Naveiñ Reet: Nordic Journal of Law and Social Research (NNJLSR) No. 9 2019, pp. 231-252

Recent Evolution of the Personal Privacy Legal Protection in People's Republic of China

Corrado Moriconi[1]

Abstract: This article explores the current legal protection of personal information in the People's Republic of China. The P.R.C. has rapidly developed legislatively and academically with comprehensive Chinese data protection regulation closely integrated with all new developments. Currently, the legal framework appeared to be fragmented in that it is composed of widely varying laws and regulations. This article will offer a description of the evolution of the modern concept of privacy within the context of Chinese political and societal norms. The relevant regulations and their development will be addressed relative to significant cases. Conclusions and perspectives on possible future improvements are described in a general summary.

Introduction

Privacy is (as) old as mankind. On the contrary, the right to privacy is a recent development. The right of personal privacy was first theorized and conceptualized by Samuel Warren and Louis Brandeis in the 1890 article, *The Right to Privacy*. This milestone has been described as 'one of the most influential law review articles of all time' (Kalven, 1966, 326) and praised as a 'brilliant excursions in the field of theoretical jurisprudence' (Adams, 1905, 37). Later on, Prosser, in 1960, established four privacy torts in his article *Privacy*. Another crucial step in the elaboration of the concept was reached in 1968 with the publication of Alan Westin's *Privacy and Freedom* in which he defined privacy in terms of self-determination.

Recently, the history of privacy has made clear that there is a strong relationship between privacy and the development of technologies. The sharing of our data has turned out to be massive and the way technology is used by both government and tech giants shows the economic and strategic value of this resource. While the phenomenon

1 I want to express my deep gratitude to Professor 徐涤宇, for the precious support, to Professor 黄美玲 for the priceless assistance, to Dr. Gianmatteo Sabatino for the valuable suggestions, to Dr. 刘禹呈 for the always useful advices, to Kurt Mitenbuler for the precious help in revising the work structure and language.

Corrado Moriconi (马思勇), J.D., Faculty of Law, University of Rome 'La Sapienza', Italy; Ph.D. candidate, Faculty of Law, Zhongnan University of Economics and Law, Wuhan, People's Republic of China; Research fellow, Faculty of Law, University of Rome 'La Sapienza', Italy. Contact: corr.90@hotmail.it

of digitalization tends to be a global trend, instead, its legal implications are perceived differently by each culture. This is clear in the different ways United States and Europe regulate privacy. Both sides of the Atlantic have different approaches that lead to differences in their legal models. In the EU, privacy and the protection of personal information are seen as fundamental rights and protected by comprehensive regulations which provide the individual with strong guarantees. In the U.S., there is no federal law covering the protection of data and local regulations typically establish less requirements and offer less protection than in the EU.

China has been slower in developing its own privacy legal model compared to the West, for complex historical and cultural differences. However, in recent years, China has sharply developed a consistent number of regulations. The country has the biggest Internet community and is a frontrunner in the area of digitalization. As a global cyber-force, it has increasingly played an active, even sometimes contested role in shaping the digital landscape through collaboration and competitiveness with Western economies. Nevertheless, China's policy regarding the regulation of cyberspace is different from policies adopted in the Western world. This affects the way Chinese policymakers perceive the value of privacy and its protection. Currently, the country is still in a process of legislative development, distinguished by its own characteristics. This article will clarify the current legal framework regarding personal data protection in China.

The Evolution of Privacy in the P.R.C.

Reform, Opening, and Digital Influence

As the distinguished Roman *prudens* Gaius taught, the *principium* is the most important part of the whole[2] (Diliberto, 2012, 53; Schipani, 2005, 80). Consequently, in order to address the current legal status of privacy in China, we will first attempt to historically contextualize the object of our research to be better informed about its origin and genesis.

It is argued that traditional Chinese culture was the cause of lack of privacy protections (Cao, 2005, 2). In the past, people tended to be more concerned about collective entities (the country and the family) than individuals. Enlightened by the principles of Confucian theories (Barrington Moore, 1984), people emphasized their interpersonal relationships (Fei, 1992), and privacy was deemed a negative word, a synonym of 'secret'.

A completely different concept of privacy arose with the reform and opening policies of Deng Xiaoping in 1978. Since then, the whole of Chinese society has experienced deep changes, caused transformations in every corner of society.[3]

---

2 Digest 1.2.1 (Gaius, XII Tables, book 1): *facturus legum vetustarum interpretationem necessario prius ab urbis initiis repetendum existimavi, non quia velim verbosos commentarios facere, sed quod in omnibus rebus animadverto id perfectum esse, quod ex omnibus suis partibus constaret:* ***et certe cuiusque rei potissima pars principium est****. Deinde si in foro causas dicentibus nefas ut ita dixerim videtur esse nulla praefatione facta iudici rem exponere: quanto magis interpretationem promittentibus inconveniens erit omissis initiis atque origine non repetita atque illotis ut ita dixerim manibus protinus materiam interpretationis tractare? namque nisi fallor istae praefationes et libentius nos ad lectionem propositae materiae producunt et cum ibi venerimus, evidentiorem praestant intellectum* ('since I am aiming to give an interpretation of the ancient laws, I have concluded that I must trace the law of the Roman people from the very beginnings of their city. This is not because I like making excessively wordy commentaries, but because I can see that in every subject a perfect job is one whose parts hang together properly. **And to be sure the most important part of anything is its beginning**. Moreover, if it is regarded as a sin for people arguing cases in court to launch straight into an exposition of the case to the judge without having made any prefatory remarks, will it not be all the more unfitting for people who promise an interpretation of a subject to deal straight off with that subject matter, leaving out its beginnings, failing to trace its origin, not even, as I might say, giving their hands a preliminary wash? In fact, if I mistake not, such introductions both lead us more willingly into our reading of the proposed subject matter, and, when we have got to the point, give us a far clearer grasp of it').

3 After the reform a new legal system with Chinese characteristics had been established with civil and commercial law as one of its major components where many national laws and numerous government regulations had been adopted in this regard. See Office of the State Council of China, 'The Socialist Legal System with Chinese Characteristics' (Oct. 27, 2011), available at http://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284659.htm

The effects of the economic reform had a great impact on the new idea of privacy. As the traditional planned economy system was replaced by a new socialist market economy, Chinese society started shifting from one in which a crucial domination of collective interests was paramount to a society in which the individual was regarded as an independent subject and individual interests more valued. As a result, pursuing individual economic interests was no longer seen as taboo and individual rights and interests achieved a more prominent position, giving the individual, a more effective protection of their individual rights.

Reform and Opening Up also had an impact on cultural perspectives. Through the 'open gate', Western values, habits and practices gradually permeated throughout the society and progressively influenced people's lifestyles. Moreover, an increasing number of Chinese scholars began studying overseas in order to broaden their horizons and enhance their knowledge. When they returned to their homeland, they inexorably shared their experiences. Western ideals advocate individual personality and praise development of individual characteristics. That tendency supports a more individualistic consideration of individuals and of their rights. Due to the rapid development of urban areas, more and more people from rural regions migrated into dense urban environments. Consequently, people that were accustomed to living in intimate conditions with their family members and neighbours began living in a diverse environment and experiencing other individuals with differing regional traditions and cultures. One result was that citizens were more reticent to share their privacy with others but also, they were not interested in others private affairs as they were in their home villages.

Moreover, China has been through a gigantic digital revolution. New technologies and popularization of the Internet made possible entering into a new dimension, the cyberspace. Indeed, with China's embrace of digital economy, an understanding of privacy's importance has followed and as a consequence, the concept of privacy evolved as well.

The Academic Development

Following the social and cultural trend and the promulgation of relevant judicial interpretations of the Supreme Court in 1988,[4] legal scholars, having as a parameter the

4 The judicial interpretation is 'Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (for Trial Implementation) 1988'.

precedent experience of Western colleagues, began developing their own explanation of the right to privacy.

In 1997, two scholars, professor Wang and professor Yang defined the right to privacy as the 'right enjoyed by natural persons, under which the person is free from publicity and any other interference by others regarding personal matters related to the person or to his personal information such as affairs in the area of personal life' (Cao, 2005, p. 147). This idea of privacy is strongly affected by the private-public dichotomy and has been a first attempt to introduce a modern notion of privacy into the Chinese legal debate. In the following years, many other speculative attempts were implemented. In the description provided by Professor Yang Lixin, the right to privacy is the 'right that allows the protection of private information, private activities and private space, which cannot be interpreted as arbitrary expansion or restriction' (Yang, 2000, p. 26). In a different but similar way, Professor Zhang states that 'the right to privacy is the personality right enjoyed by citizens and protected by law, and other people shall not illegally disturb, know, collect, use and make public' (Zhang, 2002, p. 41). Another significant delineation was offered by Professor Wang Liming, who affirms that 'the right of privacy is a right of personality, enjoyed by a natural person, under which he can dispose of all personal information, private activities and private areas which only belongs to the person and have no relation to public interest' (Wang, 2005, p. 4). All those speculations make clear the inclusion of the right to privacy into the category of personal rights and the difficulty of giving a single monolithic definition of the right itself, but they also show the increasing attention given to the problem and the will of the scholars to find a theoretical solution.

In the following decades, an increasing number of scholars began developing the study of information statutes and discussing its impact on data protection laws and they joined in conferences and seminars to study these new ideas.[5] The Chinese academy has committed itself to formally determine its legal paradigm of personal information protection.

5 In Fall 2017, the theme of the 'Forum of Legal Study' was 'Legal Mechanisms for the Use and Protection of Personal Information'.

Legislative Framework

From the Early Stage to the Present

The first normative document which explicitly states the protection of personal information was promulgated in 1994 by the State Council.[6] In December 2002, the 16th Congress of the Chinese Communist Party approved a new draft of civil code that guaranteed legal protection to human dignity, including the right to privacy. In 2004 the 'Implementation Opinions on Information Security Level Protection' (*guanyu xinxi anquan dengji baohu gongzuo de shishi yijian*, 关于信息安全等级保护工作的实施意见) and in 2007 the 'Information Security Level Protection Management Measures' (*xinxi anquan dengji baohu guanli banfa*, 信息安全等级保 护管理办法) were published. In both documents, protection of personal information was not well integrated into the system as a legal category. Privacy was still a nebulous concept in the legal discussion and the protection of personal information was not yet well established.

In 2009, the Tort Law of People's Republic of China prescribed for the first time a tort for the violation of the right to privacy. In the same year, with the seventh amendment to the Criminal Law, two new crimes concerning the protection of personal information were introduced: illegal selling or providing of personal information (article 253, paragraph 1) and illegal theft or obtaining personal information in any matter (article 253, paragraph 3). From 2010 through 2020, several important policies were implemented to strengthen personal privacy protections.

In 2010, the Government published a white paper[7] entitled 'Internet in China' (*zhongguo hulianwang zhuangkuang*, 中国互联网状况). In the document, the importance of protections of citizen's online privacy that is 'closely connected with people's sense of security and confidence in the Internet' was highlighted, and the paradigm that 'Internet service providers are responsible for protecting users' privacy' was established.

In late 2012, the Standing Committee of the National People's Congress, in order to guarantee people's online privacy, published the 'Decision on Strengthening Protection of Online Information' (*guanyu jiaqiang wangluo xinxi baohu de jueding*, 关于加强网

6 I am referring to the 'Regulations of the People's Republic of China on Computer Information System Security Protection' (*jisuanji xinxi xitong anquan baohu tiaoli*, 见算计信息系统安全保护条例).

7 The 'White paper' has been published the 8 June 2010 by the Information Office of the State Council of the People's Republic of China.

络信息保护的决定). The primary purpose of this document was to protect citizen's personal online information and online privacy and to safeguard the public interest.

In 2013, an amendment to the Consumer Protection Law introduced new dispositions regarding the protection of personal information by providing special legal protections for the consumers (article 14), by setting up rules, principles and limits for their collection (article 29) and by establishing compensation modalities (articles 50 and 56).

In 2015, the ninth amendment to the Criminal Law established heavier penalties for violations of personal information protection duty for those people who committed the crime while performing work-related activities or while providing services.

On 27 July 2016, the General Office of the State Council and the General Office of the Central Committee of the Communist Party of China published the 'Outline of National Information Development Strategy' (*guojia xinxihua fazhan zhanlve gangyao*, 国家信息化发展战略纲要) which provided for 'moving forward with the construction of a rule of law in the cyberspace' by 'strengthening the protection of network users' rights, researching the formulation of a personal information protection law, and regulations to protect minors online' and to 'comprehensively standardize acts by enterprises involving in the collection, storage and use of personal information, and prevent information abuse'.

In 2017, the National People Congress promulgated the General Principles of Civil Law, where, in Article 111, it prescribed that 'any organization or individual needing to obtain the personal information of other persons shall legally obtain and ensure the security of such information, and shall not illegally collect, use, process, or transmit the personal information of other persons, nor illegally buy, sell, provide or publish them'. In the same year, the freshly promulgated Cybersecurity Law (*zhonghua renmin gongheguo wangluo anquan fa*, 中华人民共和国网络安全法) addressed data and personal information protection comprehensively at a national law level for the first time, with an unprecedent detailed regulation.

In 2018, the 'Personal Information Security Specification' (*geren xinxi anquan guifan*, 个人信息安全规范) was officially published.

In 2019, the 'Provisions on Cyber Protection of Children's Personal Information' (*ertong geren xinxi wangluo baohu guiding*, 儿童个人信息网络保护规定) were issued.

In the official draft of the future Civil Code, which will hopefully be promulgated in 2020, in the Third Part concerning the personal rights, the Sixth Chapter is entitled 'Right to privacy and personal information' and contains several meticulous dispositions in such matters.

As it is clearly shown in the brief outline above, Chinese efforts in regulating the legal framework of protection of personal information has been substantially increased in the past decades. The legislators' approach seems multidisciplinary, many provisions are disseminated in multiple levels and in different area documents. It is not just laws, but also white papers and administrative regulations, and new standards are aligned with the legal tools used to implement the rules.

Privacy and Personal Information Protection Discipline

The Constitution of the People's Republic of China, doesn't provide a direct protection for privacy as understood in its broad meaning of a 'right to be alone' or a 'right to control your own personal information'.[8] According to some scholars, consequently, the Constitution provides inadequate protection, which can serve, at most, as a foundation for further developments (Cao, 2005, p. 660). The constitutional protection for privacy in China is currently very limited (Hao, 2011, p. 65). Comparatively, not

8 The *Constitution*, instead, after prescribing, in its Article 37, that the freedom of the person of citizen is inviolable and that unlawful detention or deprivation or restrictions of citizen freedom same as unlawful search of the person is prohibited and affirming, in its Article 38, that '*the personal dignity of citizens of the People's Republic of China is inviolable*', clearly refers to the traditional 'right of confidentiality', in its Article 39, by providing that '*the home of citizens of the People's Republic of China is inviolable. Unlawful search of, or intrusion into, a citizen's home is prohibited*', and to the 'right of privacy of correspondence', by its Article 40, providing that '*the freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or of investigation into criminal offenses, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law*'. Another interpretation could be the one that affirms that the *right of privacy* could be guaranteed in the Chinese legal system through the general clause contained in the Article 33 of the *Constitution* ('*The state respects and protects human rights*'), especially considering how the *right of privacy* has nowadays transcending the dimension of civil law (the *Universal Declaration of Human Rights*, in its Article 12 states that '*no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to protection of the law against such interference or attacks*').

many Constitutions among those in force on the planet protect the right of privacy as intended in this extensive meaning.[9]

A notable legal development for data protection was made 1 June 2017 with the entering into force of the Cybersecurity Law[10] (hereinafter 'CSL') which provides, at the time of its adoption, the most widespread and comprehensive discipline regarding privacy and personal data protection in China. Its content is innovative and aligns the degree of protection to the highest standards by considering other countries' legislations (*in primis* the European GDPR and the U.S. laws).

The CSL is a piece of legislation which has to be seen as a 'part' of wider plan of the Chinese legislator for establishing national security rules (Moriconi, 2019, 98). The purpose of the law is 'guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization' (Article 1). The Fourth Chapter is related to 'Network Information Security' but other provisions concerning the protection of data can be found in other dispositions of the law.

---

9 According to a comparative analysis, made by checking in how many Constitutions of other countries is present the syntagma 'right to privacy', it can be found that it is present in 180 Constitutions of countries in the World. However, some of them just mention it relating its meaning to the traditional concepts of 'privacy of correspondence' or 'domicile or home inviolability' (like the *Constitution of Germany, 1949, rev. 2014*, the *Constitution of Italy, 1947, rev. 2012*, the *Constitution of the Democratic People's Republic of Korea, 1972, rev. 2016*, the *Constitution of the Republic of Korea, 1948, rev. 1987*, the *Constitution of the Russian Federation, 1993, rev. 2014*,) and some other legal systems, even if they don't include it expressively in the Constitution, provide the guarantee of the right by other means (like the *Constitution of the United States of America, 1789, rev. 1992*, by using the *Amendment 9 – Construction of Constitution* of the *Constitution*, that clearly states that '*the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people*'). Very few countries clearly mention the protection of personal data (like the *Constitution of Portugal, 1976, rev. 2005,* in its Article 35: Use of Computers, the *Constitution of Spain, 1978, rev. 2011*, in its Section 18.4, the *Constitution of Switzerland, 1999, rev. 2014*, in its Article 13 – Right to privacy).

10 For completeness, regarding the legal framework prescribed by the CSL, it has to be pointed out how some other legal documents, guidelines and national standards, weekly published, are functional as a support to help organizations to comply with data protection obligations imposed under the Law, those are: the Draft Guidelines on Multi-Level Protection Scheme for Information Systems (released on June 27, 2018), the Draft National Standard of Information Security Technology – Guidelines for Personal Information Security Impact Assessment (released on June 11, 2018), the Draft National Standard of Information Security Technology – Guidelines on Data Security Capability Maturity Model (released on September 29, 2018) and the Draft Guideline for Internet Personal Information Security Protection (released on November 30, 2018).

The CSL defines personal information as 'all kinds of information recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural's person personal identity, including but not limited to the natural person's name, date of birth, identity certificate number, biology-identified personal information, address and telephone number' (Article 76.5) and what constitutes 'network data' ('all kind of electronic data collected, stored, transmitted, processed and generated through the network', Article 7.4).

Article 22 of the CSL prescribes the general duty, for all the products and services providers that collect user's information, to explicitly notify their users and to necessarily obtain their consent. In the case where personal information is involved, there is a duty to comply with all the relevant law and administrative regulations regarding the protection of personal information. Article 37 sets another duty, but this time just for critical information infrastructure operators which collect or produce personal information or 'important data',[11] to store those inside the country, and in case that information and data are needed to be provided abroad for business reasons, it is necessary to conduct a security assessment, according to the measures provided by the Cybersecurity Administration of China in accordance with the relevant department of the State Council.

The Fourth Chapter (from Article 40 to Article 50), as previously discussed, is the core of the regulation regarding the protection of personal information. Specific requirements within each Article are described in the following:

Article 41 and Article 42 recognize the three essential features of the information (confidentiality, necessity and integrity), and in order to assure the safety of the collection of the information, ensure the guarantee of its legitimate use and of their subsequent protection.

Article 41 provides principles that must be followed by network operators while collecting and using information: the principle of legality (*hefa de yuanze*, 合法的原则), the principle of rightfulness (*zhengdang de yuanze*, 正当的原则) and the principle of necessity (*biyao de yuanze*, 必要的原则). Moreover, the CSL recognizes to any subject of 'data treatment' the right to asking the network operator to delete personal information which are collected or used 'against the law' (*contra legem*) and also the

11 The meaning of 'important data' is not specified in the CSL, but according to the Cyberspace Administration of China, are those 'data closely related to national security, economic development and social public interest'.

right to ask for corrections in case the personal information contains any error or mistake (Article 43).

Article 45 sets the duty for staff members of departments that assume cybersecurity supervision and administration functions to keep strictly confidential any personal information, privacy and commercial secrets to which they have access while performing their functions and the duty of not divulging, selling or providing such information to any other entity.

The CSL sets sanctions that must be applied in case of violations of the abovementioned disposition. The range is wide. In case of lighter violations, the authority can force to take corrective actions, give it a warning, confiscate the illegal income and impose a fine up to RMB 1.000.000 (approximately Euro 130.000) plus a fine from RMB 10.000 up to RMB 100.000 to the person directly responsible or another directly liable person (approximately Euro 1.300 and Euro 13.000 respectively). In case the circumstances are more serious, the authority can take measures such as suspending the relevant business operation, ceasing business operation for rectification, closing down the website or revoking the relevant business permit or business license.

In substance, the law is very innovative. It introduces into the Chinese legal system many new rules that push forward the framework of personal information protections and put them into a systematic order. It introduces for the first time the duty for service providers who collect personal information to explicitly notify and obtain the consent of the user in order to collect data. It officially recognizes three main structural elements of the data (confidentiality, necessity and integrity), it postulates the principles (of legality, rightfulness and necessity) that must be followed by operators that threaten data and recognise two important rights, the 'right to ask the deletion of an information illegally obtained' and the 'right to ask for modifying incorrect information' that make the safeguard of the individual more effective.

Other significant legal documents providing a detailed layout of the many aspects concerning the protection of personal information are: the 'Decision of Strengthening Online Information Protection' (effective from 28 December 2012), the 'National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services' (effective from 1 February 2013) and the recent 'National Standard of Information Security Technology – Personal Information Security Specification' (effective from 1 May 2018, hereinafter, the 'Standard').

Looking from the perspective of the legal effects that those documents have within the Chinese legal system, it is worth noting that while the Decision has the same legal effect of a law and primarily provides a general overview of the guiding principles relating to data protection, the Guidelines and the Standard are 'technical guides', in the sense that they are not legally binding and that they cover by regulating in details, key issues such as data transfers, sensitive personal information and data subject rights.

Specifically, we will proceed by analysing the Standard,[12] which lays out granular guidelines for obtaining the consent for how personal information should be collected, stored, used, shared and transferred. In fact, the Standard is the most extensive document to date regarding the protection of personal information in China. In order to achieve a comprehensive understanding and to pursue a complete interpretation of the relevant dispositions, it has to be analysed as one of the systems created through the CSL.[13]

The Standard is composed of ten 'chapters' that include a total of forty-six points. The first two 'chapters' are respectively 'The scope' and 'Normative references', while the following section concerns the terms and definitions that are used in the legal document itself. By reading the provisions, is immediately clear how the Standard provides more detailed and meticulous rules than those in the CSL. Comparing the definition of personal information provided by the two documents, we find that the wording is the same, but in the Standard, and specifically in its Appendix A, a very extensive list of

12 The most important legal act regarding the discipline of standards in China is the 'Standardization Law of the People's Republic of China', promulgated the December 29th, 1988 and amended the January 1st, 2018. According to their binding force, the Law set four type of standards: 'national standards', 'recommended national standards', 'group standards' and 'completely voluntary standards'. As shown in the classification of 'GB/T' of the 'Personal Information Security Specification', it falls in the category of 'recommended national standards', which, in terms of actual effectiveness, is between 'compulsory' and 'voluntarily'.

13 Other systems are the 'Content Management System', the 'Critical Information Infrastructure Protection System', the 'Network Product and Services Management System', etc. Together they form the framework that regulates the Information and Communication Technologies (ICT) in China.

prototype of personal information[14] with the logic of the procedure of recognition of those information is provided.[15] This double approach allows inclusion of information into the category of personal information through two different patterns: some information is 'by definition' personal information, and another way, some information that may not be included in the list is 'reached' and then included into the category throughout a logical process.

Furthermore, the Standard, differently from the CSL, creates a sub-category of the general personal information that is constituted by that information that is 'sensitive'. According to Point 3.2, 'personal sensitive information' are those that 'once leaked, illegally provided, or abused, can threaten personal and property security and/or

14 The list is very detailed and includes: **personal profile** (personal name, birthday, gender, nationality, nationality, family relationship, address, personal phone number, e-mail, etc.), **personal identity information** (ID card, officer card, passport, driver's license, work permit, pass, social security card, residence permit, etc.), **personal biometric information** (personal gene, fingerprint, voiceprint, palmprint, auricle, iris, facial features, etc.); **network identity information** (system account, IP address, email address and password, passwords, password protection answer, etc.), **personal health physiological information** (relevant records generated by personal illness treatment, such as disease, hospitalization records, medical orders, inspection reports, operation and anaesthesia records, nursing records, medication records, drug and food allergy information, birth information, previous medical history, diagnosis and treatment, family history, current medical history, infectious disease history, etc., as well as relevant information generated by personal physical health, weight and height , vital capacity, etc.), **personal education information** (personal occupation, position, work unit, education background, degree, education experience, work experience, training record, report card, etc.), **personal property information** (bank account number, identification information, password, deposit information including fund quantity, payment and collection record, real estate information, credit record, credit information, transaction and consumption record, flow record, etc., as well as virtual property information such as virtual currency, virtual transaction, game exchange code, etc.), **personal communication information** (communication records and contents, SMS, MMS, e-mail, data describing personal communication, metadata, etc.), **contact information** (address book, friends list, group list, email address list, etc.), **personal online record** (it refers to the user's operation records stored through the log, including website browsing records, software use records, click records, etc.), **personal common device information** (it refers to the information describing the basic situation of personal common equipment, including hardware serial number, MAC address of equipment, software list, unique equipment identification code, such as IMEI/android ID/IDFA/OPENUDID/GUID, SIM card IMSI information, etc.), **personal location information** (including track, precise positioning information, accommodation information, latitude and longitude, etc.), **other information** (marriage history, religious belief, sexual orientation, unpublished criminal record, etc.).

15 The process is quite logic and coherent, in fact, in order to conclude that an information is a personal information there are two ways: the first one, through a process of 'identification', that is from information to individuals, from the particularity of the information itself to identify a specific a specific natural person, in this case personal information should be helpful to identify a specific individual; the second one, through a process of 'association', that is from individuals to information, that is when, if a natural person is known, the information generated by the specific natural person in its activities is personal information. An information meeting one of those two conditions shall be determined as personal information.

easily cause personal reputational damage, physical and mental health damage, or discrimination'. For that kind of information, the focus is on the relevance of the interest that needs to be protected, that is to say, the individual and his properties that may be damaged by the uncontrolled spread of such information. Appendix B of the Standards indicates a general approach in order to recognize those types of information and provides a list of examples.[16]

Also, the Standard defines two main subjects of the collection of information: the personal information subject ('the natural person identified by personal information', Point 3.3) and the personal information controller ('an organization or individual that has the authority to determine the purposes and/or method of processing personal information', Point 3.4). After setting those two definitions, the discipline of some key-activities follows, such as the collection (Point 3.5), the acquisition of explicit consent (Point 3.6), the user profiling (Point 3.7), the personal information security impact assessment (Point 3.8), the deletion (Point 3.9), the public disclosure (Point 3.10), the transfer of control (Point 3.11), the sharing (Point 3.12), the anonymization (Point 3.13) and the de-identification (Point 3.14).

Some fundamental principles regarding the security of personal information security that should be followed by controllers are prescribed in Point 4 (the commensurability of power and responsibilities principle (that impose to bear the responsibility for the damages cause to the lawful rights and interests of the personal information subject caused by the personal information process); the purpose specification principle (that impose that the purposes of the process must be legal, justified, necessary and specified); the consent principle (in force of which is necessary to obtain the consent of the

16 The list includes: **personal property information** (bank account number, identification information, password, deposit information, like fund quantity, payment and collection record, real estate information, credit record, credit information, transaction and consumption record, flow record, etc., as well as virtual property information such as virtual currency, virtual transaction, game exchange code, etc.), **personal health physiological information** (relevant records generated by personal illness treatment, such as disease, hospitalization record, medical order sheet, inspection report, operation and anaesthesia record, nursing record, medication record, drug and food allergy information, birth information, previous medical history, diagnosis and treatment situation, family medical history, current medical history, infectious disease history, and relevant information generated by personal physical health status, etc.), **personal biometric information** (personal gene, fingerprint, voiceprint, palmprint, auricle, iris, facial recognition features, etc.), **personal identity information** (ID card, officer card, passport, driver's license, work card, social security card, residence card, etc.), **network identity information** (system account, email address and password, password, password protection answer, user's personal digital certificate related to the above), other information (personal phone number, sexual orientation, marriage history, religious belief, unpublished criminal record, communication record and content, track, web browsing record, accommodation information, accurate positioning information, etc.).

personal information subject after expressively providing him with the purpose, method, scope and rules of the processing); the minimization principle (according to which only minimum type and quantities of personal information must be processed); the openness and transparency principle (by which the scope, purposes, rules of personal information should be open to public in an explicit, intelligible, and reasonable manner, and the outside supervision should be accepted); the ensuring security principle (by which is needed to possess the appropriate security capacity to safeguard the confidentiality, integrity and availability of personal information); the subject participation principle (by which means to access, correct and delete the personal information, to withdraw consent and to close accounts must be provided to the personal information subject). The Point 5 is related to the collection of personal information, provide requirements in order to operate a legitimate collection, rules about how to obtain the consent and some exceptional cases in which the consent is not required, it also sets guidelines regarding the request of explicit consent for the collection of personal sensitive information and for the publication of privacy policy.

The final points contain rules for the correct retention of personal information by collectors (Point 6), about the use (Point 7), about the delegated processing, sharing, transfer, and public disclosure of personal information (Point 8), on how to handle incidents (Point 9) and on the requirements for the organizational management (for example, it required to appoint a person responsible for PI protection and to designate a department in charge of PI protection, or to carry out PI security impact assessment, etc., Point 10).

As clearly stated, the Standard laid out a meticulous regime relating to personal information protection, in which the true will of the personal information subject is respected, and his interests are strongly protected. An objection can be made in the way that even if the rules provided by the Standard are more detailed and wide-ranged, they still don't have a binding force as the CSL does. Considering the specific legal and social system in which those rules are based, I will note that those rules can easily result in being implemented in force of the voluntary compliance of the enterprises and that, moreover, when laws, administrative regulations, mandatory standards, court or administrative decisions invoke them by quoting or by referring to them, they will gain a legally binding effect indirectly, and they will produce the same binding force as the documents that cite them. In determining the usefulness of the Standard, one can see this regulation as an important signal in releasing the will of Chinese government and legislators in striving to protect the security of personal information.

A Case Analysis

In order to better understand the degree of protection accorded to the right of protection of personal information, it may be useful to have a look at some cases concerning the privacy right violation.

With the rapid development of technologies and the fast dissemination of information, a large number of issues concerning the protection of personal information starts to occur in the Chinese daily life. The improper spreading and use of personal information have gradually become a social issue harming the civil rights of citizens. Logically, most of the cases arise when customers buy goods or services by using an online platform.

In the 'Pang Lipeng v. China Eastern Airlines Co. Ltd. and Beijing Qunar Information Technology Co. Ltd.', a case of 2017, the dispute was over an infringement upon citizen' right to privacy arising from online ticketing involving an airline company (China Eastern Airlines) and a famous online ticketing platform (Qunar). The plaintiff, having booked a flight through the online platform, received from an unknown mobile number fake information about his flight. He sued the company for having not assured an adequate protection of his personal information and let strangers access them. In this case, the divulged information of Pang Lipeng (name, mobile phone number and flight schedule) were caused by the airline and ticketing platform company's negligence to take adequate precautions. Therefore, the judge decided they were at fault and that they shall assume their liability for the infringement.

In a similar case, the plaintiff ordered a flight ticket through a mobile phone app platform but his information (traveller's name, flight date, landing place, flight number and reservation phone number) were leaked and consequently the customer was defrauded. The Court identified two relevant principles, the one that in the protection of personal information, the focus has to be in information identification relationship and not in the information itself and the other that in disputes arising from the companies' use of personal information for business activities, individuals are in a weak position and so declared that the company in such a case has not fulfilled its obligation to keep and prevent leakage of personal information and should bear liability.

In another case, 'Yan v. Beijing Sina Interconnection Information Service Co., Ltd. and Beijing Baidu Netcom Technology Co., Ltd.', some Sina bloggers published articles in which a plaintiff's personal information was disclosed to the public. The plaintiff sent to the two companies (Sina and Baidu) two letters and required them to take necessary measures such as deletion of those articles and providing the authors' information.

But while Baidu did take such measures, Sina didn't. The People's Court of Haidian District, Beijing Municipality held that Sina should assume the legal consequences of this behaviour. This case is quite interesting in the way it shows how to find a balance between the interest of determining the identity of an infringer for allowing the plaintiff to maintain his right and the opposing interest of the Internet company to fulfil its duty of keeping confidential the information of its network users.

Since the CSL entered into effect, one of the largest fines targeted the operator Luoyang Beikong Water Group. When the company's remote data monitoring platform was hacked, law enforcement determined that their data had not been sufficiently secured, and subsequently the company was fined for RMB 80.000 and three managers a total of RMB 35.000.

Baidu, Alibaba and Tencent and other big players in China's internet have seen trouble over content moderation policies. In September 2017, the Cyberspace Administration of China fined Baidu and Tencent for failing to manage pornographic and violent content on their platform. In January 2019, Baidu, Alibaba and Bytedance's Toutiao were asked to meet with authorities for failing to respect their user right to know what data was collected.

By analysing the judgements concerning the application of CSL and other regulations it seems that the jurisdictional protection is quite efficient in the way it implements the rules.

Conclusion and Perspectives

In order to draw some conclusions, it may help to address some reflections.

Firstly, the Western discussion on the right to privacy has in some degree influenced the discussion in China. Chinese laws and regulations on data privacy arrives some decades after than in the U.S. or in EU, but that doesn't have to be perceived negatively. In fact, Chinese scholars took Western experiences as a model giving them a factual advantage providing a solid basement for their original theorization and development. That is exactly what happened since the beginning: China started to develop its own framework through sectorial laws (like in the U.S.) while now, the country is on the path of enacting a comprehensive data protection law (like the EU).

Considering the theoretical development of the data protection scholarship, from a comparative perspective, American law pays more attention to the use of personal information to promote the development of data industry, and on the opposite European law is more focused on the protection of individual rights. China seems to follow a third way: it starts from the practical need of developing the data industry but also pays attention to the protection of individual's right in order to ensure an orderly and healthy development (Wang, 2019, 56).

Foreign experience is important but is not the only element of the process. As a well-known Chinese idiom says, it is important to adopt the Western knowledge for its practical uses while keeping Chinese values as the core. This idea is reflected in the way Chinese scholars are attempting to find the best legal approach to this phenomenon. In fact, during the academic discussion, some original ideas emerged. An example is the theory of the principle of "two-headed strengthening, three way-balance"[17]. Another unique pattern of the Chinese approach is evident in the way it affirms the principle of 'cyberspace sovereignty'. One of the consequences of the application of this principle in the field of privacy and data protection is the regime of cross-border data transfer of personal information processed by critical information infrastructure (CSL, Article 37). In fact, those can be transferred out of the country only when it is strictly necessary and after passing a security assessment. A similar obligation to store personal information within the country is not found in either U.S. or EU law.

It is important to understand these policies are still developing. Currently, China doesn't have a comprehensive data protection law but the will of the government to work for it has been made clear on 10 September 2018, when the Standing Committee of the National People's Congress of China updated its legislative agenda and planned to enact it by March 2022. However, even without it, the general legal framework can be described as very effective and well-structured even if it lacks a systemic and cohesive approach. A good turning point has been made with the promulgation of the CSL; with its promulgation the protection of the online user's personal information entered into a new stage and this can be considered a valid temporary measure. It is innovatively, in that it separates personal information rights from privacy rights; it includes the

17 In which 'two-headed strengthening' refers to differentiating between personal information and sensitive personal information in order to create value, in fact it allow to support the exploitation of the former and at the same time to strengthen the protection of the latter and 'three way-balance', refers to the necessary balance that has to be found between the interests of the individuals in the protection of personal information (which core is the freedom of personality and the respect of personal dignity), the interests of information collectors in the use of personal information (the core is to obtain economic benefits through business activities), and the public interest of the state management society.

protection of personal online information as a fundamental civil right and leverages its legal *status quo* and it seeks to establish the paradigm that Internet service providers, either individual or organizations, must undertake the responsibility for data protection.

While the CSL is currently the most authoritative law protecting personal information (it can be considered a milestone of data protection law in China), the Standard is the regulation that provides the most detailed guidance for compliance in information processing. The discussion on the effectiveness and function of Standards, fully reveals the complexity of personal information protection in China. Unlike the CSL that applies only to network operators, the Standard applies to all types of entities in China using information system to process personal data. Furthermore, with the Standard the stereotype that 'Chinese government and companies are committed to collect personal data in order to create a social credit score for everyone' falls and China can officially aim to become the frontrunner of privacy protection in Asia.

Moreover, the new adopted Civil Code of People's Republic of China, approved on May 28, 2020 by the Third Session of the 13th National People Congress, specifically disciplines privacy and personal information protection. In the part of the code that regulates the personality rights (Book Fourth of the Civil Code), in the Chapter VI, there are eight articles (from Article 1032 up to Article 1039) in such matters. The new code prescribed protection for personality rights as an independent compiled part. That is an innovation that maximizes and strengthen the protection of those rights within the Chinese civil law system. From the substantial perspective the provisions of the Code don't prescribe anything different from what the CSL and the Standards stipulate. They are innovative in the way they find a systematic position within the Chinese Civil law system for those rights (to privacy and to personal information protection).

Finally, even if it is right to look into the future of personal information protection, it is also important to give attention to the unsolved issues that are still on going. For example, the interpretation of Article 111 of the General Principles of Civil Code; for some, the enactment of this Article implies that China endorses citizen's fundamental right to 'information self-determination', others argue that this article only admits the need for personal information protection and does not mention the right to personal information as a fundamental right.

Bibliography

Adams, E. L. (1905) *The Right of Privacy, and Its Relation to the Law of Libel*, American Law Review, Vol. 39.

Barrington Moore, Jr. (1984) *Privacy. Studies in Social and Cultural History*, M. E. Sharpe, Inc.

Cao, J. (2005) *Protecting the right to privacy in China*, Victoria University of Wellington Law Review, 645.

Deng, X. (2018) *Personal data protection: rethinking the reasons, nature, and legal framework*, Frontiers of Law in China (Special Issue), Vol. 13(3).

Diliberto, O. (2012) *La lunga marcia. Il diritto romano nella Repubblica Popolare Cinese*, Disegnare il futuro con intelligenza antica. L'insegnamento del latino e del greco antico in Italia e nel mondo, Bologna.

Fei, X. (1992) *From the Soil. The Foundations of Chinese Society (A Translation of Fei Xiaotong's* Xiangtu Zhongguo *with an Introduction and Epilogue by Gary G. Hamilton and Wang Zheng)*, University of California Press, Berkeley.

Fei, X. (2015) *Globalization and Cultural Self-Awareness*, 1st edn., Foreign Language Teaching and Research Publishing Co., Ltd and Springer-Verlag, Berlin Heidelberg.

Kalven, H. (1966) *Privacy in Tort Law – Were Warren and Brandeis Wrong?*, Law & Contemporary Problems, Vol. 31.

Hao, W. (2011) *Protecting Privacy in China. A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, 1st edn., Springer, London.

Hong, X. (2009) *Privacy and Personal Data Protection in China: An Update for the Year End 2009*, Computer Law and Security Review.

Hong, Y. (2018) *Responses and explanations to the five major concerns about the Personal Information Security Specification* [Online]. Available at: https://mp.weixin.qq.com/s/rSW-Ayu6zNXw87itYHcPYA (accessed 19 February 2020).

Moriconi, C. (2019) *Legge sulla sicurezza informatica della Repubblica Popolare Cinese. Nota alla traduzione*, Roma e America. Diritto romano comune, Vol. 40.

Min, J. (2010) *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, The SAIS Review, Volume 30(2), Summer-Fall 2010.

Pernot-Leplay, E. (2020) *China's Approach On Data Privacy Law: A Third Way Between The U.S. And The EU?*, Penn State Journal of Law & International Affairs, Vol. 8(1).

Pohl, K. (1993) *Zu Beiträgen Li Zehous in der Debatte um Tradition und Identität in den 80er Jahren in der Volksrepublik China* ('Western Learning for Substance, Chinese Learning for Application' – Li Zehou's Thought on Tradition and Modernity), Sinologische Traditionen im Spiegel neuer Forschung (Sinological traditions in the mirror of new research), Leipzig.

Prosser, W. L. (1960) *Privacy*, California Law Review, Vol. 48, 383.

Rodotà, S. (2014) *Il mondo nella rete. Quali diritti, quali vincoli*, 1st edn. Bari: Gius. Laterza & Figli – Gruppo Editoriale L'Espresso.

Sacks, S. (2018) *China's Emerging Data Privacy System and GDPR* [Online]. Available at: https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr (accessed 9 October 2019).

Schipani, S. (2005) *Iustiniani Augusti Digesta Seu Pandectae. Digesti o Pandette dell'Imperatore Giustiniano. Testo e Traduzione*, Università degli Studi di Roma Tor Vergata – Pubblicazioni della Facoltà di Giurisprudenza, I 1-4, Giuffrè Editore, Milano.

Shils, E. (1966) *Privacy: Its Constitution and Vicissitudes*, Law and Contemporary Problems, Privacy (Spring), Vol. 31(2), 281-306.

Tomba, L. (2006) *In transito? Riforme, continuità e tecniche di governo in Cina*, Il Politico, Cina: l'avvio del terzo millennio (Settembre-Dicembre 2006), Rubbettino Editore, Vol. 71(3) (213), 54-70.

Wang, L. (2005) *Study on the law of personality rights*, 1st edn. China Renmin University Press, Beijing.

Wang, L. (2019) *Data sharing and personal information protection*, Modern Law Science, Vol. 41(1).

Wang, L. and Yang, L. (1997) *The Law of The Right of the Person*, 1st edn. The Press of Law, Beijing, quoted by Cao, J. (2005) 'Protecting the Right to Privacy in China', Victoria University of Wellington Law Review.

Warren, S. D. and Brandeis L. D. (1890) *The Right to Privacy*, Harvard Law Review, 193.

Westin, A. F. (1968) *Privacy and Freedom*, Washington and Lee Law Review, 166.

Yang, L. (2000) *Several issues on privacy and its legal protection*, 1st edn. People's Procuratorate, Beijing.

Zhang, X. (2002) *The legal protection of privacy*, 1st edn. Mass Publishing House, Beijing.

Zhang, X. (2016) *The right to privacy and the personal information protection* [Online]. Available at: http://www.legalinfo.gov.cn/index/content/2016-05/12/content_6622867.htm?node=66707 (accessed 10 October 2019).