ECIJA

November 2020

Keeping up with China: thoughts and legal updates

ECIJA's China Desk Newsletter

www.ecija.com

ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

China: what legal updates do business need to know?

ECIJA's China Desk Newsletter - November 2020 – Nº 1

Content

1. Legislation roundup

- ### China's Export Control Law published. It establishes a unified export control regime

On October 17, 2020, the Standing Committee of the PRC's National People's Congress approved the Export Control Law of the People's Republic of China (**ECL**), which will come into effect on 1 December 2020. It is China's first comprehensive and unified export control law, and introduces various control mechanisms that resemble certain aspects of the US export control regime. The ECL will likely have a wide impact on businesses involved in the trading of items subject to the export controls.

- ### New Release: First Draft of Personal Information Protection Law

On October 21, 2020, the National People's Congress ("NPC"), China's top legislative body, released its first draft of the Personal Information Protection Law (the "Draft Law") for public comment (official Chinese version available here). The period for public comment ends on November 19, 2020 and comments can be submitted through NPC's official website.

As the country's first comprehensive law in the area of personal information protection, the Draft Law aims to "protect the rights and interests of individuals," "regulate personal information processing activities," "safeguard the lawful and orderly flow of data," and "facilitate reasonable use of personal information".

Although bearing a resemblance to the European Union's ("EU") General Data Protection Regulation ("GDPR") and other recent privacy legislation in major jurisdictions in some important areas, the Draft Law introduces a number of provisions that are consistent with recent trends in other Chinese laws in the areas of data and technology, such as the draft Data Security Law and the newly enacted Export Control Law. These include, for example, rules establishing extraterritoriality of the Draft Law and a "blacklist" that would restrict or prohibit listed foreign organizations from receiving personal information from China.

- ### Changes in Trade Secrets' Protection in China

On September 4, 2020, the Chinese State Administration for Market Regulation (SAMR) released a new set of proposed rules that may increase protections for trade secret holders. SAMR is now seeking comments on the draft rules.

The old rules were criticized for not going far enough. One issue with the existing trade secret regulations was that they limited protections to Chinese citizens. The new rules extend the protections to foreigners. The new provisions also provide more clear and broader definitions for "trade secrets," "business information" and "commercial information." Regarding infringement, the new provisions place the burden of proof on

the defendant after the plaintiff makes out a prima facie case. This is designed to improve and streamline the enforcement scheme.

The changes may reflect China's growth from a developing country to one of established economic expansion. China may finally be recognizing that its investments in education and innovation will require the protection of intellectual property rights in order for its economy to expand further.

- **China signs off on PRC Biosecurity Law**

On 17 October 2020, the Standing Committee of the PRC National People's Congress ("NPC") passed the PRC Biosecurity law which will become effective on April 15, 2021 (the "Biosecurity law").The Biosecurity law establishes a comprehensive legislative framework for the somewhat piecemealed pre-existing regulations in the following areas:

- epidemic control of infectious diseases for humans, animals and plants
- research, development, and application of biology technology
- biosecurity management of pathogenic microbials laboratories
- security management of human genetic resources and biological resources
- countermeasures for microbial resistance
- prevention of bioterrorism and defending threats of biological weapons

The highlights are that (i) strengthens regulations on the conduct of biotechnology research and development activities in China; (ii) it aggravates the penalties for illegal conducts and (iii) launches a management system for controlled essential equipment and special biological agents.

- **Announcement on Entry by Foreign Nationals Holding Valid Chinese Residence Permits of Three Categories**

On 23 September 2020, the Ministry of Foreign Affairs and National Immigration Administration of the People's Republic of China published the new entry measures for foreigners, and established: In view of the current COVID-19 situation and the need of epidemic prevention and control, adjustments are now made to the Announcement by the Ministry of Foreign Affairs and the National Immigration Administration on the Temporary Suspension of Entry by Foreign Nationals Holding Valid Chinese Visas or Residence Permits issued on 26 March 2020.

Effective from 0 a.m., 28 September 2020, foreign nationals holding valid Chinese residence permits for work, personal matters and reunion are allowed to enter China with no need for applying for new visas. If the above three categories of residence permits held by foreign nationals expired after 0 a.m., 28 March 2020, the holders may apply for relevant visas by presenting the expired residence permits and relevant materials to the Chinese embassies or consulates on the condition that the purpose of the holders' visit to China remains unchanged. The above-mentioned personnel shall strictly abide by the Chinese regulations on epidemic prevention and control.

Other measures in the Announcement issued on March 26 will continue to be implemented. While ensuring effective epidemic control, the Chinese government will continue resuming people-to-people exchanges in a step-by-step and orderly manner.

2. Jurisprudence

- **Chinese Court Decision Reinforces Need for Clear and Precise Drafting of China-Related Arbitration Agreements**

In a dispute between Hebei Zhongxing Automobile Manufacturing Co., Ltd. (HZAM), a Chinese company, and Automotive Gate FZCO (FZCO), a UAE company, the Shijiazhuang Intermediate People's Court declared invalid two related arbitration agreements that provided for arbitration in accordance with the Arbitration Rules of the International Chamber of Commerce (ICC) and to be held "in China".

The decision of the Shijiazhuang Intermediate People's Court highlights the need for parties to draft clear and precise arbitration agreements that concern Chinese parties, a seat in China, Chinese law, or that may require enforcement in Mainland China. Contracting parties should state expressly and unambiguously basic elements of an arbitration agreement, including the seat of arbitration, the governing law of the arbitration agreement, the arbitral rules, and the administering institution. This is especially important because Chinese arbitration law does not follow the UNCITRAL Model Law and has certain differences that may lead to an arbitration agreement valid elsewhere to be declared invalid by a Chinese court.

3. Analysis

Factors to take into account regarding dumping and subsidies in the European Union for companies from third countries (China)

- **Anti-dumping measures**

The EU applies the principle of free trade, which creates jobs and wealth. However, this freedom to trade can be disrupted when countries unfairly subsidize products or produce above demand and sell at reduced prices in other markets.

This makes it difficult for other companies to compete and could lead to the closure of national businesses and layoffs. To protect companies and workers, the EU has the option of using anti-dumping and anti-subsidy measures.

Dumping is the practice in trade used by companies to lower their prices in such a way as to distort trade and prevent fair competition between other producers and endanger domestic production in the European Union.

The principles governing the application of anti-dumping measures in the European Union are set out in Regulation (EU) 2016/1036 of the European Parliament and the Council.

The principles governing anti-dumping control are as follows:

(i) **Universality**: The anti-dumping duty will be imposed on any dumped product causing injury in the Union by being released for free circulation.
(ii) **Comparison**: A product is dumped if the export price to the European Union in the ordinary course of trade is less than the price established for a like product in the country of export.
(iii) **Origin**: The country of export shall be the country of origin, or the intermediary, unless the products merely transit through the country or are not produced there, or where there is no comparable price for such products in that country (further qualification).

(iv) **Identity**: the like product means an identical product (which is alike in all respects), or alternatively, a product which has characteristics closely resembling those of the product under consideration, even if not identical.

- **Measures in the area of grants**

A subsidy is a financial contribution, such as a grant or loan, generally paid by the government of a country outside the EU, which confers a benefit on a company or industry importing its products into the EU and which distorts competition on the EU market. To offset this distortion and to establish fair competition, the EU can impose so-called countervailing duties on such imports.

The legal measures applied by the European Union to combat state subsidies are set out in Regulation (EU) 2016/1037 on anti-subsidy measures.

The purpose of the Regulation is to lay down the European Union's (EU) rules on defense against subsidized imports from countries outside the EU and the conditions for the application of countervailing measures, the main aspects of which are:

- A countervailing duty is applied to counteract the injurious effects of subsidized imports and to restore fair competition. The duty is borne by the importer and collected by the customs authorities of the EU country concerned.
- If an EU industry considers that imports of a product from a non-EU country are subsidized and are causing injury to the EU industry producing the same product, it can lodge a complaint with the European Commission.
- If the complaint provides initial evidence of a subsidy or injury to the EU industry and a causal link between the subsidy and the injury, the Commission opens an anti-subsidy investigation.
- The Commission may impose provisional countervailing duties pending further investigation.
- Following the reinvestigation, the Commission may impose definitive measures within 13 months, normally for a period of five years.

- **Links to information sources in the EU**

The European Union has extensive information available to any company in any country on its anti-dumping and anti-subsidy programs and measures. The main sources of information are the following:

- https://ec.europa.eu/trade/policy/accessing-markets/trade-defence/actions-against-imports-into-the-eu/anti-subsidy/
- https://ec.europa.eu/trade/policy/policy-making/
- https://ec.europa.eu/trade/policy/accessing-markets/

4. Legal opinion of the month

Highlights and Perspectives on China's Personal Information Protection Law Project

This content was powered by ECIJA's joint venture with Grandall Law Firm

The draft of the Personal Information Protection Law (hereinafter referred to as the "draft " was officially announced on October 21, 2020. As a law of great social interest, highly integrated in the development of technology and having a huge impact on the digital economy, the draft has attracted wide public attention and has raised debates among professionals. The provision of high fines "a fine of up to 50 million yuan or 5% of the previous year's turnover", as is the extraterritorial application of its provisions, the extension of individual rights, etc. This article will attempt to summarize only some of the highlights of the draft, and provide a preliminary overview of the law to analyze its impact on information protection compliance by companies, and will examine in more depth the key issues of the draft, such as the "informed consent" mechanism and the rights of individuals.

I. Summary and brief commentary on project highlights

1) Reaffirmation and enhancement of rights and interests in personal information

The draft law uses the concept of "interests of personal information", which follows the expression of the Civil Code and has not used the more controversial concept of "rights of personal information", but in chapter IV of the draft, "Rights in the processing of personal information" it still uses a series of "rights" such as the right to information, the right to make decisions, etc. Thus, although the legislator has chosen to use the concept of interests in personal information with caution for various reasons, it does not mean that the protection of these interests by the government is significantly weaker than other rights (e.g., the right to privacy).

2) First provision on extraterritorial application and requirements for personal information controllers outside China

Paragraph 2 of Article 3 of the draft provides for the applicable effect of this Law on the activities of foreign entities in processing personal information of natural persons in China, which covers activities aimed at providing products or services to natural persons in China (e.g., international sale of products on platforms such as Taobao), as well as activities aimed at analyzing and evaluating the behavior of natural persons in China (e.g., portraits of Chinese users, etc.). It also establishes a general provision of " Other circumstances provided by laws and administrative regulations". At the same time, in accordance with Article 52 of the draft, controllers of personal information outside the country who meet the requirements of this paragraph are also obliged to establish a specialized agency or appoint a representative in China and comply with the obligation to submit relevant information.

Regarding the effectiveness of extraterritorial application, in order to resolve possible jurisdictional conflicts, the European Data Protection Committee has published a "Guide on the territorial scope of the GDPR (Article 3)" in the process of implementing the GDPR, which is used to restrict and clarify the provisions on extraterritorial application. It is expected that in the future there will also be further detailed rules to determine the specific scenarios of extraterritorial application in China.

3) Broadening the definition of personal information

Article 4 of the draft defines personal information as "information recorded electronically or by other means in relation to an identified or identifiable natural person, excluding anonymous information", and differs from the definition of personal information in the Cyber Security Law and the Civil Code, which state that personal information is "any type of information that, alone or in combination with other information, may identify a natural person as an individual". In addition to excluding

anonymous information from the scope of personal information (anonymous information is defined in article 69 of the draft, which requires that it meet the criterion of "non-identifiable and unrecoverable"), it also broadens the scope of the definition, including the scope of information "related to" natural persons.

Since the publication of the draft, there have already been voices from the legal and business sectors requiring that the definition of personal information in the draft should be coordinated as closely as possible with the provisions of the Cyber Security Law and the Civil Code. It is believed that the debate on the definition of personal information will continue next year until the Personal Information Protection Law is officially adopted.

4) Introduction of the figure of the controller of personal information

The draft introduces the concept of "personal information processor" as a central figure who fulfills the obligation to protect personal information, and defines it as "a person who independently determines the purpose, form of processing and other matters related to the processing of personal information", a figure similar to the GDPR Data Controller.

Unlike the GDPR, the draft does not establish the concept of Data Processor, but regulates the possible processing of data by specific provisions in scenarios such as joint processing, delegated processing and providing data to third parties. It remains to be seen whether such regulation is sufficient to regulate the widespread presence of "fiduciaries" who may be, to some extent, much more powerful from a technological and financial point of view than personal data processors.

5) Broadening the legal basis of the treatment of personal information

Article 13 of the draft establishes six legal bases for the treatment of personal information, adding, in addition to the general concept of " consent ", that is necessary for the fulfillment of a contract, for the performance of a legal duty or obligation, for responding to a public health emergency or, in the event of an emergency, for protecting the life, health or property of a natural person, or for journalism and the monitoring of public opinion in the public interest. With the possibility of withdrawing consent (Article 16 of the draft), we believe that, of the above-mentioned bases of legality, for the performance of contracts and for the fulfillment of legal duties or legal obligations, they will have a great margin of implementation after the application of the future law.

At the same time, the provisions on the basis of legality required to respond to public health emergencies are also appropriate for the collection and use of personal information during this year's epidemic prevention and control. However, although articles 33 to 37 of the draft already provide for the treatment of personal information by State administrations, but it is only applicable to State administrations, it seems impossible to directly regulate issues such as inadequate reporting, collection of irrelevant information and leakage of data that may exist during the prevention and control of this year's epidemic.

6) Attempts to establish a consent mechanism

The consent mechanism is the most important legitimate basis for the treatment of personal information, the draft establishes a series of requirements, in addition to

general consent, it also establishes requirements such as individual consent, written consent, special consent, reacquired consent, etc.

Of course, the premise of consent is voluntary and informed (see the GDPR requirement of "free, clear, informed and clear through statements or positive actions"), to solve the problem of compulsory consent and forced consent, Article 17 of the draft provides that "the personal Information controller may not refuse to supply a product or service on the grounds that the person has not consented to provide personal information or has withdrawn his consent for the treatment of personal information; except where the treatment of personal information is necessary for the supply of the product or service". The scope of this prohibition to provide services or products (for example, whether it includes discriminatory pricing) and the interpretation of whether the information is "necessary" for the provision of the product or service is not be determined yet. It is believed that the provisions of standards such as "Information Security Technology: Basic Regulations on the Collection of Personal Information through Mobile Internet Applications (Apps)" may provide some guidance for subsequent legislative and enforcement work.

With respect to children's personal information, the draft seems less stringent than the "Regulations on the Protection of Children's Personal Information on the Internet" since it has added a requirement that the personal information controller "knows or should know", which seems to leave space for the personal information controller's exemption from liability. However, it is necessary to pay attention to the convergence with Article 72 of the recently approved Law on the Protection of Minors: "Those responsible for handling the personal information of minors on the Internet shall abide by the principles of legality, legitimacy and necessity. When handling the personal information of minors under the age of fourteen, the consent of the parents or other guardians of the minors is required, unless otherwise provided for by laws and administrative regulations". At the same time, the "know or should know" rule does not exist in foreign legislation, such as the GDPR, and its limits should be further clarified in the future.

7) Clarification of the concept of sensitive personal information

The concept of sensitive personal information has been mentioned by congressmen and academics during the debate of the Civil Code, and was previously stipulated in the "Information Security Technology: Personal Information Security Regulation". The draft has followed the criteria and definition of sensitive personal information of this regulation.

It is worth mentioning that article 27 of the draft provides for the installation of image capture and personal identification devices in public places, which has already provoked a strong debate in society. Although the draft already requires the installation of visible signs and the purpose is limited to public safety, this article seems to lack the necessary supervising authority, and the scope of "public safety" is too broad. In practice, there is a possibility that this could be interpreted as a permissive clause.

8) Establishment of rules for the cross-border transfer of personal information

Thanks to the development of cloud technology, the Internet of Things, the blocks chain and other technologies, the cross-border flow of data has become a major act affecting national sovereignty and security, international trade and information exchange. Several events in the technology sector of this year, such as the cloud in

Guizhou and the blocking of Tok-tok in the United States, have been related to the cross-border transfer of data.

Establishing standards for the cross-border transfer of personal information is the main focus of this draft. In addition to establishing special provisions on the behavior of government administrations, critical information infrastructure operators, and personal information controllers which handling personal information up to the amount specified by the national department of networks and telecommunications, the project also establishes provisions for personal information controllers transmitting personal information across borders due to business needs, requiring the establishment of security assessment measures, certification of personal information protection, and the signing of contracts that meet compliance requirements.

It should be noted that while international cooperation is encouraged (draft articles 12 and 41), the draft also maintains countermeasures against political discrimination and non-compliance (draft articles 42 and 43).

9) Compliance requirements for personal information controllers

The draft establishes a special section on the organizational and technical measures to be taken by personal information controllers to fulfil their personal obligations, and requires that controllers who handle personal information up to the amount specified by the State Information Agency on the Internet, should appoint a personal information protection officer and fulfil the corresponding obligation to communicate such information to the relevant authorities. At the same time, the draft also requires that personal information controllers must carry out prior risk assessments of their processing, as well as personal information security audits.

In addition, it remains to be seen whether the above-mentioned person (officer) in charge of personal information protection will become a "directly responsible supervisor and other directly responsible persons" under the section on legal liability, and thus assume personal responsibility.

10) Strengthening administrative supervision and civil indemnification measures

The draft follows the previous practice of general coordination of the Internet and Telecommunications Department and the specific responsibilities of the relevant departments in each industry, and there is a need to further complicate the way in these measures are coordinate between different department, as well as the specific way for individual complaints. However, the draft gives departments responsible for the protection of personal information the power to conduct on-site inspections, inspect and copy relevant materials, and seize and seal relevant equipment and items, providing those departments with more effective weapons in addition to traditional interviews.

On the civil indemnification issues, the draft provides for the determination of liability based on the loss of the affected person or the gain of the personal information controller, but in practice there may be many difficulties in proving such loss or gain. In similar cases in the United States, causation and burden of proof have also become major points of controversy, and we believe that further refinement of the specific rules will be necessary in the future. In addition to individual claims, the project also provides a mechanism for the prosecution of public interest litigation, but how this will relate to the current public interest litigation system is still under discussion.

II. Conclusion

Although the project has been based in many ways on the GDPR, it also makes adaptations based on current administrative and regulatory practices in China and the realities of the data industry in China. In general, the project imposes more stringent compliance requirements on personal information controller, including requirements for organizational and technical measures, as well as contingency plans, personal information security assessment and auditing, etc. It is expected that companies will face greater challenges following the adoption of the Personal Information Protection Law and the Data Security Law in the future, and must respond in advance.

Author
Mr. Che Jie
Executive Partner, Grandall Law Firm
Mr. Che Jie is deputy of the 13th National People's Congress, executive partner of Grandall Law Firm, managing partner and party secretary of Grandall Nanjing, vice president of the Jiangsu Bar Association, and president of the Jiangsu Bankruptcy Administrators Association.

Mr. Fu Xin
Partner, Grandall Law Firm Nanjing
Mr. Fu Xin is currently member of the Internet and High Technology Committee of the All Chinese Lawyer Association, member of the E-Commerce Legal and Information Network Committee of the Jiangsu Bar Association, and member the Legal Services Committee of the Jiangsu Internet Association.

China Desk
+ 34 917 81 61 60
info@ecija.com
www.ecija.com


ECIJA
EXPANSIÓN
2016, 2017,
2018 & 2019
Most innovative Project
Best Economy
Digital Firm
FT
FINANCIAL TIMES
FINANCIAL
TIMES
2019
Among the 20
most innovative
European Firms
TOP RANKED
Chambers
EUROPE
2019
The LEGAL 500
-2019-
Band 1 in TMT by
Chambers & Partners
and Legal 500
THE LAWYER
2019
Best TMT
European Firm
Forbes
FORBES
2017
Best Technological
Spanish Firm
Torre de Cristal
Pº de la Castellana, 259C
28046 Madrid