Cybersecurity obligations of ICT Companies in P. R. China

PhD Shenkuo Wu *

Abstract

With the fast development of new generation of ICT technologies, the entire Chinese community is in front of numerous opportunities and, at the same time, is also forced to face various risks. Under this emerging perspective, among others, the issue of cybersecurity obligations of ICT companies in China is becoming much more relevant and the undergoing debates on this can deeply help to understand better the real logic and approach of the actual Chinese cyber governance. In fact, as an important characteristic, the current numerous Chinese dispositions related to cybersecurity governance are basically provided at three levels, the systematic study of which helps to provide a complete insight on the effective cybersecurity obligations of ICT companies in China. Meanwhile, in practice, the before-mentioned multi-level cybersecurity obligations cannot be interpreted beyond the numerous institutional limitations already rooted in the current Chinese legal system, as the rational balance between the industry developments and the security interests, as well as the strict proportionality between the rights and the obligations, are always the top priority of the Chinese regulation approach in this area.

Keywords: *Cybersecurity obligations, ICT companies, China*

I. Introduction

In nowadays P. R. China, with the fast development of new generation of ICT technologies, the entire Chinese community is in front of numerous opportunities and, at the same time, is also forced to face various risks[1].

On one hand, thanks to the new technologies, the Chinese community can get benefits at three levels: (1) obtaining new technical supports, especially from big data, AI, etc.; (2) introducing new operation models, including cloud computing, IoT etc.; and (3) developing new business applications, such as eHealth, eLife, eFinance, etc.

On the other hand, the Chinese community is constantly suffering from more and more serious risks, which reflect at three levels as well: (1) new technical offences, such as virus, DDos attack, etc. (2) new organizational offences, especially ICT fraud, etc.; *and* (3) new content offences, including child pornography, terrorist propaganda, etc.

Indeed, from the year of 2014, China has started to accelerate its own policy and legal framework improvements, with the double purpose of promoting the digital economy development as well as enhancing the cybersecurity capacity building.

Under this emerging perspective, among others, the issue of cybersecurity obligations of ICT companies in China is becoming much more relevant and the undergoing debates on this can deeply help to understand better the real logic and approach of the actual Chinese cyber governance.

---

* *Associate Professor of Law School of Beijing Normal University, P. R. China.* *This research is supported by National Social Science Foundation of China (15CFX035).*

[1] On the scenario of ICT related opportunities and risks, see Zhang Boqin-Sun Shuyang, 2019 *Development Trend Prospects of Network Security in China*, in Cyberspace Security, 2019, no. 1, p. 37.

II. Policy and Legal Framework on Cybersecurity Obligations of ICT

Companies

In fact, as an important characteristic, the current numerous Chinese dispositions related to cybersecurity governance are basically provided at three levels: (1) the Policies; (2) the Legislations; and (3) other Norms.

Generally speaking, from the point of view of their functions, the Policies establish the *core values* pursued in the area of cybersecurity, the Legislations introduce the systematic rules as the essential *legal institutions*, and other Norms offer the more detailed *operational indications* for the further implementations:

1. Main Policies related to cybersecurity governance

Facing the cyber governance issues, the Chinese policy maker tries constantly to achieve the better balance between the development (digitalization) and the security (cybersecurity) as two basic values:

(1) The *„Internet Plus" Action Plan*[2], issued by the State Council on 4 July, 2015, strengthens the integration between the Internet related innovations and the traditional social-economic elements, as well as the necessity to enhance the cybersecurity through the improvement of the standard norms, the legal norms, the security awareness and the security managements.

(2) The *National Strategy for the Big Data*[3], issued by the State Council on 31 August, 2015, highlights the multi-benefits that the big data innovations can bring to the people, as well as the importance to guarantee the cybersecurity through the integration among the updated policies, legislations, standardizations, market development mechanisms, financial supports, talents educations and international cooperations.

(3) The *13th National Five-Year Plan for Informatization*, issued by the State Council on 15 December, 2016, considers the cybersecurity as the basis for the development and strengthens the high relevance of joint efforts of the governments, industries, civil societies and individuals for the safeguard of cybersecurity.

(4) The *Development Planning for the New Generation of Artificial Intelligence*[4], issued by the State Council on 20 July, 2017, highlights not only the great opportunities but also the serious security risks connected to the application of AI, and promotes the AI regulation through the ad hoc technical, legal and moral norms as well as the cooperations among the public and private stakeholders for the continuous risk assessment.

(5) The *National Cyberspace Security Strategy*[5], issued by the Cyberspace Administration of China on 27 December, 2016, establishes the targets, principles and tasks for the cybersecurity building, and declares the high necessity of rule of law for the open and transparent Internet governance, as well as the importance of the public

---

[2] On the practical perspective of „Internet Plus" Action Plan, see Li Congyuan, *Future of „Internet Plus" Action Plan*, in Information Research, 2018, no. 2, p. 95.

[3] On the logic of the National Strategy for the Big Data, see also Liao Jingwei-Yu Juan, *Research on the Big Data Industry*, in Modern Business Trade Industry, 2018, no. 6, p. 7.

[4] Related to the AI planning in China, see Yuan Hui, *Studies on the Development Planning for the New Generation of Artificial Intelligence*, in Tech Wind, 2018, no. 31, p. 37.

[5] On the approach of the National Cyberspace Security Strategy, see also Wang Kewei-Zheng Zai, *Analysis on the National Cyberspace Security Strategy*, in Digital Communication World, 2019, no. 2, p. 115.

private partnership for the further harmonization between the development and security interests.

(6) The *International Strategy of Cooperation on Cyberspace*[6], jointly issued by the Cyberspace Administration of China and Ministry of Foreign Affairs on 1st March, 2017, emphasizes the basic principles, strategic targets and action plans for the international cooperations in the are of Internet governance, and encourages the deep interaction among the public and private stakeholders to facilitate the mutual promotion between the ICT innovation and the cybersecurity.

2. Main Legislations related to cybersecurity governance

Indeed, on the basis of the values and approaches established by these Policies, the Chinese lawmaker starts to introduce the ad hoc cyber Laws and, at the same time, to reform and update the related traditional Laws, in order to provide a more systematic institutional framework. From these main legislations, the ICT companies in China can explore better their cybersecurity obligations for the compliance purpose.

2.1 In regards to the new cyber Laws, until now the most important are two:

(1) The *Cybersecurity Law*, as the actual „top-level design" for cybersecurity affairs in China, was issued by the Twenty-fourth Meeting of the Standing Committee of the Twelfth National People's Congress on 7 November, 2017 and entered into force on 1st July, 2017. This Law has 79 articles in total and is composed of the following seven Chapters: Chapter I General Provisions (Art.1-Art.14), Chapter II Cybersecurity Support and Promotion (Art.15-Art.20), Chapter III Network Operation Security (Art.21-Art.39), Chapter IV Network Information Security (Art.40-Art.50), Chapter V Monitoring, Early Warning and Emergency Response (Art.51-Art.58), Chapter VI Legal Liability (Art.59-Art.75), and Chapter VII Supplementary Provisions (Art.76-Art.79)[7].

(2) The *E-Commerce Law*, also containing cybersecurity obligations norms for this specific sector, was issued by the Fifth Meeting of the Standing Committee of the Thirteenth National People's Congress on 31 August, 2018 and entered into force on 1st January, 2019. This Law has 89 articles in total and is composed of the following seven Chapters: Chapter I General Provisions (Art.1-Art.8), Chapter II E-Commerce Businesses (Art.9-Art.46), Chapter III Formation and Performance of E-Commerce Contracts (Art.47-Art.57), Chapter IV Settlement of E-Commerce Disputes (Art.58-Art.63), Chapter V Promotion of E-Commerce (Art.64-Art.73), Chapter VI Legal Liability (Art.74-Art.88), and Chapter VII Supplementary Provisions (Art.89)[8].

Besides, in the beginning of 2019, the Legislation Plan of the Standing Committee of the Thirteen National People's Congress (2018-2022) has listed, among others, the *Personal Information Protection Law, the Data Security Law and the Telecommunication Law*, which means these three Laws will also be the future legislative reference for the discussions on the cybersecurity obligations of ICT companies in China respect to the specific technological environments.

---

[6] In relation to the values of cooperation on cyberspace for digital economy, see also Li Haiying, *Digital Economy and International Cooperation on Cyberspace*, in Civil-Military Integration on Cyberspace, 2018, no. 6, p. 24.

7 For more information on the framework of the Cybersecurity Law, see Meng Lu, *Analysis on the Rule of Law in Cyber Governance*, in Journal of Chongqing University of Science and Technology, 2018, no. 5, p. 21.

[8] Related to the regulation approach of the E-Commerce Law, see also Xue Jun, *New Questions in the Application of the E-Commerce Law*, in People's Rule of Law, 2019, no. 5, p. 1.

2.2 With reference to the reforms of traditional Laws for modern cyber governance purpose, the most relevant legislative initiatives can be found in the Chinese civil law and criminal law:

(1) The *General Provisions of the Civil Law*, adopted at the 5th Session of the Twelfth National People's Congress on 15 March, 2017 and entered into force on 1st October, 2017, has introduced the Art. 111 for the protection of personal information and the Art. 127 for the protection of data and network virtual property, both of which have enlarged the landscape of cybersecurity obligations for ICT companies[9].

(2) The *IXth Amendment of the Criminal Law*, adopted at the 16th Session of the Standing Committee of the Twelfth National People's Congress on 29 August, 2015 and entered into force on 1st November, 2015, has introduced the Art. 253-1 for the Crime against personal information, the Art. Art. 287-1 for the Crime of Illegal use of information network and the Art. 287-2 for the Crime of Assistance for cybercrime, all of which have provided the ICT companies with more criminal protection instruments in front of serious offences against their cybersecurity interests[10].

2.3 For the illustration completeness considerations, it seems necessary to point out also that there are several other related Laws, mentioned frequently during the discussions on the cybersecurity obligations for ICT companies in China, particularly: (1) the *Counterespionage Law*, adopted at the 11th Session of the Standing Committee of the 12th National People's Congress on 1st November, 2014 and accompanied with the *Detailed Rules for the Implementation* issued by the State Council on 22 November, 2017; (2) the *Counterterrorism Law*, adopted at the 18th Session of the Standing Committee of the Twelfth National People's Congress on 27 December, 2015 and amended on 27 April, 2018; as well as (3) the *National Intelligence Law*, adopted at the 28th Session of the Standing Committee of the Twelfth National People's Congress on 27 June, 2017 and amended on 27 April, 2018 (*See also III and IV for their more detailed analysis*).

3. Other relevant Norms related to cybersecurity governance

Furthermore, in order to facilitate the effective implementation of cybersecurity governance at substantive and procedural level, the Chinese Authorities don't hesitate to develop other norms in specific practice areas, which can be mainly divided in to two groups:

3.1. Firstly, at administrative level, there are various implementation norms usually issued, separately or jointly, by the State Council, the Cyberspace Administration of China, the Ministry of Public Security, the Ministry of Industry and Information Technology, etc.

These operational norms can provide more detailed practical rules for the activities of the Chinese Authorities, ICT companies and other stakeholders, already covering the issues related to online content governance, cybersecurity graded protection, critical information infrastructure protection, personal information protection, network products and services security review, cybersecurity incidents regulation and so on. Among others, the following regulations can be considered as the relevant references for understanding better the Chinese approach in this area.

---

[9] For analysis on the ratio legis of the General Provisions of the Civil Law, see also Wan Haoxuan, *Principles System of the General Provisions of the Civil Law*, in Legal System and Society, 2019, no. 13, p. 11.

[10] For more information on the background of the IX Amendment of the Criminal Law, see Wang Disheng, *Contributions of the IX Amendment of the Criminal Law for the current criminal system*, in Journal of Lanzhou Institute of Education, 2017, no. 4, p. 156.

(1) The *Regulations on Protecting the Safety of Computer Information Systems*, promulgated by the Order No. 147 of the State Council on 18 February, 1994 and amended by the Order No. 588 on 8 January, 2011, has 31 articles in total and is composed of five Chapters: Chapter I General Provisions (Art.1-Art.7), Chapter II System of Safety Protection (Art.8-Art.16), Chapter III Safety Supervision (Art.17-Art.19), Chapter IV Legal Responsibilities (Art.20-Art.27), and Chapter V Supplementary Provisions (Art.28-Art.31).

(2) The *Provisions on Internet Security Supervision and Inspection by Public Security Organs*, promulgated by the Ministry of Public Security on 5 September, 2018, has 29 articles in total and is composed of five Chapters: Chapter I General Provisions (Art.1-Art.7), Chapter II Supervision and Inspection Objects and Contents (Art.8-Art.12), Chapter III Supervision and Inspection Procedures (Art.13-Art.20), Chapter IV Legal Responsibilities (Art.21-Art.27), and Chapter V Supplementary Provisions (Art.28-Art.29).

3.2. Secondly, at judicial level, there are also numerous so called „Judicial Interpretations" issued, separately or jointly, by the Supreme People's Court and the Supreme People's Procuratorate. These general directives, focused on certain judicial phenomenon instead of single case, can offer the practice guidelines for the activities of the Chinese judicial Authorities to guarantee better the unified application of Laws on the emerging cybersecurity issues. Without doubt, it's necessary to strengthen the importance of the following two Judicial Interpretations for the purpose of this article.

(1) The *Provisions on Several Issues concerning the Application of Law in the Trial of Cases involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks*, issued by the Supreme People's Court on 21 August, 2014, has 19 articles in total and provides judicial guidelines for the civil litigation questions related to the rules of jurisdiction, the burden of proof, the forms of notifications, the attribution of liability, the legal nature of technological measures, the causes of justification, the petition for retrial, the trial supervision procedure, etc.

(2) The *Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information*, jointly issued by the Supreme People's Court and the Supreme People's Procuratorate on 8 May, 2017, has 13 articles in total and provides a sophisticated set of operation rules for the judicial application of the Art. 253-1 (Crime against personal information) of the Criminal Law, and replies to the emerging concerns related to the criminal definition of the personal information, the classification of the personal information, the sources of legal obligations, the *actus reus* judgment rules, the *mens rea* judgment rules, the serious circumstances, the causes of justification, the criminal participation liability, the criminal assistance liability, the criminal liabilities of the entities, the lenient punishment rules, the calculation rules for the personal information, the criminal fine application rules and so on.

III. Systematic Understanding of Cybersecurity Obligations of ICT Companies

In reality, only by the systematic study of the aforementioned sophisticated cyber governance framework, it's possible to obtain a complete insight on the effective cybersecurity obligations of ICT companies in China.

In the first place, the current governance framework marks out in this regard the „bottom lines" for the daily operation activities of ICT companies:

On one hand, *there are eight activities that are clearly declared as forbidden*, i.e.: (1) using the network to conduct any activity that endangers national security, honor and interest; (2) inciting to subvert the state power or overthrow the socialist system; (3) inciting to split the country or undermine the national unity; (4) advocating the terrorism or the extremism; (5) propagating the ethnic hatred or discrimination; (6) spreading the violent or pornographic information; (7) fabricating or disseminating false information to disrupt the economic and social order; and (8) infringing upon the reputation, privacy, intellectual property rights or other lawful rights and interests of any other person.

On the other hand, *there are five conducts that are specifically provided as illegal and can be punished at administrative and criminal law level*, i.e.: (1) illegally intruding into any other person's network; (2) interfering with the normal functions of any other person's network; (3) stealing network data; (4) providing programs or tools specifically used for conducting activities endangering the cybersecurity, such as network intrusion, interference with normal functions and protective measures of the network, and stealing of network data; and (5) intentionally providing the technical support, advertising promotion, payment and settlement services or any other assistance to any other person that conducts any activity endangering the cybersecurity.

In the second place, the same Chinese cyber governance framework also gives birth to a full set of detailed cybersecurity obligations for the ICT companies in China, reflected at technical, organizational and content level, that can be mainly divided into the following four groups:

1. Obligations for the technological protection

Without doubt, the ICT companies shall adopt the technological measures to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified, especially including: (1) developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection; (2) taking technical measures to prevent computer viruses, network attack, network intrusion and other acts endangering cybersecurity; (3) taking technical measures to monitor and record the status of network operation and cybersecurity incidents, and preserving relevant weblogs; and (4) taking measures such as data categorization, and back-up and encryption of important data; etc.

Besides, the ICT companies shall continuously provide security maintenance for their products and services, and shall not terminate the provision of security maintenance within the stipulated period or the period agreed upon by the parties. They shall not install malware and, when discover any risk such as security defect and vulnerability of the network products or services, shall immediately take remedial measures, inform users in a timely manner, and report to the competent Authority in accordance with relevant provisions.

Furthermore, the ICT companies shall make emergency response plans for cybersecurity incidents, and deal with system bugs, computer viruses, network attack, network intrusion and other security risks in a timely manner. When any incident endangering cybersecurity occurs, the related ICT company shall immediately initiate the emergency response plan, take corresponding remedial measures, and report to the competent Authority in accordance with relevant provisions.

2. Obligations for the organizational management

Considering the principle of proportionality, on the basis of technology and market power, the ICT companies shall also fulfill the various cybersecurity obligations at the organizational management level:

In the first place, Where the ICT companies provide network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide true identity information when signing agreements with users or confirming the provision of services. If any user fails to provide his or her true identify information, the ICT companies shall not provide him or her with relevant services.

In the second place, as the electronic information sent by and application software provided by any individual or organization shall not be installed with malware, or contain any information of which the release or transmission is prohibited by any law or administrative regulation, the electronic information release service companies and application software download service companies shall perform security management obligations.

If these companies find that any user commits any conduct as set forth in the preceding paragraph, they shall cease the provision of services, take deletion or any other handling measure, preserve relevant records, and report to the competent Authority.

In the third place, the ICT companies shall establish complaint and reporting systems for network information security, disclose the ways for filing complaints and reports and other information, and accept and handle complaints and reports related to network information security in a timely manner.

3. Obligations for the personal information protection

Actually, in today's China, the public opinion pays unprecedently high attention to the issue of personal privacy protection and building an outstanding reputation in this regard is becoming crucial for the business success of the ICT companies in the Chinese market. Therefore, the fulfillment of the obligations related to the personal information protection are widely considered by themselves as one of the top priorities, which covers at least the core legal requirements listed below:

(1) As the starting point for all, the ICT companies shall strictly keep confidential users' personal information collected by them, and establish and improve the system for the protection of users' information. They shall not divulge, tamper with or damage the personal information collected by them, and shall not provide personal information to any other person without the consent of the persons whose information is collected (except that the information has been processed in a manner that it is impossible to distinguish a specific person and it cannot be retraced).

(2) When collect and use the personal information, the ICT companies shall follow the principles of legality, rightfulness and necessity, disclose the rules for collection and use, explicitly indicate the purposes, means and scope of collecting and using information, and obtain the consent of the persons whose information is collected. They shall not collect personal information irrelevant to the services provided by them, shall not collect or use personal information in violation of the provisions of any law or administrative regulation or the agreement of both parties, and shall dispose of personal information preserved by them in accordance with the provisions of laws and administrative regulations and agreements with users.

(3) Where an individual finds that any ICT company collects or uses his or her personal information in violation of the provisions of any law, administrative regulation or the agreement of both parties, the individual shall be entitled to request the network operator to delete his or her personal information. If the individual finds that his or her personal information collected or stored by the ICT companies has any error, he or she shall be entitled to request them to make corrections and the ICT companies shall take measures to delete the information or correct the error.

(4) No ICT company may acquire personal information by stealing or any other illegal means, or illegally sell or provide personal information to any other person.

4. Obligations for the law enforcement assistance

Like in other jurisdictions where the ICT companies are comm considered as very important stakeholders also in the cybersecurity law enforcement area, the Chinese cyber governance system has introduced as well the specific norms to which they can refer when the competent Authorities require assistance or support for the law enforcement purpose.

For one thing, where any security incident occurs, the emergency response plan for cybersecurity incidents shall be initiated immediately to investigate and assess the incident, and the relevant ICT companies shall be required to take technical measures and other necessary measures to eliminate potential security hazards and prevent the expansion of the harm, and release to the public the warning information relating to them in a timely manner.

For another, where the relevant Authority at or above the provincial level finds any relatively high security risk or security incident on the network in the performance of cybersecurity supervision and administration functions, it may hold an interview with the legal representative or primary person in charge of the ICT companies according to prescribed powers and procedures, and the ICT companies shall take measures to make rectification and eliminate hidden risks as required.

Furthermore, as frequently discussed, the ICT companies shall provide technical supports and assistances to the public security and national security Authorities for their activities of investigating crimes or safeguarding national security according to the provisions of Law.

In this regard, it is necessary to point out that the similar assistance obligation of ICT companies can be found in several current Chinese Laws, including the Cybersecurity Law of 2017(Art. 28), the Counterespionage Law of 2014(Art. 13), the Counterterrorism Law of 2015(Art. 18) as well as the National Intelligence Law of 2017(Art. 7, Art. 12 and Art. 14), the effective application of which, however, should be integrated with other connected institutions established by the Chinese legal system (*See also IV for a more detailed analisys*).

IV. Principle of Legality and Cybersecurity Obligations of ICT Companies

As strengthened before, it's possible to more precisely determine the real extent of cybersecurity obligations of the ICT companies in China only by the the systematic reading of the entire Chinese cyber governance framework.

Meanwhile, in practice, the before-mentioned multi-level cybersecurity obligations cannot be interpreted beyond the numerous institutional limitations already rooted in

the current Chinese legal system, as the rational balance between the industry developments and the security interests, as well as the strict proportionality between the rights and the obligations, are always the top priority of the Chinese regulation approach in this area.

In fact, among others, the most fundamental benchmark for the fulfillment of the cybersecurity obligations by the ICT companies in China is the principle of legality, which effectively requires all stakeholders to avoid any extensive interpretation of these obligations without an explicit legal basis, in order to guarantee the correct implementation of the ratio legis.

As prominent example, specifically speaking to one of the most debated topics, with reference to the forenamed obligations of the ICT companies for the law enforcement assistance (*See also III.4 for a detailed illustration*), such interpretive paradigm is much more than emblematic and already reflected at the following three levels:

1. Principle of Legality and territorial scope of Cybersecurity Obligations

As the first interpretive limitation, it is indispensable to recall the territorial scope provided by the Chinese law for the cooperation and assistance obligations of the ICT companies.

For one thing, on the basis of the Art. 2 of the Cybersecurity Law, itself shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China. Logically, this means only the ICT companies directly operating within the Chinese territory should fulfill the cooperation and assistance obligations in front of the competent Authorities, and no overseas subsidiary of these ICT companies outside of the Chinese territory should satisfy the assistance requests of the Chinese Authorities.

For another, even in other Laws such as Counterespionage Law, Counterterrorism Law and National Intelligence Law, etc., there is no disposition that asks for extending the cooperation and assistance obligations beyond the Chinese territory to cover also the overseas subsidiaries of the ICT companies.

At the same time, for the business activities of the overseas subsidiaries of the Chinese ICT companies, the Chinese regulators commonly strengthen the necessity of the local compliance managements to guarantee the no harm for the interests of the host countries (regions):

The *Code of Conduct for Overseas Investment and Operation of Private Enterprises*, jointly issued by National Development and Reform Commission, Ministry of Commerce, People's Bank, Ministry of Foreign Affairs and All-China Federation of Industry and Commerce on 6 December, 2017, provides that the private enterprises carrying out investment and operation activities shall comply with the laws and regulations of the host countries (regions) and comply with the relevant treaty provisions and other international practices[11].

Furthermore, the same Code encourages the private enterprises to select and hire domestic and overseas firms specialized in law, assessment, and credit rating, etc., strictly implement compliance examination for major decisions and transactions, effectively conduct follow-up analysis and compliance training on the regulatory rules relevant to overseas investment business, strengthen the communication with the

[11] On the relationship between the international law and domestic law, see He Zhipeng, *Values of the International Law for Nowadays China*, in Tsinghua University Law Journal, 2018, no. 1, p. 10.

supervision departments in the host countries (regions), and actively cooperate with the supervision work.

More recently, the *Guidelines for Compliance Management of Enterprises' Overseas Operations,* jointly issued by National Development and Reform Commission, Ministry of Foreign Affairs, Ministry of Commerce, People's Bank, State-owned Assets Supervision and Administration Commission, State Administration of Foreign Exchange and All-China Federation of Industry and Commerce on 26 December, 2018, also requires that the overseas subsidiaries of the Chinese companies shall comply with the laws and regulations of the host countries (regions) related to employment protection, environment protection, data and privacy protection, intellectual property protection, anti-corruption, anti-bribery, anti-monopoly, anti-money laundering, anti-terrorist financing, trade control and financial taxation, etc., in order to effectively realize the all-round local compliance of their daily operation activities abroad[12].

2. Principle of Legality and Constitutionality of Cybersecurity Obligations

The second important interpretive limitation on the extending application of the cooperation and assistance obligations of the ICT companies is the constitutionality, which demands, among others, that: (1) the passive subject of assistance obligations should be determined; (2) the scope of assistance should be determined; (3) there should be no conflict of obligations.

(1) In regards to the first requirement of *determined passive subject of obligations*, a specific assistance obligation does not always cover all types of the ICT companies.

Actually, the Cybersecurity Law of 2017 aims the network operators (*including the owners, managers, and network service providers of the networks*) operating within the Chinese territory, which means the other ICT companies such as the manufacturers of telecommunication equipments cannot required by the Chinese Authorities to fulfill the assistance obligations on the basis of this Law when they merely engage in R&D and production and sale of telecommunication equipment.

In the same way, the Counterterrorism Law of 2015 provides the telecommunications business operators and internet service providers as the passive subjects of assistance obligations. Among them, the telecommunication business operators refer to the basic telecom service provider and the access provider, and the Internet service providers refer to providers who provide users with content services such as news, information, data, audio and video, and communication platform. Again, in this case, the manufacturers of telecommunication equipments as well as other ICT companies cannot be considered as the qualified passive subjects respect to their business activities different from the aforesaid ones.

(2) In relation to the second requirement of *determined scope of assistance*, it's also necessary to strengthen that the assistances of the ICT companies cannot serve the purpose beyond the specific scope established by the Laws.

The Counterespionage Law of 2014 applies only for the purpose of carrying out the counterespionage activities which are clearly defined by the Law itself and have obvious nature of defensive actions rather than attacking actions, which means, among others, the Chinese Authorities are not authorized to order the ICT companies to hack into products they make to spy on or disable communications of other countries. In fact, the same approach is followed also by the the Counterterrorism Law of 2015.

---

[12] On the current compliance practices of the Chinese companies, see Xie Jinhui, *Considerations on the Framework of the Compliance Practices*, in Construction Enterprise Management, 2019, no. 5, p. 25.

Meanwhile, the National Intelligence Law of 2017 refers only to the intelligence related to the conduct against the national security and other national interests of China, which means, for example, planting backdoors, eavesdropping devices or spyware in its equipment is obviously contrary to the ratio legis of the same Law.

(3) In concern of the third requirement of *no conflict of obligations*, the Chinese legal system substantively prohibits that the ICT companies can be put into a status of conflict when they are ordered to fulfill a determined obligation[13].

Among others, the first example is the National Intelligence Law of 2017, which contains a safeguard that discharges individuals and organizations from providing support, assistance and cooperation to the national intelligence agencies that would contradict their legitimate rights and interests, let alone where doing so would violate the laws of another country.

Another relevant example is the Cybersecurity Law of 2017 which prohibits definitively the conduct of installing malware, which means planting backdoors, eavesdropping devices or spyware in ICT equipments will be punished strictly according to the same Law. Without doubt, it's a serious conflict of obligation under this perspective if the Chinese Authorities require the ICT companies to plant backdoors, eavesdropping devices or spyware, hence this kind of requirement will be considered as unlawful.

3. Principle of Legality and due process

The third fundamental interpretive limitation on the extending application of the cooperation and assistance obligations of the ICT companies is the due process, which requires, among others, that: (1) the operational procedure of law enfocement; (2) the liability of the competent Authority; and (3) the right remedy of the interested party.

(1) In accordance to the first requirement of *operational procedure of law enforcement*, it's mandatory for the competent Authority to follow the operational procedure provided by the applicable Law when they exercise the statutory duties[14].

In case of the Cybersecurity Law of 2017, the special procedural provisions are indeed established. For example, information obtained by relevant authorities in fulfilling their duties of protecting cyber security can only be used for the purpose of maintaining cyber security, and must not be used for other purposes (Article 30).

Furthermore, the Counterespionage Law of 2014, the Counterterrorism Law of 2015 as well as the National Intelligence Law of 2017 respectively provide stringent procedural requirements and restrictions on specific law enforcement activities

(2) On the basis of the second requirement of *liability of the competent Authority*, the same competent Authorities should be liable for their law enforcement actions.

According to the Cybersecurity Law of 2017, if relevant authorities are in violation of the provisions of Article 30 of this Law and use the information obtained in performing their duties of cyber security protection for other purposes, the directly responsible person in charge and other directly responsible personnel shall be punished according to law. If the staff of the relevant authorities neglects their duties, abuses their power, or engages in malpractice for personal gains, which activities don't reach the threshold of crimes, they shall be subject to sanctions (Article 73). If they violate the

---

[13] On the principle of no obligation conflict in China, see Liu Sheng, *Studies on the Obligation Conflict*, in Law and Economy, 2011, no. 4, p. 9.

[14] On the legality requirements of statutory duties, see Wang Fang, *Legality for the Statutory Duties of the Modern Government*, in People's Tribune, 2019, no. 1, p. 15.

provisions of this Law and cause other people to suffer damage, they shall bear civil liability according to law.

Also the the National Intelligence Law of 2017 provided that the conduct of the state intelligence agency and its staff is subject to legal restrictions, and potential abusive conduct, including infringement of legitimate rights and interests of citizens and organizations, would be subject to investigation and punishment in accordance with the law. The same liability approach can be found in Counterespionage Law of 2014 as well as the Counterterrorism Law of 2015.

(3) For the sake of the third requirement of *right remedy of the interested party*, any ICT company has the right to seek judicial relief in accordance with the Administrative Procedure Law.

A common framework under the Cybersecurity Law of 2017, the Counterespionage Law of 2014, the Counterterrorism Law of 2015 as well as the National Intelligence Law of 2017 is that, as stipulated in article 12 of Administrative Procedure Law, citizens, legal persons and other organizations shall have the right to bring a lawsuit to the people's court if they believe that the administrative authorities have violated the law.

References

1. He Zhipeng, *Values of the International Law for Nowadays China*, in Tsinghua University Law Journal, 2018, n. 1, p. 10.

2. Li Congyuan, *Future of „Internet Plus" Action Plan*, in Information Research, 2018, n. 2, p. 95

3. Li Haiying, *Digital Economy and International Cooperation on Cyberspace*, in Civil-Military Integration on Cyberspace, 2018, n. 6, p. 24.

4. Liao Jingwei-Yu Juan, *Research on the Big Data Industry*, in Modern Business Trade Industry, 2018, n. 6, p. 7.

5. Liu Sheng, *Studies on the Obligation Conflict*, in Law and Economy, 2011, n. 4, p. 9.

6. Meng Lu, *Analysis on the Rule of Law in Cyber Governance*, in Journal of Chongqing University of Science and Technology, 2018, n. 5, p. 21.

7. Wan Haoxuan, *Principles System of the General Provisions of the Civil Law*, in Legal System and Society, 2019, n. 13, p. 11.

8. Wang Disheng, *Contributions of the IX Amendment of the Criminal Law for the current criminal system*, in Journal of Lanzhou Institute of Education, 2017, n. 4, p. 156.

9. Wang Fang, *Legality for the Statutory Duties of the Modern Government*, in People's Tribune, 2019, n. 1, p. 15.

10. Wang Kewei-Zheng Zai, *Analysis on the National Cyberspace Security Strategy*, in Digital Communication World, 2019, n. 2, p. 115.

11. Xie Jinhui, *Considerations on the Framework of the Compliance Practices*, in Construction Enterprise Management, 2019, n. 5, p. 25.

12. Xue Jun, *New Questions in the Application of the E-Commerce Law*, in People's Rule of Law, 2019, n. 5, p. 1.

13. Yuan Hui, *Studies on the Development Planning for the New Generation of Artificial Intelligence*, in Tech Wind, 2018, n. 31, p. 37.

14. Zhang Boqin-Sun Shuyang, *2019 Development Trend Prospects of Network Security in China*, in Cyberspace Security, 2019, n. 1, p. 37.