The Antitrust Guidelines prohibit platforms from using data and algorithms to enter into monopoly agreements. They also prohibit platform operators of facilities that are necessary for data control and other platform economies from refusing to conduct transactions with counterparties on unreasonable conditions. Furthermore, the Antitrust Guidelines prevent platforms from leveraging their dominant position to misuse users' personal information, such as "using big-data analysis to disadvantage existing customers", as well as the mandatory collection and use of personal information and other violations of personal information protection regulations. With the release of the Antitrust Guidelines, law enforcement authorities are more active in the field of platform economies. On December 14, 2020, SAMR began to investigate Alibaba's suspected conduct of monopolization

[10] See http://www.cbirc.gov.cn/cn/view/pages/ItemDetail.html?docId=903298&itemId=925&generaltype=0。

[11] See https://static.nfapp.southcn.com/content/202011/25/c4344441.html。

[12] See https://static.nfapp.southcn.com/content/202003/19/c3288072.html。

due to its “select one from two options” request or other misuses of its dominant position in the market according to the law. This reflected the general trend in further strengthening antitrust regulations in the field of platform economies. “Using big-data analysis to disadvantage existing customers” and other abuses of a dominant position in the market may become the focus of regulation in the coming year. As an overlap of the areas between antitrust law enforcement and data law enforcement, data monopoly laws are noteworthy.

Our observation

The public has become increasingly concerned about privacy protection and data security. Accordingly, legislation and the enforcement of data related laws are being developed quickly, particularly in the last 12 months. In 2021, the data protection regulatory system in China is expected to be further improved and reinforced, and data compliance issues will become more important to enterprises. Together with businesses we will closely follow up the changes and developments in legislation and the enforcement of data protection laws and promptly provide constructive advice to our clients.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Chao GUO	Associate	Tel: 86 10 8553 7733	Email:guoch@junhe.com
Junjie DONG	Associate	Tel: 86 10 8540 8722	Email:dongjj@junhe.com

(Many thanks to Peng Jian, a member of the translation team of our firm, for her great support for the English translation of this report.)