ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 124

International Conference on Contemporary Education, Social Sciences and Humanities (ICCESSH 2017)

Public Interest Litigation for Personal Information Protection in Big Data Era

A Discussion Based on Chinese Law*

Dudu Jiang
Guangdong University of Foreign Studies
Guangzhou, China 510420

***Abstract*—The promulgation of *Network Security Law* has established our citizens' right to self-determination of personal information and limited right to be forgotten. However, it is still a long way to protect personal information. In the era of big data, the right to self-determination and the right to be forgotten of personal information become feeble and futile. The introduction of public interest litigation will make up for this shortcoming. In the era of big data, personal information has a strong public right attribute, and we can protect our personal information in the form of public interest litigation, and there is no theoretical barrier. The current implementation of public interest litigation of personal information has system obstacles in burden of proof, evidence collection and legal liability system. It is good to convert appropriate burden of proof, stipulate the defendant to coordinate evidence collection and establish civil punitive compensation system on personal information and innovate the main body qualification of the plaintiff in the protection of personal information in big data, and thus facilitate the protection of personal information by public interest litigation.**

Keywords—big data; personal information; public interest litigation; right to self-determination of personal information; Network Security Law

I. INTRODUCTION

On November 7, 2016, the Standing Committee of the National People's Congress passed the *People's Republic of China Network Security Law* (hereinafter referred to as *Network Security Law*), which opened a new era of rule of law in cyberspace. *Network Security Law* has laid a solid foundation for the protection of personal information. First of all, *Network Security Law* establishes the category and use principle of personal information; secondly, it stipulates the personal information protection responsibility of network operators; finally, it also defines citizens' right of claim and information right. [1] It can be said that *Network Security Law* basically meets the legal needs of citizens' personal information protection. However, if we put this protection mode under the background of big data and consider carefully, we will find it may be vague in the protection of personal information. That is to say it couldn't effectively guarantee personal information security. *Network Security Law* has the newest regulations of personal information protection in our country, so it is a comprehensive representation of personal information protection in China. Therefore, the paper first analyzes the deficiencies in the protection of personal information, concludes the demand for public interest litigation in personal information protection, and then discusses theory and practical feasibility of public interest litigation of personal data, and the protection mechanism of public interest litigation on personal data information.

*Fund Project: Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation. ("Climbing Program" Special Funds), Project Number: pdjh2017a0171.

II. THE DEMAND FOR PUBLIC INTEREST LITIGATION IN PUBLIC INFORMATION PROTECTION: DEFICIENCIES IN THE EXISTING LAWS, TAKING *NETWORK SECURITY LAW* AS REPRESENTATIVE

Network Security Law has latest regulations of personal information in our country. It timely responds the network space and network behavior demand for the rule of law in the era of big data, but it, as a general law, did not achieve comprehensive and detailed provisions for each content. It is a foundation of *Network Security Law*. In the traditional fields it is very effective in the protection of personal information, because it stipulates the rights of citizens and network operators' responsibilities. And its intensity of administrative punishment is not weak. However, in the era of big data, the protection role of these regulations is weakened in practice because of the fission effects caused by big data and intelligent technologies. The author concludes its deficiencies in the protection of personal information in the following.

A. The Feeble and Futile Right to Self-Determination and Right to Be Forgotten of Personal Information in the Information Age

1) Network Security Law's protection on personal information: the establishment of right to self-determination and the right to be forgotten of personal information: Network Security Law has a highlight in protection of personal data information that it gives citizens the right to self-determination and the right to be forgotten of personal information.

The right to self-determination of personal information theory was originally produced in Germany. According to German Scholar Steinmüller's definition, the content of this

right is that: people have the right to freely determine what extent the surrounding worlds get their thoughts and actions. The theory maintains the control right on all his/her personal information. It forbids others to collect, spread or use personal information in theory unless the owner of personal information allows. And collectors shall define collecting purpose to order to limit their future information processing behaviors. [2] To this, *Network Security Law* has introduced this theory. In this law, the right to self-determination of personal information is embodied in Article 41 and Article 42. The first paragraph of Article 41 stipulates network operators shall get approval of owners and define collecting and using purpose, methods and scope before collecting and using their personal information. The second paragraph stipulates network operators shall collect and use personal information according to the agreement, and shall process and preserve personal information in accordance with the provisions of laws and administrative regulations and the agreement. The first paragraph of Article 42 stipulates network operators shall not disclose, tamper, deface collecting personal information or provide them to others without the consent of owners.

The right to be forgotten was also first born in Europe. In 2014, the European Court of Justice formally established the concept of the right to be forgotten in the judgment of Google Accusing Gonzales's right to oblivion. "The right to be forgotten refers to the right of personal information owners to ask information control to eliminate their inappropriate and outdated personal information publishing on the internet which will lead to lowering of social evaluation if continue to maintain." [3] In this regard, China's *Network Security Law* has made a reference to the selective right to be forgotten. Article 43 stipulates the owners preserve the right to ask network operators to eliminate their personal information on condition that network operators collect and use personal information in violation of laws and administrative regulations or agreement, and the right to require network operators to alter their personal information on condition that the network operators collect and preserve personal information wrongly. It can be seen that compared with the right to be forgotten in EU law *Network Security Law* only gives the owners the right to ask network operators to eliminate or alter their personal information on condition that network operators collect and use personal information in violation of laws and administrative regulations or agreement or wrongly, while EU law stipulates the owners preserve the right to ask network operators to eliminate all personal information. Therefore, the right to be forgotten in our *Network Security Law* is conditional or amended right.

2) The weakening of the right to self-determination and the right to be forgotten of personal information: unequal parties and low probability of safeguarding rights: The provisions of the personal information right and the right to be forgotten in *Network Security Law* stop network operators' collection at will, infringing and abusing behaviors of any personal information from the law, and citizens have a legal basis for the protection of personal information. We can expect that after *Network Security Law* coming into force, network operators will regulate personal information collection and use behavior to some extent. However, in my view, the provisions of the two rights are still difficult to play a practical role in the protection of personal information. In the environment of big data network and intelligent equipment, the right to self-determination and the right to be forgotten of personal information are feeble and futile.

In the era of big data, all kinds of intelligent equipment develop by leaps and bounds, which provides convenience for people's production and life. Along with the popularization of the technologies and equipment, people depend more and more on smart devices and networks. So, it forms a kind of unequal status between network operators and users. In the case of unequal circumstances, the individual's right to self-determination and the right to be forgotten of personal information are only in name.

Discuss from the right to self-determination of personal information. First of all, as the service provider, the network operator usually asks the user to give certain authorization in the product service. If the user does not authorize it, it will directly result that the consumers can not enjoy the service. In this case, users often have to agree to collect personal information. Secondly, in the big data and network technology environment, except for staff network technology professional and a few enthusiasts interested in network technology, Internet users mostly have limited knowledge on the network technology knowledge. They do not know the consequences that allow network operators to collect and use their personal information. Therefore, in the absence of awareness of the matter users' decision is tantamount to the act of the person without the capacity for civil conduct. Finally, because of the privacy of cyberspace and technology, it is difficult for average citizens to find out when and where their personal information are being collected and used. Therefore, even if *Network Security Law* stipulates "network operators shall collect and use personal information in accordance with legal, legitimate and necessary principles. They shall open collecting and using rules, define collecting and using purpose, methods and scope, and get approval of owners". If the network operator does not comply with the provisions of the law and collect personal information in violation of law, network users are also difficult to find it and safeguard their rights, especially in the era of big data. It is difficult for ordinary people to find their information used for the second time. As for the right to be forgotten of personal information, *Network Security Law* also exists such a problem. Because of the characteristics of the network, it is difficult for citizens to find their personal information being collected and used illegally or wrongly. When citizens find it, it often has result in damage to the citizens. Based on the characteristics of the big data era, "the current personal information protection strategies, such as notification and licensing, fuzzy information, anonymous information and other means, have become infeasible"[4]. In addition, it should be noted that even if it is found that individual citizens' personal information is collected and used in the network illegally, citizens often choose to give up to protect

their rights due to lack of personal power. It means network operators' the cost of illegal collection and use of personal information is next to nothing. Even if the individual citizens choose to maintain their personal information right and claim for damages, the network operator's loss is not worth mentioning. Therefore, in the face of the huge economic value in collection of personal information, some network operators often like to collect and use personal information in a way that is difficult to be found by users and at low cost.

B. The Limitation of Administrative Penalty on Personal Information Protection in Network Security Law

According to Chapter 6 Legal Responsibilities in *Network Security Law*, it stipulates network operators' administrative penalties for violations of law, and the punishment intensity is enough. The maximum fine can be ten times of the illegal cost. Even it may revoke the business license of network operators. Then, can the administrative penalties in *Network Security Law* overcome the drawbacks of the low illegal cost of network operators? The author believes that administrative responsibility can play a certain deterrent role to the data information behavior of network operators. But it is difficult to fully and effectively play the role of personal information protection. First of all, the network administrations have numerous affairs. They should be responsible for all aspects of network security. In the case of limited resources, the administrative organs often tend to supervise major security network events related to state and society. As for the protection of personal information, it is easy to neglect supervision. Secondly, it is not easy to determine the infringement scope of collection and use of personal information. Some behaviors seem to be legal, but are tortuous in essence as mentioned above. It is difficult for administrative organs to determine whether they infringe citizens' personal information right or not. They may be accused by network operators or censured by the society, so administrative organs often refrain from the use of administrative punishment in the protection of citizens' personal information. Finally, some administrative organs are lazy and corrupt. They tend to shelter the strong or be of inaction. Therefore, administrative punishment can play a role in protecting personal information of citizens in a certain extent, but this effect is limited. It is difficult to effectively implement the objective of law to only rely on sufficient law enforcement of administrative organs according to the previous legal practice.

III. FEASIBILITY ANALYSIS OF PUBLIC INTEREST LITIGATION PROTECTION OF PERSONAL INFORMATION

The public interest litigation system is formulated to safeguard the public interest of the society, and the protection of personal information embodies private interests. Therefore, it is necessary to analyze the feasibility of public interest litigation protection of personal information. The following analysis is from three aspects, the reality, the theory and the legal basis of the public interest litigation of personal information.

A. To Eliminate the Inequality of the Two Parties and to Raise the Rate of Safeguarding Rights: the Introduction of Public Interest Litigation to Protect Personal Information

The introduction of the public interest litigation to protect personal information protection can reduce the inequality of individual citizens and the network operator on status, perceptivity and technical capacity, so as to improve the rate of safeguarding rights and increase the illegal collection and use cost of network operators.

First of all, it is often unknown or difficult for ordinary citizens and individuals to find illegal collection and use of personal information behavior. But professional organizations and individuals can perceive and recognize such behaviors. Therefore, if relevant organizations and personnel are allowed to accuse network operators when they illegally collect and use personal information in a large number, it can fully protect citizens' personal information right. Secondly, individual citizen is not enough to deter network operators with limited social influence and filed damages, but relevant organizations and personnel representing social interests can deter them by public interest litigation, for the damages are generally large and have a broad social impact. Finally, public interest litigation's safeguarding power is greater than that of citizen. Therefore, the public interest litigation is the best choice to protect personal information from recognition and perception of network data information behavior, safeguarding power and deterrent power on network operators.

B. The Theoretical Basis of the Public Interest Litigation Protection of Personal Information: the Public Right Attribute in Personal Information

"Public interest litigation refers to the modern lawsuit that a specific organ files to the court to accuse the infringement of social public interest according to the authorization of law" [5]. The public interest litigation system requires that the object of litigation should be public. That is to say it should be a lawsuit for public interest. From our traditional point of view, personal information belongs to the private interests of citizens. However, in the era of big data, personal information is more and more showing the characteristics of public interest. First of all, in the era of big data, personal information is usually collected on a large scale. For network operators, the data information of a single person is worthless, and the value of personal data lies in the aggregation of a large number of personal data. Therefore, the objects of network operators are social public interest since they begin to collect and use personal information data. Secondly, in the large data environment, the accumulation of personal data has great potential value, and the use of these accumulated data can directly affect the public interest. For example, Google successfully predicted the spread of winter flu by collecting people's online search records. [6] It reflects the service of the network operators in the use of personal information for public interest. In addition to serving the social public interests, these methods are also can be used by criminals to violate public interests. Therefore, in the big data environment, the collection, use, reveal and transaction

of personal information have completely broken through the scope of private rights, and have the attributes of public rights. This requires greater protection of personal information than ever before. So, the public interest litigation protection of personal information is in line with the object requirements of public interest litigation.

C. Analysis of the Legal Basis of Public Interest Litigation Protection of Personal Information:

Article 55 of Civil Procedure Law stipulates "law authorities and relevant organizations have the right to file a lawsuit to people's court toward the behaviors of polluting environment, against the legitimate rights and interests of many consumers and damaging the interests of the public". This clause of public interest litigation is easy to make people think that public interest litigation cases are limited to environmental pollution and consumer rights protection. But in reality it is not. Although Article 55 only lists environmental pollution and the protection of consumers' rights and interests, it adopts the incomplete enumeration method and supplements with the behaviors of damaging social public interests. Thus, the examples of environment and consumer problems embody the positive response of legislation to social hot spots. Therefore, in the civil public interest litigation, the case is not limited to environmental pollution and consumer rights protection. As for other public interest litigation cases, it needs to be decided according to its public welfare nature and judicial operability. In a sense, this is to "leave a space for the judicial organs to constantly improve the public interest litigation system in the process of law enforcement" [7]. It avoids introducing some immature public interest litigation cases into judicature.

IV. System Obstacles in Public Interest Litigation Protection of Personal Information and Suggestions for Improvement

The advantages and feasibility of public interest litigation protection of personal information are mentioned above. Ideally, if the various elements to carry out public interest litigation are clear, it is feasible. But the big data and information environment makes all aspects become blurred. It will be difficult to take public interest litigation. The author analyzes the possible obstacles in public interest litigation of personal information in big data environment, and puts forward some relevant suggestions.

A. System Obstacles in the Public Interest Litigation Protection of Personal Information

1) The burden of proof and evidence collection in personal information: Under the network environment and the big data background, the network operator can collect and store all kinds of data information at low cost, on a large scale and simply, which brings a series of difficulties to the lawsuit. As for the burden of proof, according to the existing civil procedural law, the burden of proof is "who advocates who provides proof". Therefore, in the personal information litigation, it is necessary for the plaintiff to provide proof in terms of network operators' illegal behavior. In general, personal information collected by network operators are stored and controlled by the single side. Network data collection has the secret characteristic. It makes it difficult for others to prove network operators collected and used personal information illegally. When the parties concerned charge them, the collectors can modify and control the information. In addition, in the era of big data, the secondary use of data information makes it difficult for others to find and identify violations of personal information. Without evidence, it is difficult to reach prosecution standards or fail to win in cases.

In fact, the problem lies in evidence collection. According to the civil procedure law, the parties concerned may apply to the court for investigation and collection of evidence. But this will involve two questions; one is whether the court has the professional technical ability; the other is that almost all personal information is controlled by collectors. If all apply to the court for investigation in such cases, it may result in litigation exhaustion and resource shortage of the court. These are all obstacles to take public interest litigation of personal information.

2) The incomplete legal liability system: At present, there is no complete legal system for protecting personal data in China. *Network Security Law* issued recently has systematically incorporated personal information into the scope of legal protection. However, as mentioned above, *Network Security Law* is a foundation of law. It directs the rule of law in the whole network space. But it did not make detailed provisions on the comprehensive aspects. In the legal responsibility, *Network Security Law* only stipulates the administrative liability of illegal activities, and does not stipulate civil liability. It results that the court lacks appropriate judgment basis in the public interest litigation of personal information and only requires to stop infringement, recover the original state or eliminate the obstruction according to current law. As for damages, the court can only make judgment according to specific loss. As mentioned above, it is difficult to determine the loss caused by personal information data infringement. So it is difficult to deter network operators.

In addition, Article 111 *General Rules of Civil Law* issued recently also emphasizes the protection of personal information. But because it is a legislation of general rules, it doesn't stipulate legal liability. So it is still a declaratory protection and needs the stipulation of the specific parts of civil law in the future. [1]

B. Suggestions to Perfect Public Interest Litigation of Personal Information Protection System

1) Appropriate conversion of burden of proof and duty to cooperate with evidence collection: As mentioned above it is difficult to collect proof in personal information

[1] See Article 111 of *General Rules of Civil Law*: The personal information of natural persons is protected by law. Any organization and individual shall legally get and ensure information security if needs to obtain personal information of others, and shall not collect, use, process, transmit, exchange, provide or open personal information of others illegally.

litigation. So, it is necessary to rationally distribute the burden of proof. According to the characteristics of network data collection, the plaintiff can claim network operators to provide the evidence of no illegal collection, use, storage behaviors as they control collecting information and "prove the legal source of collecting information, otherwise, judge network operators as infringement" [8]. Specifically, require them open its internal information collection system, program, procedure and characteristics of information collection technology and require users to demonstrate its legal sources of information and specific ways of use, and the related results obtained from the data in use (these results may be related to the citizens' privacy).

The network operators sometimes prove their legality by concealing, transferring or deleting information. Therefore, the plaintiff still needs to request the court or other participants in the proceedings of investigation. At this time network operators shall cooperate to take evidence in their platform and not set up technical barriers.

2) The establishment of civil penalty compensation system for personal information: As mentioned above, *Network Security Law* only stipulates the administrative liability for network operators and lacks civil liability. Although Consumer Rights and Interests Protection Law stipulates operators' responsibilities to "stop infringement, rehabilitate reputations, eliminate effects, apology and compensate for loss" when provide goods or services. But in the era of big data it is difficult to determine the losses. So, the simple stipulation about "damages" is hard to protect personal information in the era of big data. Moreover, Consumer Rights and Interests Protection Law applies only to the collection and use of personal information in the consumer field. Therefore, it is necessary to provide more diversified civil liability for the protection of personal information. Among them, the author thinks that the most important thing is to set up the punitive compensation liability for infringing personal information. The network operators covet the huge economic value brought by personal information collection and take a risk. Only by taking punitive damages from network operators can we deter illegal behaviors of network operators and they make rational behavior.

3) The plaintiff's subject qualification innovation adapting to the Big Data Era: In the era of big data, the network technology of collecting and using personal information is changing constantly. It is difficult for ordinary people to recognize and understand the change of network knowledge. Due to professionalism and timeliness, the plaintiff of the public interest litigation of personal information shall be acted by parties that grasp network technology and big data technology. In this regard, the author believes that the plaintiff of public interest litigation of personal information shall give network operator the qualification of plaintiff in addition to the plaintiff qualification of relevant organs and organizations (usually refer to the procuratorial organs and industry associations etc.) stipulated by current civil procedure law. First of all, the network operator has incomparable network technology recognition ability. They can easily find illegal collection behavior of other network operators. Secondly, it can make full use of competitive effect and mutual supervision among network operators by giving them the qualification of plaintiff. For example, Qihoo 360 and Tencent criticize each other infringing users' personal information [9]. This is the competition effect. If it can stop competitors infringing personal information to give the main body of public interest litigation qualification and form benign space network. Finally, it will not result in abuse of accusation to give network operators the main body qualification of public interest litigation. One the one hand it is because the finite number of network operators (comparing with that of the ordinary citizen personally). On the other hand, according to economic rationality, network operators generally crack down the competitors by accusing their peer operators. So the number will be more limited.

REFERENCES

[1] Zhu Wei. The Problem of Personal Information Security in *Network Security Law* (Draft). China Information Security. 2015 (08).

[2] Yang Fang. The Theory and Review of the Right to Self-determination of Personal Information - Protection Object of Personal Information Protection Law. Comparative Law Research. 2015 (06).

[3] Yang Lixin & Han Xu. Chinese Localization and the Legal Application of the Right to be Forgotten. Application of Law. 2015 (02).

[4] Hou Fuqiang. Problems and Legal Countermeasures of Personal Information Protection in Big Data Era. Journal of Southwest University for Nationalities (HUMANITIES AND SOCIAL SCIENCES), 2015 (06).

[5] Xiao Jianhua, Tang Yufu. Theoretical Basis and Procedural Construction of Public Interest Litigation. Journal of Henan Institute of Political Science and Law, 1st Edition in 2008.

[6] (British) Victor Maier • Schoenberg, Kenneth • Cukier. The Era of Big Data: Changes in Life, Work and Thinking. Zhejiang People's Publishing House. 2013: 3.

[7] Sun Youhai. Understanding of the Public Interest Litigation System in the Revised Civil Procedure Law. Journal of Law. 2012 (12).

[8] Wang Shuo. To Implement the Conversion of Burden of Proof in Personal Information Protection. Chinese Consumer Newspaper. 2014/6/13 (A01).

[9] See Liu Kun. After the Company War between QQ and 360. Three Controversial Issues in the Legal Profession: Do Laws Protect Free Users? [EB / OL]. http://www.nbd.com.cn/articles/2010-11-18/410498.html. The last access time: February 28, 2017 15: 50.