Article

China & WTO Rev. 2022:2; 255-276
http://dx.doi.org/10.14330/cwr.2022.8.2.02
pISSN 2383-8221 • eISSN 2384-4388

CWR
China and WTO Review

Genesis of Data Security Mechanism in China: The Next Step to Data Nationalism

Ella Gorian*

The study aims to analyse data security in the financial and banking sector of China. The data laws provide a 'consent-oriented' approach where consent, along with a limited list of exceptions, is the legal basis for the processing of personal information. The personal data protection mechanism comprised the Data Security Law, the Cybersecurity Law, and the Personal Information Protection Law. Taken together, they cover all areas of information security and establish a severe data protection regime: they determine the scope of regulation, objects and subjects, responsibility, and institutional control mechanisms. For an accurate assessment, it is necessary to wait for the adoption of by-laws that specify the provisions of these laws. The financial and banking sector already has several by-laws in place that set stringent standards for the security of personal information. The leading role in this mechanism is taken by the financial regulator - the People's Bank of China.

Keywords: Personal Data, Cross-Border Data Transfer, Financial Regulator, Data Security, Big Data, Personal Data Operator

* Associate Professor of Vladivostok State University School of Law. Ph.D. in Jurisprudence (Parliament Inst. of Legislation, Kyiv). ORCID: http://orcid.org/0000-0002-5962-3929. The reported study was funded by RFBR, project 20-011-00454 "Ensuring the rights of investors in the banking and financial sectors in the context of the digitalization of the economy in the Russian Federation and the leading financial centres of East Asia: a comparative legal aspect." The author may be contacted at: ella.gorian@gmail.com/Address: 41, Gogol Str., Vladivostok, 690014, Russian Federation.

All the websites cited in this article were last visited on August 2, 2022.

I. Introduction

The digitalization of the economy and the penetration of information technologies into all spheres of human life and society have made personal information vulnerable. The personal data is often not only unaware of its collection and processing, but also the purpose of such actions. The state mainly tries to guarantee the security of personal data, but the legal mechanism for securing personal data in modern conditions should be more improved.

Since 2019, the People's Republic of China (PRC) has been implementing an ambitious plan to regulate Big Tech (large companies that contribute to significant changes in society through their own dominance and role in online activities). Therefore, Alibaba Group, LinkDoc and DiDi have already received orders and bans on listing their shares on foreign exchanges. The concern of the Chinese government about the personal data protection is also observed in the automotive industry, so that manufacturers of high-tech cars are required to comply with data protection regulations. Today, almost all situations in which people find themselves in or near a car fall under these regulations.

In May 2020, the Cyberspace Administration of China published a draft of Several Provisions on Administration of Automobile Data Security,[1] which contains a number of provisions for the protection of personal data. This measure is caused, among other things, by the recent investigation by the Cyberspace Administration of the Ministry of Public Security, the Ministry of State Security, the Ministry of Natural Resources, as well as the tax, transport and antitrust authorities of the PRC against one of the largest companies - DiDiChuxing Technology Co. (previously called DidiDache and DidiKuaidi, car rental companies with over 550 million users and tens of millions of drivers). According to preliminary data, DiDi does not sufficiently ensure the security of the personal data of its customers.[2]

The People's Bank of China plays a special role in this process, which promotes a strict approach to regulating the activities of FinTech companies - applying to them the same rules as to classical financial companies: compliance with the rules on the information security of consumers' personal data; improving corporate governance (increasing transparency); following the standards of prudential supervision (sending reports to the financial regulator for early identification of possible problems); and preventing illegal lending, and insurance and financial asset management.[3]

Given the leading role of China in the digitalization of the economy and public administration processes, this national policy is a very important direction for improving the Russian legal system in this regard.

The primary purpose of this research is to emphasize that Chinese data protection model embodies the logical and anticipated response of national authorities to internal and external threats in circumstances of fragmentation. This paper is composed of four parts including Introduction and Conclusion. Part two will review the newly implemented approach to personal data regulation. Part three will discuss the impact of PRC laws on data and information protection on national security in the era of digital economy and fragmentation of world order.

II. Personal Data in China's Legislation

In China, the term "personal data" is rarely used in legislation. Instead, "personal information" is more popularly stipulated in relevant laws and regulations. The PRC Civil Code adopted in 2020 included Book Four (Personality Rights) that contains "Rights to Privacy and Protection of Personal Information" (Chapter VI).[4]

Article 1034 of the PRC Civil Code defines personal information as "information recorded electronically or by other means that can be used alone or in combination with other information to identify an individual."[5] The law directly refers to such data as the name, date of birth, identification number, biometric information, residential address, telephone number, e-mail address, medical information, and location of the person, leaving this list open. Notably, relevant provisions on the right to privacy apply to sensitive personal information.

Currently, mainland China is carrying out full-scale work to update the legislation in the field of personal data protection in order to reduce trade barriers. In particular, the Cybersecurity Law[6] and the E-Commerce Law was adopted in 2017 and 2018, respectively.[7] In a working conference of the Thirteenth Standing Committee of the National People's Congress held in 2018, particularly, a five-year plan for reforming the legislation of the PRC was approved with separate attention given to personal data.[8]

Following the growth in the number of information networks and, most importantly, the volume and quality of data transmitted through them, China revised

its information policy. Chinese researchers note the legislator's desire to improve legal instruments for regulating not only data production, but also their storage and processing which will allow them to become world market leaders.[9] Big data is collected and processed by both public authorities and private sector entities which increase the value of such information and its impact on political, social and economic processes, as well as their regulation.

Meanwhile, the use or processing of personal data in the absence of legal instruments (regulators) can lead to their compromise (encroachment) and even jeopardize national security. Therefore, ensuring the personal data security should be considered with a description of the legal and institutional framework.

The PRC Legislation Law defines the National People's Congress and its Standing Committee as the legislative bodies of the Chinese state.[10] The Standing Committee of the National People's Congress is empowered to "adopt and amend laws other than those to be adopted directly by the National People's Congress."[11] These laws and regulations, issued by the National People's Congress and its Standing Committee, have the highest binding force in shaping the legal system in China. In June 2021, the PRC Data Security Law was issued and came into force quickly on September 1, 2021.[12] The adoption of this law ended a busy period of law-making and active discussion by representatives of both public and private sectors. In particular, some kind of decentralization in the proposed model was noted for the personal data protection.[13] This is explained, first of all, by the special legal system of the PRC, which endows by-laws with legal force that is not comparable with similar documents issued in other states.

The rules regarding the personal data protection in China are laid down in the PRC Constitution as well as civil, administrative and criminal law. Following the digitalization of economy, legal instruments has been demanded in relation to its specific objects such as telecommunications, the Internet, and e-commerce, which are directly related to personal data in the production or provision of products and services.

The PRC Constitution regulates the basic rights and obligations of Chinese citizens,[14] such as the right and duty to work[15] such as freedom of speech, the press, associations, etc.[16] The PRC Constitution, however, does not directly refer to the personal data protection, but some articles can be interpreted as to include the personal data protection as human dignity or privacy. Article 38 of the PRC

Constitution states that the dignity of citizens is protected as one of the constitutional rights and Article 40 regulates the freedom and confidentiality of individual communication. Obviously, personal data can have a close relationship with human dignity and privacy, especially data on health, marital status, which by their nature are confidential. All this in the PRC Constitution allows us to talk about the indirect regulation of the personal data.

When the personal data regime is violated damaging the privacy of a person, certain privacy provisions would apply to such relationship to prevent the illegal collection or processing of personal data. For example, Article 2 of the Tort Liability Law attributed the right to privacy to the subjective civil rights and legitimate interests of individuals confirms the independent status of the right to privacy.[17] This right was ensured particularly in the case of contacting medical institutions,[18] which are required to maintain the confidentiality of patient information including medical history data. In this case, the personal data regime can be violated as an interference with privacy.

Adopting the PRC Civil Code in 2020 was an noticeable event in China's legislation history, which is called an encyclopaedia of the life of civil society.[19] Among the seven books such as General Part, Real Rights, Contracts, Personality Rights, Marriage and Family, Succession and Tort Liability, the privacy policy is included in Chapter VI (Rights to Privacy and Protection of Personal Information) of Book Four (Personality Rights).[20] As mentioned above, the personal information is defined in Article 1034. The processing of personal information should be carried out in accordance with the principles of legality, reasonableness and within the necessary limits (should not be subjected to excessive processing), which is subject to the following conditions: (1) obtaining consent from an individual or his guardian, unless otherwise not provided for by laws or administrative regulations; (2) the rules for the processing of information should be published; (3) a clear indication of the purpose, method and scope of information processing; and (4) the processing must not be contrary to laws or administrative regulations (consent of the subject).[21] The processing of personal information includes the collection, storage, use, clarification, transfer, provision, disclosure and other actions in relation to personal information.[22]

Prior to adopting the Civil Code, the legality the of personal information processing was determined by the General Provisions of the PRC Civil Law, which "regulate personal relations and property relations between individuals, legal

entities and organizations without a legal entity as equal parties."[23] Article 111 stated that the personal data of an individual shall be protected by law; no organization or individual may unlawfully collect, use, process, transfer, provide, trade or disclose personal data.[24] Thus, compared with the PRC Law on Torts and the General Provisions of the PRC Civil Law, the PRC the Civil Code has strengthened the protection of personal data.

In addition to defining personal information, the PRC Civil Code has fixed the principles of its protection, the rights of subjects, the obligations of authorized subjects, as well as the obligation of state bodies to maintain confidentiality. Separate provisions are devoted to special relationships regarding personal information. For example, Article 1226 of the PRC Civil Code requires that a medical institution and staff maintain the confidentiality of patient data.[25]

The adoption of the Civil Code was a significant milestone for protecting personal information in China. To some extent, it separates the protection of personal information from the protection of dignity or confidentiality, recognizing the protection of personal information as an independent object of regulation.[26]

III. PRC Laws on Data and Information Protection

Today, there are three laws in China for data and information protection such as the PRC Cybersecurity Law,[27] the PRC Data Security Law,[28] and the PRC Personal Information Protection Law.[29] These three legal instruments are creating an effective mechanism for ensuring data security.

A. The PRC Cybersecurity Law

The PRC Cybersecurity Law was developed for 2014-16. Its structure includes seven chapters: (1) general provisions; (2) ensuring and promoting cybersecurity; (3) the security of the network, which includes two sections: general provisions and security of operations at critical information infrastructure facilities; (4) security of information on the network; (5) monitoring, prevention and response to cyber-attacks; (6) legal liability; and (7) additional provisions.[30]

Chapter IV of the PRC Cybersecurity Law defines the regime for protecting

information in cyberspace, primarily personal data.[31] In accordance with the provisions of this chapter, network operators have obligations such as (1) ensuring the confidentiality of information; (2) ensuring the criterion of necessity and sufficiency of personal data;[32] (3) depersonalization of information;[33] (4) deletion of information obtained in violation of the law or containing incorrect information;[34] (5) taking immediate measures to protect information in case of illegal usage;[35] (6) creation of a system of interaction with clients, cooperation with authorized bodies;[36] and (7) termination of transmission, processing and other operations with information, and application of necessary technical measures at the request of authorized bodies.[37] The law also bans the illegal receipt and dissemination of information[38] and obliges the authorities to comply with confidentiality requirements.[39] In addition, it prevents creating the Internet pages or means of communication for illegal activities, including the dissemination of information about the methods of such activities and trade in prohibited or limited-circulation means.[40] Distribution of malicious programs and prohibited (restricted in use) information is also prohibited.[41]

B. The PRC Data Security Law

The PRC Data Security Law consists of seven chapters covering General Security Provisions (Chapter I); Data Security and Development Regulations (Chapter II); Data Protection Systems (Chapter III); Data Security Obligations (Chapter IV); Provisions on the Security and Openness of Government Data (Chapter V); Legal Liability (Chapter VI); and Additional Provisions (Chapter VII).

The law was developed to regulate data processing activities; ensure data security; promote the development and use of data; protect the legitimate rights and interests of individuals and organizations; and ensure the sovereignty, security; and development interests of the state.[42] The term "data" refers to the recording of information by electronic or other means,[43] while the term "data processing" [数据处理] mentions any activity with "data," including the collection, storage, use, processing, transfer, provision, disclosure, etc.[44]

This law focuses on the role of the state in ensuring data security, which is obliged to take measures to effectively protect and ensure a state of continuous security by following the general concept of national security and creating and improving the data security management system.[45] The institutional mechanism for ensuring data security will include public authorities of both general[46] and special competence

in the fields of industry, telecommunications, transport, finance, natural resources, healthcare, education, science and technology and related industries and areas.[47] The State Department of Network Information is responsible for overall network data security coordination and oversight.

The law defines the principles for ensuring data security as: "compliance with the law; observance of public morality and ethics; compliance with business and professional ethics; honesty and good reputation of data operators; compliance with safety requirements; no threat to national security and public interests; not causing harm to the legitimate rights and interests of citizens and organizations."[48] The legislator implements the system of general guarantees to ensure data security: (1) promotion and popularization of knowledge about data security; (2) raising public awareness and the level of data protection at the public level; (3) encouragement of joint activities of relevant departments, industry organizations, research institutions, enterprises and individuals on data protection; (4) creation of favourable conditions for joint maintenance of data security and promotion of the development of the whole society; (5) development of codes of conduct for data operators and staff development; (6) international cooperation in the field of data security management; and (7) confidentiality of consideration of applications and complaints.[49]

Regarding personal information, the following provisions of the law deserve closer consideration. First, there are the requirements for cross-border data transfers enshrined in Articles 31 and 36. According to Article 31, the cross-border transfer of sensitive data collected and generated by critical information infrastructure operators in China is regulated by the Cybersecurity Law which establishes the requirement to store data collected by and generated by critical information infrastructure operators.[50] If it is necessary to transfer such data abroad, a security assessment is carried out.[51]

Meanwhile, the PRC Data Security Law has introduced the term "important data," defined as "data related to national security, the state of the national economy, the vital activity of important government officials and the public interest."[52] With respect to such data, a more stringent control system is being introduced.

For cross-border transmission of sensitive data collected and produced in the course of work by data controllers in China, Article 31 of the Data Security Law provides that security verification measures should be coordinated by the Cyberspace Administration of the PRC with the relevant departments under the

State Council.[53] Now, there are no specific rules regarding the assessment of the security of sensitive data when it is transferred abroad. Data operators who violate the above article and illegally transfer sensitive data abroad shall be ordered by the authorized government agency to correct the violation and may be fined from CNY 100,000 to 1 million.[54] If the circumstances of the violation are serious, then the fine will be from CNY 1 to 10 million, followed by suspension of activities and revocation of licenses and permits.

The person(s) directly responsible for the violation shall be fined between CNY 100,000 and 1 million.[55] Article 36 of the Data Security Law establishes the procedure for providing data to foreign judicial or law enforcement requests: any organizations and individuals in China should obtain permission from the competent authority when dealing with requests for data transfer abroad made by foreign judicial or law enforcement agencies.[56] The competent authority shall consider such requests in accordance with relevant laws, international treaties and agreements entered by the PRC, or on the basis of the principle of equality and mutual benefit.[57]

If violating the procedure for providing data to foreign judicial or law enforcement authorities without the permission of the competent authorities of China, a fine will be imposed up to CNY 100,000 to 5 million with the simultaneous issuance of an order to suspend the company's activities until the violations are eliminated and the withdrawal of licenses and permits.[58] It should be noted that the law itself neither regulates the procedure for obtaining such a permit, nor establishes an authorized body (system of bodies). It is assumed that a corresponding by-law will be issued.

Secondly, these are compliance requirements for intermediary service providers (data intermediary services provider), the number of which has been steadily growing in recent years. In fact, such companies as Tianyuan Data, Jingdong Cloud, Guiyang Big Data Exchange, Shanghai Data Exchange Centre provide a trading platform for transactions between suppliers and buyers (consumers) whose object is data. Prior to adopting the Data Security Law, there were neither special provisions regulating the monitoring and control of data trading processes, nor standards for the activities of intermediary service providers which negatively affected the interests of the parties involved in data transactions.

This gap has been filled by the provisions of Article 33 of the law. It puts forward formal requirements for the data exchange process, namely, for those

entities providing intermediary services for the sale of data as follows. The first is the obligation to require the data provider to explain the source of the data. The data should be free of property defects, which means that the data should be neither obtained by theft or other illegal means, nor among those prohibited by Chinese laws and regulations. The second is the obligation to check the legal status of both parties to the transaction. The data should be legal or natural persons. For certain data trading operations that require the respective parties to obtain certain licenses in order to transact, the intermediary should verify that the parties have the required licenses. The third is the obligation to keep records of research and transactions.[59] This provision is similar to "the Yarovaya law" of Russia implying that data telecom operators store any data for a period determined by the government.[60] The records of research and transactions and related metadata should be retained on the mainland China and the expiration periods are to be set through by-laws that specify these regulations.

Brokering providers who violate the above provisions may be subject to numerous fines. Illegally obtained profits will be confiscated and a fine up to ten times of the amount of illegally obtained profits will be imposed. Absent such profits or if its amount is less than CNY 100,000, then the subject will be fined in the amount of CNY 100,000 to 1 million. In addition, it is possible to suspend the activities of the subject and withdraw permits and licenses. As shown in the previous case, the Data Security Law neither regulates the procedure for checking the activities of intermediary service providers, nor establishes an authorized body (system of bodies). The adoption of the relevant by-laws is expected.

Thirdly, the Data Security Law emphasises the protection of the interests of special groups of the population. Here, we are referring to people with disabilities due to age (elderly) and health (disabled). As often noted, in practice, cash payment is refused many times, although the elderly does not know how to use Alipay or WeChat Pay. In addition, after the outbreak of Covid-19, in some cities, people were denied access to public transport or services due to not receiving a digital health code which was implemented as part of the epidemic prevention measures.[61] To protect the rights of these groups and ensure the principle of equality, Article 15 of the Digital Security Law obliges any entity to fully consider the needs of older and disabled people when developing mobile applications for public services. On the one hand, the elderly and the disabled should not be forced to use so-called

smart products. For example, in addition to ordering food by scanning QR code and paying the bill with digital payments, restaurants should provide traditional ordering and payment methods as alternatives. On the other, it is necessary to take into account their needs when the relevant products are developed by connecting additional technological functions to the interface (large print, voice assistant, etc.).

Finally, personal data should adhere to the social morality and ethics. In particular, Article 28 of the Data Security Law provides that any data operators and developers of new data processing technologies "should contribute to economic and social development, the improvement of human well-being and the observance of social morality and ethics."[62] This norm clearly shows the legislator's requirements for the security of personal information: if before adopting this law the emphasis was on the legal aspects of data processing, this issue would be considered now in a moral context. Therefore, all subjects related to the data processing must take the norms of social morality and ethics into consideration.

C. The PRC Personal Information Protection Law

The PRC Personal Information Protection Law (PIPL), entered into force on November 1, 2021, is comprised of 8 chapters: (1) General Provisions; (2) Rules for Processing Personal Information; (3) Rules for Cross-border Provision of Personal Information; (4) Rights of Individuals in Activities of Processing Personal Information; (5) Obligations of Personal Information Processors; (6) Departments Performing Duties of personal information protection; (7) Legal Liability; and (8) Supplementary Provisions.[63]

The PIPL has built the personal data protection model. In general, China's privacy law has been developed on a "consent-based" approach, where consent, along with a limited list of exceptions, is a legal basis for the processing of personal information.

Many jurisdictions in the Asia-Pacific implemented the provisions of the EU General Data Protection Regulation (GDPR) that generally do not cover processing in the framework of "legitimate interests." In this regard, the operator has the right to process personal information in the public domain without prior consent of the person. It is subject to an appropriate balance between business interests, and the privacy interests of data subjects and fair processing. This narrower approach was implemented in the first edition of the draft PIPL. In the second edition, an

additional legal basis was introduced for personal information processors (persons who process personal information, a term similar to "data controllers" in accordance with the GDPR), which process available personal information publicly "within a reasonable scope."[64] The law does not disclose the content of the term "reasonable limits," except for the proviso that the purpose of processing publicly available personal information should not significantly deviate from the main purpose of publishing information.

The PIPL sets higher standards for processing the personal information of minors.[65] In cases of handling the personal information of minors under the age of 14 years, old personal information processors are obliged to obtain the consent of the minor's parents or other guardian in order to formulate special rules to deal with it. The draft law provides for the possibility of withdrawing consent to the processing of personal information.[66] Accordingly, the data processor must provide data subjects with a convenient way to withdraw consent. This will not affect any processing activities before the consent was withdrawn.

The procedure for data processing by third parties is separately defined:[67] if the agreement with third parties on data processing does not enter into force or is invalid, cancelled or terminated, third parties should not store personal information but return it to the data processor or delete it.

The PIPL expands the responsibilities of personal information processors who operate 'basic' Internet platform services to serve a 'massive' number of users (without specifying a threshold number) and have 'complex' business types.[68] Such responsibilities include: (1) establishing a steering committee, independent of the processor, to oversee the personal information processing; (2) suspending the provision of services to providers of products or services running on the platform of the personal information processor if they are in serious breach of data protection laws; and (3) issuing regular social responsibility reports regarding the processing of personal information.[69] It is noted that the fulfilment of the duties of such entities is associated with a number of uncertainties of: (1) terminology ('basic' Internet platform, 'massive' number of users, or 'complex' business types); (2) the grounds for suspension of services to providers of products or services running on the platform of the processor of personal information; and (3) the content of social responsibility reports.[70]

The PIPL protects the rights of deceased persons. Article 49 provides that

relatives of deceased persons can exercise rights in relation to personal information on their behalf.[71] The rights of the deceased to his/her personal information were mentioned neither in the previous version of the draft, nor in any other data protection regulation. However, the law does not disclose such aspects of the implementation of the right as: (1) the procedure for determining the authorized relative of the deceased; and (2) the mechanism of its implementation by the processor of personal information, including the procedure for confirming the identity of relatives and the fact of death of a person.[72]

The Chinese lawmakers oblige critical information infrastructure operators and personal information processors to store the personal information collected and generated within the Chinese territory[73] in cases when the processing of personal information reaches the number prescribed by the national cyberspace administration. If indeed necessary to provide such information and data to overseas parties, it shall be subject to the security assessment organized by the State cyberspace administration.[74]

The practitioners evaluate the following implications of the PIPL for multinational companies operating in China: (1) reassessment of existing storage practices of data originating in China; (2) providing Chinese data to foreign regulators or foreign courts only after consultations with Chinese counsel on transmitting such information overseas; and (3) restrictions on marketing activities.[75]

In the financial and banking sector, personal information is perhaps the most important asset for both investors and financial institutions. They require customers to provide detailed personal data (including sensitive data) in order to provide financial services. Improper processing of this personal data may result in threats to the personal safety or property of customers. The PRC Law on the People's Bank,[76] the PRC Law on Commercial Banks[77] and the PRC Law on Insurance[78] have provisions regarding the protection of personal financial data. For example, the PRC Law on Commercial Banks obliges banks to maintain the confidentiality of their depositors.[79]

In 2017, the People's Bank of China issued the Implementation Measures for the Protection of Financial Rights and Interests of Customers.[80] Article 3 of this Implementation Measures provides that collecting personal financial data should be carried out in accordance with the principles of voluntariness, equality, fairness and good faith.[81] In April 2019, the People's Bank of China's Regulations Development

Work Plan was adopted, which includes a plan to develop Measures for the Protection of Personal Financial Data.[82]

Meanwhile, the State Administration of Market Regulation (SAMR)'s special unit, the Standardization Administration of China, has developed a set of guidelines to regulate personal information protection in the financial and banking sector. On March 6, 2020, the Personal Information Security Specification Revisions (GB/T 35273-2020) was issued,[83] in order to establish specific requirements for strengthening the protection of personal information. In addition, Guidance for Personal Information Security Impact Assessment (GB/T 39335-2020) came into effect on June 1, 2021 to detail Article 54 of the Personal Information Protection Law.[84] Finally, the PRC Cyberspace Administration has issued a series of guidelines and standards for data processing by mobile application operators, including self-assessment, the use of SDKs (software development kits), and the minimum amount of personal information required for operation.[85]

Meanwhile, the role of the financial regulator (PBOC) in setting personal data protection standards should be noted. In particular, three standards were adopted in 2020. First, Personal Financial Information Protection Technical Specification (JR/T 0171-2020) defines the levels (3 levels) and categories (7 categories) of personal financial information.[86] In particular, the level of sensitivity distinguishes between user identification information (C3) that can identify a person and financial status (C2), and internal information assets (C1). Information is categorized depending on its types: (1) account; (2) identification; (3) financial transactions; (4) personal identification; (5) property; (6) loans; and (7) certain situations with a specific subject of financial information.[87]

Second, Guidelines for Data Security Classification (JR/T 0197-2020) require segregation of security levels from high to low, taking into account the impact on national security, public availability, interests, privacy and legal rights of the enterprise, as well as the degree of impact of damage to the security of these financial institutions (4 levels in total).[88]

Third, Measures of the PBOC on the Protection of Financial Consumers' Rights and Interests tightens the requirements for financial operators.[89] These Measures now have greater legal force whose violation can be regarded as a criminal offense.[90] Also, special attention is paid to consumers' rights to financial services such as the right to property security, the right to respect, the right to information,

the right to fair transaction conditions, and the right to enhanced information security.[91]Moreover, the standardization of direct marketing emphases on the right to receive information.[92] The sanctions for violation of laws and regulations have increased up to CNY 500,000.[93]

Regarding data protection, states either imposes the responsibility for data safety on the users and information system operators themselves, setting strict rules for providers ("liberal" model), or introduces special requirements for localizing all data within the state's jurisdiction ("data nationalism" model).[94] The "data nationalism" is fulfilled in national regulations worldwide (Russia, India, Australia, Singapore). It proclaims that data operators collect (including online), record, systematize, accumulate, store, refine (update, change) and extract personal data using databases located within the territory of a certain state.[95] Many states have adopted the so-called data localization laws to a certain extent. For example, Nigerian law establishes the rule that all government data should be placed within its borders; Vietnam obliges the Internet providers to store data on its territory for possible state verification; Australia prohibits in some cases the transfer of data on health status abroad; and special European Union Data Protection Directives encourage localization of data within it, setting strict requirements for the transfer of personal data to non-EU countries. Furthermore, Singapore's legislature pays attention to the protection of personal data after its mass compromise in 2018, including the personal data of the head of state.[96]

Data nationalism is part of the global trend of digital nationalism, whose essence is a division of the online world along offline borders. The course towards isolation from the global network is being taken not only by Russia and China, but also by other countries-often with linguistic features (China, India, Russia, Kazakhstan, Iran) or the religious ones (the 'halal' Internet of Islamic countries). States block objectionable content or interfere with information that is recognized in their territories as illegal or threatening to the regime. But the sovereignty of one or another segment of the network is not limited to the regulation of information dissemination.[97] There are at least three additional factors facilitating digital nationalism: politics, security, and protectionism. In the first case, the aim is to request for centralizing government or national self-identification. As a result, an alternative Wikipedia appears (Russia) or some regions disconnected the network without taking into account the economic consequences (Kashmir, Iraq).[98]

In order to ensure security, the state trusts only its own cryptographic systems and platforms. Unfortunately, in the contemporary world, it is practically impossible to implement the whole complex of technologies in isolation. Therefore, as redundant systems appear, the ideas of isolation and restrictions on the use of certain technologies are implemented where there are no real technological restrictions. Some countries are trying to regulate the inflow of foreign capital into the digital services transaction in order to protect domestic markets. For example, there is a technological front of the trade war between the US and China. The threat of the Internet balkanization is becoming more than just real. While segmenting is rooted in technical and economic reasons, governments drastically contribute the fragmentation. The global network is not global de facto.[99]

However, some have not assessed fragmentation so pessimistically. Multipolarity in the field of mass culture and consumer culture has already made a symbolic result. The infamous Orientalism, the perception of everything from the West as dynamic and progressive, and everything from other regions as frozen in time and archaic have almost completely disappeared. Both China and other East Asian economies, which a couple of decades ago seemed to be a hopelessly backward outskirts of the world, today have become powerful sources of innovation, being a hard die to American Silicon Valley and other Western centres to compete with. In a political sense, the melting pot of global popular culture undoubtedly creates many advantages for leading Asian economies including China and threatens the US's international leadership. The current phase of globalization - a combination of political and economic nationalism with an ever-accelerating cultural globalism - puts in a better position those countries that find the strength to stay away from the political xenophobia. China retains the status of a politically authoritarian state in the Western sense, but, in the cultural sense, wins the competition with Western states, primarily the US, due to its consistent support for the ideology of globalism.

The instinct of national self-preservation, on which politicians in different countries try to earn points, is a very powerful factor as well as dangerous destructive potential. The growing interdependence with technological progress may be only a weak antidote which would not prevent the new wars or international conflicts. Moreover, the very new information space can turn into the arena of these wars and conflicts. At the same time, the existence and development of a common cultural environment, which today is played by the Internet and global market for goods,

ideas and cultural meanings, gives hope for a qualitative change in the structures of the mass consciousness of residents of different countries. Perhaps, at some point, their desire to take advantage of the benefits from the new digital civilization will be stronger than the instincts of national xenophobia. As a result, the next generation of politicians will have to accept it as a reality and act in accordance with the aspirations of the voters of the digital age.[100]

IV. Conclusion

China's personal data law has been and will be developing based on a "consent-based" approach, where consent, along with a limited list of exceptions, is the legal basis for the personal information processing. Developing a mechanism for protecting personal data has been completed. In addition to the Civil Code, which laid the legal foundation for personal data protection, three special laws have been adopted on cyber security, data security and personal information security in China. Taken together, they cover all areas of information security and establish a strict data protection regime which determines the scope of regulation, objects and subjects, responsibility, and institutional control mechanism. The legal regime covers such aspects as personal data of deceased persons, disabled persons (due to age and health), as well as transnational data transfer. The financial and banking sector already has a few by-laws in place that set stringent standards for the personal information security. The leading role in this mechanism is played by the financial regulator-the People's Bank of China. The elaboration of data protection mechanism in China is a trend similar to that in the international community which contributes to national information security.

Received: May 15, 2022
Modified: July 15, 2022
Accepted: Aug. 15, 2022

References

1. Kevin Duan, Tina Wang and Kemeng Cai, Brief Comments on Draft Automobile Data Security Provisions, Hankun: Legal Commentary (May 27, 2021), https://www.hankunlaw.com/downloadfile/newsAndInsights/8c9f977eb01519c5f6f342e5a0ace6da.pdf.
2. Edwin Chan, *China Weighs Unprecedented Penalty for Didi after U.S. IPO*, Bloomberg, July 22, 2021, https://www.bloomberg.com/news/articles/2021-07-22/china-is-said-to-weigh-unprecedented-penalty-for-didi-after-ipo.
3. Pan Gongsheng, Deputy Governor of the People's Bank of China, answered a reporter's question on the financial management department's interview with Ant Group again [中国人民银行副行长潘功胜就金融管理部门再次约谈蚂蚁集团情况答记者问], People's Bank of China Website (Apr. 12, 2021), http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4229432/index.html.
4. The PRC Civil Code (Dec. 31, 2020), http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.
5. *Id*. art. 1034.
6. PRC Cybersecurity Law, https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html.
7. PRC E-Commerce Law, https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf.
8. Xiaojuan Wu, Research on Personal Data Protection in the Guangdong-Hong Kong-Macao Greater Bay Area 10 (2020) (Unpublished LL.M. Dissertation, University of Macau), https://umlibrary.primo.exlibrisgroup.com/discovery/fulldisplay?context=L&vid=853UOM_INST:umlibrary&tab=LibraryCatalog&docid=alma991009926485006306.
9. J. Ning, *Actively Promoting the Development of the Big Data Industry and Promoting China's Transition from a Big Data Country to a Strong Data Country*, 1 World Telecommunications 44 (2014).
10. PRC Legislation Law (2015 Amendment), art. 7, https://www.chinalawtranslate.com/en/2015lawlaw.
11. PRC Const. (2018 Amendment), art. 67(2), http://www.npc.gov.cn/englishnpc/constitution2019/constitution.shtml.
12. PRC Data Security Law, https://npcobserver.com/legislation/data-security-law.
13. Meng Zhou, *On Personal Data Protection Via Right to be Forgotten* [个人信息保护的被遗忘权实现], 2 J. Guangxi Admin. Cadre Institute of Pol.& L. [广西政法管理干部学院学报] 28-30 (2017).
14. Wu, *supra* note 8, at 22.
15. PRC Const. art. 42.
16. *Id*. art. 35.

17. PRC Tort Liability Law, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620761.htm.
18. *Id*. art. 62.
19. Qigang Wang & Linchuan Li, *Civil Code: The Guarantee of Civil Rights and the Encyclopedia of Social Life - A New Milestone and Synthesizer of Civil Legislation in China* [《民法典》:民事权利的保障书和社会生活的百科全书-中国民事立法新的里程碑和集大成者], 4 Contemp. China Hist. Stud. [当代中国史研究] 18 (2020).
20. PRC Civil Code, http://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html.
21. *Id*. art. 1035
22. Wu, *supra* note 8, at 25.
23. *Id*.
24. PRC Civil Code art. 111.
25. *Id.* art. 1226.
26. Wu, *supra* note 8, at 25.
27. *Supra* note 6.
28. *Supra* note 12.
29. PRC Personal Information Protection Law, https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation.
30. PRC Cybersecurity Law art. 40.
31. *Id*.
32. *Id*. art. 41.
33. *Id*. art. 42.
34. *Id*. art. 43.
35. *Id*. art. 47.
36. *Id*. art. 49.
37. *Id*. art. 50.
38. *Id*. art. 44.
39. *Id*. art. 45.
40. *Id*. art. 46.
41. *Id*. art. 48.
42. PRC Data Security Law art. 1.
43. *Id*. art. 3.
44. *Id*.
45. *Id*. art. 4.
46. *Id*. art. 5.
47. *Id*. art. 6.
48. *Id*. art. 8.
49. *Id*. arts. 9-12.

50. PRC Data Security Law art. 31.
51. *Id*. art. 36.
52. *Id*. art. 21.
53. *Id.* art. 31.
54. *Id*. art. 45.
55. *Id*. art. 46.
56. *Id*. art. 36.
57. *Id*. art. 36.
58. *Id*. art. 48.
59. *Id*. art. 33.
60. Ella Gorian, *Genesis of Russian cyber security legal mechanism: an authentic or a trend alike model?*, *in* Smart Technologies and Innovations in Design for Control of Technological Processes and Objects 937-49 (D. Solovyev ed., 2020).
61. Abby Chen, *A Close Reading of China's Data Security Law, in Effect Sept. 1, 2021*, China Briefing from Dezan Shira & Associates Website (July 14, 2021), https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021.
62. PRC Data Security Law art. 28.
63. PRC Personal Information Protection Law, https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation.
64. *Id*. art. 13.
65. *Id*. art. 31.
66. *Id*. art. 15.
67. *Id*. art. 23.
68. *Id*. art. 58.
69. *Id*.
70. Mark Parsons, Sherry Gong, Jessie Xie & Lan Xu, *China's first personal information protection law in the home stretch*, JD Supra Website (June 3, 2021), https://www.jdsupra.com/legalnews/china-s-first-personal-information-1211024.
71. PRC Personal Information Protection Law art. 49.
72. *Id*. art. 49.
73. *Id*. art. 40.
74. *Id*. art. 36.
75. Ryan Junck et al., *China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies*, Skadden, Arps, Slate, Meagher & Flom LLP Website (Nov. 3, 2021), https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws.
76. PRC Law on the People's Bank of China, http://www.pbc.gov.cn/english/ 130733/2941519/2015082610501049304.pdf.
77. PRC Law on Commercial Banks, http://www.china.org.cn/english/DAT/214824.htm.

78. PRC Insurance Law, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620648.htm.
79. PRC Law on Commercial Banks art. 79.
80. Implementation Measures for the Protection of Financial Rights and Interests of Customers, Law Info China Website (Sept. 15, 2020), http://lawinfochina.com/display.aspx?id=34143&lib=law.
81. *Id*. art. 3.
82. Jia Chen, *China unveils fintech development plan*, China Daily, Aug. 22, 2019, http://www.chinadaily.com.cn/a/201908/22/WS5d5e5ed7a310cf3e35567595.html.
83. Personal Information Security Specification Revisions (GB/T 35273-2020), Max.book118.com (Mar. 17, 2020), https://max.book118.com/html/2020/0317/8112141116002102.shtm.
84. Guidance for Personal Information Security Impact Assessment (GB/T 39335-2020), Max.book118.com (June 3, 2021), https://max.book118.com/html/2020/1218/7000125131003032.shtm.
85. Cybersecurity Review Measures, Cyberspace Administration of China Website (Jan. 4, 2022), http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm; Online Data Security Management Regulations (Draft for Comment), Digichina Stanford University Website (Nov. 14, 2021), https://digichina.stanford.edu/work/translation-online-data-security-management-regulations-draft-for-comment-nov-2021.
86. Personal Financial Information Protection Technical Specification (JR/T 0171-2020), Chinese Standard Website (Feb. 13, 2020), https://www.chinesestandard.net/PDF/English.aspx/JRT0171-2020.
87. *Id*.
88. Guidelines for Data Security Classification (JR/T 0197-2020), Chinese Standard Website (Sept. 23, 2020), https://www.chinesestandard.net/PDF.aspx/JRT0197-2020.
89. Measures on the PBOC on the Protection of Financial Consumers' Rights and Interests, The People's Bank of China Website (Sept. 18, 2022), http://www.pbc.gov.cn/tiaofasi/144941/144957/4099060/index.html.
90. *Id*. art. 64.
91. *Id*. arts. 14-21.
92. *Id*. art. 30.
93. *Id*. art. 60.
94. Gorian, *supra* note 60.
95. Courtney Bowman. *Data Localization Laws: An Emerging Global Trend*, Jurist: Legal News & Commentary (Jan. 6, 2017), https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization.
96. Gorian, *supra* note 60. *See also* Irene Tham, *Personal info of 1.5m Sing Health patients, including PM Lee, stolen in Singapore's worst cyberattack*, Straits Times, July 20, 2018, https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

97. Bo Zhao & Yang Feng Deng, *Mapping the development of China's dataprotection law: Major actors, core values, andshifting power relation*, 40 Computer L. & Security Rev. 1-16 (2021), https://www.sciencedirect.com/science/article/abs/pii/S0267364920301035?via%3Dihub.
98. Piotr Ahmad, *Digital nationalism as an emergent subfield of nationalism studies. The state of the field and key issues*, 1 Nat'l Identities 1-11 (2022).
99. Krisztina Lajosi & Pál Nyíri, *Introduction*: *The transnational circulation of digital nationalism*, 1(28)Nations & Nationalism 263-66 (2021), https://onlinelibrary.wiley.com/doi/10.1111/nana.12778.
100. Ivan Tsvetkov, *New nationalism and the struggle for dominance in the global digital cultural space* [Новый национализм и борьба за доминирование в глобальном цифровом культурном пространстве], 13(4)Herald of Saint Petersburg University: International Relations [Вестник Санкт-Петербургского университета. Международные отношения] 478-87 (2021).