CSCanada
Canadian Social Science
Vol. 14, No. 9, 2018, pp. 30-36
DOI:10.3968/10582

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

Research on Chinese Personal Information Protection Legislation in the Era of Big Data

CHENG Ying[a],*

[a]Ph.D. candidate. Institute for Human Rights, China University of Political Science and Law, Beijing, China.
*Corresponding author.

Received 29 June 2018; accepted 10 September 2018
Published online 26 September 2018

Abstract
In Chinese personal information protection legislation, consent should not be the sole legal basis for data processing, and data processing under regulation should be encouraged. At the same time, the accountability of data controllers and the transparency of data processing should be improved, and risk-based approaches should be introduced to provide proportional, situational and low-cost regulatory regulation.

Key words: Personal information protection; Big data; Accountability; Transparency; Consent

Cheng, Y. (2018). Research on Chinese Personal Information Protection Legislation in the Era of Big Data. *Canadian Social Science, 14*(9), 30-36. Available from: http://www.cscanada.net/index.php/css/article/view/10582
DOI: http://dx.doi.org/10.3968/10582

INTRODUCTION
The development of new technologies and the continued globalization of the economy and the society have led to a proliferation of the personal information that is collected, sorted, transferred or otherwise retained. The risks to such data therefore multiply. With the rapid development of the Internet and the popularization of the digital economy in China, the current personal information protection model has failed to respond to the threat. Based on the strategy to develop Internet and big data, China's policies mainly focus on the idea about network security and data sovereignty but ignore the protection of personal information rights. To be specific, the government and enterprises in China utilize the grey zone of law and abuse the big data, which generate a series of social problems. For example, there are obvious regional discrimination in the event of Today's Event Headlines. Alipay tried to collect users' consent using deception. In the face of the urgent needs for protection of personal data, it is of great significance to legislate according to the special political, cultural and social background of China and the law should meet the challenges of big data at the same time.

1. THE STATUS OF PERSONAL INFORMATION PROTECTION IN CHINA

1.1 Social Foundations of Personal Informational Protection in China
The absence of the concept of privacy in traditional culture, the idea of paternalism in government management and underdeveloped non-governmental organizations, are the major causes of the lack of information protection in China. China has a weak historical foundation for privacy recognition and protection, as it isn't valued either in Chinese philosophical traditions or more recent political history. The protection of privacy was firstly stated by The Analects of Confucius in the early days of the Warring States periods. Confucius did state that "do not watch what is improper, do not listen to what is improper, do not speak improperly, and do not act improperly." This traditional ethical sense of justice suppresses and erodes individual rights. At the same time, China has practiced a top-down patriarchal system since ancient times, which has led to the intervention from parents to children, from superiors to subordinates, from organizations to individuals. This has been a generally accepted social phenomenon. The unique status of public property in China also hinders the development of privacy protection

in China. The principle that public property and interests are 'sacred and inviolable' is a legal principle peculiar to socialist countries which are built on the foundation of public ownership.

After the founding of People's Republic of China in 1949, the concept of personal information protection in China experienced four stages, including the traditional concept of privacy, the concept of privacy in civil law, the concept of personal information protection in public law, the concept of personal in data big data era. At the same time, the concept of personal information protection developed from procedural rights to substantive rights and the rights protection methods tend to be diversified. Till now, China has not enacted a general personal information law. The current personal information protection mainly reflects in three aspects. First, some laws and regulations set specific personal information protection provisions to provide legal protection of personal information. The second is to extend the content like "personal dignity", "personal privacy" or "personal secrets" in the current legislation to the protection of personal information. The third is to set specific industry self-regulation or the unilateral commitment of information controllers and processors to protect personal information. However, over the past several years, China has enacted several important laws related to personal information protection. Altogether this body of laws and regulations could be piled up to formulate a "cumulative" information protection effect that is typical of the Chinese approach to personal information protection today.

1.2 Personal Information Legislations in China

Personal information protection is closely connected with privacy protection in China. Since the late 1970s and early 1980s, personal privacy protection provisions have appeared in the criminal law, the procedural law, and the constitution. In the field of civil law, although the "General Principles of Civil Law" promulgated and implemented in 1986 did not include privacy rights in the first place, but in the subsequent judicial interpretation published by the supreme court, an alternative approach was adopted, which recognized the infringement of the privacy as a kind of reputational damage. The "Answer to Several Questions on the Trial of Honorary Rights Cases" published in 1993 made clear provision for this. For a period after this, the Supreme Court held that the violation of privacy rights can be protected by the application of the relevant rules of reputation rights. Until the promulgation of the "Interpretation of Several Issues on Liability for Mental Injury" in 2001, privacy was officially recognized as a legal status in civil justice, and privacy interests were protected directly. In 2009, The Tort Liability Law established the legal status of privacy as a specific personality right. The Article 2 in paragraph 2 clearly stipulates that privacy right is one of the civil rights protected by the tort law. In the "General Principles of Civil Law" in 2017, Article 110 stipulates the right to privacy, and Article 111 stipulates the protection of personal information. At present, the subsections of civil law are also being drafted.

Cybersecurity Law is currently one of the most important laws in the field of personal information protection in China. The law was passed by the Standing Committee of the National People's Congress on November 7, 2016 and implemented on June 1, 2017 with a total of 79 legal provisions. One special chapter provides for the protection of personal information with 12 articles. At the same time, the law places more emphasis on the responsibilities and obligations of network operators, of which there are 34 provisions concerning network operators. The purpose of this law is to first emphasize the protection of cybersecurity, safeguarding the sovereignty of cyberspace and national security and social and public interests while emphasizing the protection of the legitimate rights and interests of citizens, legal persons and other organizations and the development of economic and social informatization.

It is the first time to add information protection into civil law when the General Rules of the Civil Law (2017) published. It applies to any organization or individual. The personal information of a natural person shall be protected by law. Any organization or individual who needs 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 the personal information of other persons.The NPC Standing Committee is China's second-highest legislative body. It amended the PRC's Law on the Protection of Consumer Rights and Interests in 2013 to include provisions on protection of personal information, along with other amendments. The amendments apply to the use of consumers' personal information by all industries, in both online and offline situations. This law applies to all consumer transactions, not only in the Internet and telecommunications sectors.

Recently, the draft of Civil Code has been released on September 5th to solicit opinions from the public. The articles related to personal information protection in the part of right of personality triggered the attention from the public. This draft stipulates the right to privacy and personal information together. The content about personal information is composed of five terms, including the legal basis of information protection, the rights of the information subjects, obligations of information controllers, the principles of information processing and exemption situations.

2. ISSUES IN PERSONAL INFORMATION PROTECTION IN CHINA

2.1 Issues in Personal Information Protection Legislation

2.1.1 Lawfulness of Processing

The information processing is legislative only when the information controllers and processors get the consent from individuals. This approach is called notice and consent which empowers individuals themselves to exercise their privacy rights as they see fit. It is generally understood as an effective means to maintain individual autonomy and achieve personal self-determination. Also, individual control theory which regards informed consent as its core is a starting point and cornerstone of the traditional information protection law in practice. However, informed consent has increasingly become the methods and reasons to evade responsibility for information controllers and processors. (Joshua, 2015). Today, almost everywhere that individuals venture, like social network, e-commerce etc., they are presented with very complex privacy policies, and then requested to either 'consent' or abandon the use of the desired service. Besides this, in the era of big data, even information controllers do not know the real value of personal information at the time of collection, when consent is normally given by individuals. So it is even more complex and realistic for individuals to fully assess the complexity of the situation. To take just one example, the New York Times reported in 2012 that one US company that few people have ever heard of engages in more than 50 trillion transactions involving recorded personal information every year.

What is more important is that the foundation of legitimacy of personal control theory or information self-determination is also impacted by the era of big data.(Purtova, 2014) The public attribute and multiple legal interests of personal information have become increasingly prominent, and the demand for the circulation and sharing of the value of information property has increased. Big data not only brings huge economic benefits to information controllers, but also brings various conveniences to consumers such as free use, high-quality services and rapid iterative innovation. (Sokol & Comerford, 2015) Accordingly, technology has fundamentally changed the concept of property rights, and it is not in line with the requirements of the age of big data to completely own or control data by individuals. A key sentiment expressed in all of the discussions is that those new approaches must shift responsibility away from information subjects towards information users, and towards a focus on accountability for responsible information stewardship, rather than mere compliance while ensuring that expectations and protection of privacy is preserved. (Cate & Schönberger, 2013). So it is not legitimate and feasible to regard consent as the necessary premise for information processing in China.

2.1.2 The Nature of Personal Information Rights

Chinese legislators and academics give too much attention to tort relief and the private law. This means that it presumes the equal status between individuals and information controllers. Qi Aimin believes that China should establish general personality rights as the basis for personal information protection. Legal protection of personal information is to protect the spiritual personality interests of information subjects. (Qi, 2004) The expansion of the connotation of privacy reflects the protection of personal information. Therefore, some scholars believe that the protection of personal information is rooted in the protection of privacy. China should base itself on the existing legal environment, respect its own social culture and values, and choose personality rights rather than privacy as the right basis for personal information protection legislation. (Xie, 2013)

However, in the era of big data, the economic value of massive information has been significantly increased, making it a new resource available for social distribution. The technology barrier makes enterprises to own the hegemony of information development and rules making. A small number of enterprises have more and more quasi-legislative, quasi-judicial and quasi-executive powers, and may play the roles of rule-maker, dispute solver and stakeholder at the same time. Collecting and collating personal information became a way to acquire power(Froomkin, 1999), and gave rise to concepts such as information power, algorithmic power, and technological power. In the context of decentralization of power, the protection of personal information in the age of big data must be considered in the tripartite framework of state, society and individual, and the three parties should be incorporated into the new power structure and confrontation model together. This means that the path of private law, such as the right of personality, the right of privacy and the right of property, is not enough to solve the problem.

We should try to explore how to realize the balance mechanism of information power in information protection law and explore the protection of personal information from the perspective of public law. Information protection may not only be about protecting a perhaps old fashioned and perhaps too rigid and too inflexible socio-psychological concept of the "self". Information protection legislation may even not only be about the right to informational self-determination in an age of local, regional, national and international social and economic dependencies. Information protection may be about the distribution of power within and between societies, addressing conflicts of power in such constellations by reframing them as informational and communicative power conflicts.(Herbert, 2009)

2.1.3 Principles

In Chinese legislation, personal information protection principles are not as comprehensive as the global practice. It stipulates legitimacy, fairness and necessity principles. Also, there are articles related to purpose limitation purpose. But there are several important principles that should be added to the legislation. The first one is information quality principle. It means that information should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal information that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Another one is the accountability principle which means controllers shall be responsible for and be able to demonstrate compliance with all the information processing principles. However, the purpose limitation purpose is inconsistent with the world of Big Data in which new uses for information are discovered over time. The language 'to be used' in the principle, 'personal information should be relevant to the purposes for which they are to be used', could be interpreted as suggesting that the determination as to relevance might need to be made only at the time of collection, with an eye toward intended use.

2.2 Issues in Personal Information Practices in China

2.2.1 Private Sector

In private sector, the protection level of personal information varies. Most of the private sectors in China do not have strong awareness of personal information protection, and there are no related personal information protection policies. Except the Internet industry, there are few private sector industries that have self-regulatory conventions to protect personal information. Some large commercial websites have been clearly aware of the great value of personal information and the significance of personal information protection to information subjects, thus providing users with relatively detailed privacy protection policies to boost their confidence in online consumption. But evidently it is not effective, and individuals usually have no choice but agree. Even badly, some small websites only make profits by over-collecting, improperly using or even illegally selling users' personal information, causing losses to users.

2.2.2 Public Sector

The management of personal information in public departments attaches more importance to duties than rights. Many public sectors in China have not fully adapted themselves from the role of public affairs managers to public service providers. They pay more attention to personal information from the perspective of management, emphasize the obligation of the subject of personal information to provide information, and ignore the basic rights that the subject of personal information enjoys with respect to its own information. There is little text on government websites at all levels like "privacy policy" published by some large commercial websites. With the gradual implementation of e-government in China, government departments have mastered a large amount of personal information submitted by citizens through the Internet. If there is a lack of personal information protection policies and measures, it may violate the legitimate interests of the subject of personal information. Information protection must move from 'theory to practice'. Legal requirements must be translated into real information protection measures.

3. ACCOUNTABILITY OF CONTROLLERS AS THE MAIN FACTOR IN LEGISLATION

The term "accountability" comes from the Anglo-Saxon world where it is in common use and where there is a broadly shared understanding of its meaning. Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed. The increase of both the risks and the value of personal information *per se* support the need to strengthen the role and responsibility of information controllers.

3.1 Justification

Information protection is embodied as a positive right and procedural right. Its main purpose is to provide various specific procedural guarantees for the protection of interests such as individual privacy, equality and autonomy, and on the other hand to promote and improve the responsibility of the government and private subjects as information controllers. This part will prove why we need to enhance the accountability of controllers.

Firstly, we are witnessing a so-called 'information deluge' effect, where the amount of personal information that exists, is processed and is further transferred continues to grow. Both technological developments, i.e. the growth of information and communication systems, and the increasing capability for individuals to use and interact with technologies favor this phenomenon. As more information is available and travels across the globe, the risks of information breaches also increase. This further emphasizes the need for information controllers, both in the public and private sectors, to implement real and effective internal mechanisms to safeguard the protection of individuals' information. (Julia, 2010)

Secondly, the ever-increasing amount of personal information is accompanied by an increase in its value in social, political and economic terms. In some sectors, particularly in the on-line environment, personal information has become the *de facto* currency in exchange for on-line content. At the same time, from a societal point of view, there is an increasing recognition of information protection as a social value. In sum, as personal

information becomes more valuable for information controllers across sectors, citizens, consumers and society at large are also increasingly aware of its significance. This in turn reinforces the need to apply stringent measures to safeguard it.

Finally, it follows from the above that breaches of personal information may have significant negative effects for information controllers in public and private sectors. Potential glitches in eGovernment, eHealth applications will have devastating consequences in both in economic and particularly in reputational terms. Thus, minimizing risks, building and maintaining a good reputation, and ensuring the trust of citizens and consumers is becoming crucial for information controllers in all sectors.

In summary, the above shows the critical need for information controllers to apply real and effective information protection measures aimed at good information protection governance, while minimizing the legal, economic and reputational risks that are likely to derive from poor information protection practice. As further developed below, accountability-based mechanisms aim at delivering these goals.

3.2 Accountability in American and EU Data Protection Law

Strengthening data usage responsibility is the basic idea of personal information protection in the era of big data in Europe and America. The United States believes that privacy protection in the era of big data should focus on the usage responsibility system, so that data collectors and users are responsible for data management and possible harm, rather than narrowly defining their responsibility as whether to collect data through normal channels. Therefore, the Consumer Privacy Rights Act regulates the accountability of data use from the aspects of employee behavior control, internal use supervision and disclosure of data to third parties. First, an enterprise should train its employees to make use of personal data in compliance situations and conduct performance evaluations on a regular basis. Second, the enterprise should carry out comprehensive internal control and supervision to ensure that the data is used within a reasonable range. Third, unless provided by law, companies that disclose personal data to third parties should at least ensure that the companies receiving such data could assume contractual obligations in compliance with the principles of the act.

In the existing legal framework, the General Data Protection Regulation further strengthened the data usage responsibility. On the one hand, the regulation requires data controllers to take appropriate measures to ensure the data processing in accordance with the law, including follow the principle of "privacy protection by design", to full lifecycle management of data, ensure the accuracy of the data, integrity, confidentiality, etc. In case of larger, more complex or high-risk data processing, the effectiveness of the measures adopted should be verified regularly. There are different ways to assess the effectiveness (or ineffectiveness) of the measures: monitoring, internal and external audits, etc. On the other hand, it is required to restrain the data processing behavior of related parties by means of contract, etc. For example, multiple data controllers should clarify their respective responsibilities by agreement, and data processors representing data controllers should restrain the data behavior of both parties by agreement or other legal means. Under such an approach the legal framework would include not only a general accountability principle but also an illustrative list of measures that could be encouraged at national level7. This provision could give an illustrative and non-exhaustive list of measures that could constitute a "toolbox" for data controllers.

4. IMPROVING CHINESE PERSONAL INFORMATION LAW

4.1 Revision of Legal Basis for Data Processing

According Chinese legislation, the usage of personal information must be subject to the "consent" of the information subject. This implies that the law recognizes that personal information is controlled by the individual, who has the right to determine whether other could and how to use his or her personal information. However, China is the only country in the world that legislatively requires the consent of information subjects for the collection and use of personal information. There is no explicit provision in the US law that the collection of personal information must be approved by the information subject, and the latest EU legislation only provides consent as one of the legal bases for the collection of personal information. European countries are affected by EU legislation and have no such regulations.

At present, only China's legislation, such as the Consumer Protection Law, the Cybersecurity Law and the draft of the personality rights in the Civil Code, explicitly requires controllers to obtain the consent of the information subject in advance. As mentioned above, this transfers risks to individuals, which is not conducive to the protection of personal interests. Therefore, foreign legislation should be used for reference to allow necessary information processing based on other legitimate reasons, such as performing contracts, performing legal obligations of information controllers, and pursuing legitimate interests of information controllers. But sensitive information can only be processed with the explicit consent of an individual, based on the need to protect human dignity. Sensitive information means those could reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or genetic information, biometric information, health or information concerning a natural person's sex life or sexual orientation.

4.2 Transparency

Transparency is an important prerequisite to ensure fair information processing and accountability, and it has become a synonym for information protection. In recent years, the concept of transparency has been attached importance to information protection legislation in various countries. The European Union's general information protection regulation stipulates transparency as one of the core principles of information processing for the first time. As information controllers occupy big data and algorithms, they gradually invade the field of public power and exercise some public management ability. The flow of personal data from the weak to the strong has become an endogenous demand for greater transparency and accountability and is an important prerequisite for enhancing public trust and effective regulation. (Tene, 2013) Transparency, as an inherent requirement of fairness and due process, embodies the idea of "quasi-administrative law" to restrict "quasi-public power". Meanwhile, in the context of big data, the theory of privacy has been difficult to cover the value of information quality and transparency. Therefore, understanding information protection from a transparency perspective is conducive to the development of an independent, dynamic and positive system of information protection rights.

With the emergence of algorithm black box and algorithm tyranny, the requirement of transparency becomes more prominent. Some scholars claim that the right of interpretation exists in GDPR. Article 13-14 can be understood as the notification obligation of information controller and article 15 is the access right of information subject. It states that the information subject should at least provide useful information about the logic used in automatic decision making, the importance of the process, and its possible consequences to the information subject. Some scholars have also invoked preamble article 71," *...to interpret the decision to help the information subject understand the process of the algorithm and achieve relief.*" Therefore, information controllers should not only ensure that people are aware of the existence of the database, but also disclose the standards used in the decision-making process. It is necessary not only to ensure the accuracy of metadata, but also to review the definition of data sets, the presentation of assumptions, the reasoning of algorithms, and the logic behind them.

4.3 Risk-Based Approach

In a nutshell, a statutory accountability principle would explicitly require information controllers to implement appropriate and effective measures to put into effect the principles and obligations of the information protection law and demonstrate this on request. In practice this should translate into scalable programs aiming at implementing the existing information protection principles. The risk-based approach is an appropriate way to provide scalable protection. The so-called "risk-based approach" is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20).It has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation. GDPR requires data controllers to demonstrate compliance with it having regard to, among other things, the '*risks for the rights and freedoms of the data subjects*. Under a wide variety of circumstances, the controller would be required to '*carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks*'.

Risk has become a new boundary in the information protection field and a key indicator in deciding whether additional legal and procedural safeguards are required in a context to shield information subjects from potential negative impacts stemming from specific information processing activities. In this vein Spina notes that EU data protection legislation is undergoing a progressive "riskification". He defines the "riskification" as a shift "from the limited boundaries of formal legality of processing of data and enforcement of individual rights against companies" towards "a model of 'enforced self-regulation' for managing technological innovation in uncertain scenarios". (Alessandro,2017)[1] Risk has been used to steer the way in which regulators are to make use of their discretion to adjust the legal duties and obligations of data controllers. Kuner denotes the new obligation to evaluate risks using Data Protection Impact Assessments as part of a shift from "paper-based bureaucratic requirements" towards "compliance in practice". (Christopher, 2012)

To be specific, when using personal data, enterprises should take appropriate measures to manage the whole lifecycle of the information to ensure the accuracy, integrity and confidentiality of the information. When an enterprise shares personal information with a third party, it shall ensure that the third party receiving personal information complies with obligations such as personal information protection stipulated by law. In case of any breach, sale or illegal provision of personal information by a third party, the enterprise sharing personal information shall also bear corresponding responsibilities.

CONCLUSION

It is necessary to enact the personal information protection act, which is advantageous to the systematic legislation of personal information protection practice in contemporary China. It could improve the status of personal information protection legislation system in our country and promote the information flow which will benefit the development of the information industry. There are many problems

in China's existing legislation and practice. In future legislation, consent should not be the sole legal basis for information processing, and information processing under regulation should be encouraged. At the same time, the accountability of information controllers and the transparency of information processing should be improved, and risk-based approaches should be introduced to provide proportional, situational and low-cost regulatory paths.

REFERENCES

Alessandro, S. (2017). A regulatory marriage de Figaro: Rica ethics. *European Journal of Risk Regulation*, *8*(1), 88-94.

Cate, F. H., & Victor. M. S. (2013). Notice and consent in a world of big data. *International Data Privacy Law*, *3*(2), 67-73.

Christopher, K. (2012). The European commission's proposed data protection regulation: A copernican revolution in European data protection law. *Privacy & Security Law Report*, *11*(6), 1-27.

Fairfield, J. A., & Engel, C. (2015). Privacy as a public good, *Duke L.J. 65*, 385-457.

Froomkin, A. M. (1999). The death of privacy. In L. Stan (Rev. ed.), *52*, 1461-1506.

Herbert, B. (2009). *Towards a new generation of data protection legislation*. In S. Gutwirth et al. (Eds.), Reinventing Data Protection? Amsterdam: Springer.

Julia, B. (2010). *The role of risk in regulatory processes*. In B. Robert, C. Martin, & L. Martin (Eds.), The Oxford Handbook of Regulation. Oxford: Oxford University Press .

Purtova, N. (2014). Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table… and back on again?. *Computer Law & Security Review*, *30*(1), 6-24.

Qi, A. M. (2004). *Research on the principle of personal data protection law and the law of cross-border circulation*, Wuhan, China: Wuhan University Press.

Sokol, D. D., & Comerford, R. (2015). Antitrust and Regulating Big Data. In L. Geo. Mason (Rev. ed.), *23*, 1129-1181.

Tene, O. & Polonetsky, J.(2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*(5), 239-256.

Xie, Y. Z. (2013). *Research on personal data protection legislation*, Beijing. China: People's Court Press.